kaspersky

Kaspersky Anti Targeted Attack Platform

© 2026 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky Anti Targeted Attack Platform

О Kaspersky Anti Targeted Attack Platform

- Что нового
- Исправленные проблемы
- Использование Kaspersky Threat Intelligence Portal
- Комплект поставки
- Аппаратные и программные требования
  - Совместимость версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform
  - Совместимость версий Kaspersky Endpoint Security для Linux с версиями Kaspersky Anti Targeted Attack Platform
  - Совместимость Kaspersky Endpoint Security для Mac с версиями Kaspersky Anti Targeted Attack Platform
  - Совместимость версий KUMA с версиями Kaspersky Anti Targeted Attack Platform
  - Совместимость версий XDR с версиями Kaspersky Anti Targeted Attack Platform
  - Совместимость версий KPSN с версиями Kaspersky Anti Targeted Attack Platform
  - Совместимость Kaspersky Anti Targeted Attack Platform с VK Cloud
- Ограничения
  - Общие ограничения
  - Развертывание Central Node в виде кластера
  - Ограничения Sensor
  - Ограничения Sandbox
  - Развертывание приложения на платформах виртуализации
  - Использование приложения в режиме распределенного решения и мультитенантности
  - Ограничения совместимости с Kaspersky Endpoint Security для Windows
  - Ограничения совместимости с Kaspersky Endpoint Security для Linux
  - Ограничения совместимости с Kaspersky Endpoint Security для Mac
  - Ограничения совместимости с XDR
  - Интеграция с прокси-сервером по протоколу ICAP

Предоставление данных

- Служебные данные приложения
- Данные компонентов Central Node и Sensor
  - Данные трафика компонента Sensor
  - Данные в обнаружениях
  - Данные в событиях
  - Данные в отчетах
  - Данные об объектах в Хранилище и на карантине
- Данные компонента Sandbox
- Данные, пересылаемые между компонентами приложения
- Данные в файлах трассировки приложения
- Данные Kaspersky Endpoint Security для Windows
- Данные Kaspersky Endpoint Security для Linux
- Данные Kaspersky Endpoint Security для Mac

Лицензирование приложения

- О Лицензионном соглашении
- О Лицензионном сертификате

- О лицензии
- О лицензионном ключе
- О файле ключа
- О коде активации
- О подписке
- Добавление лицензионного ключа
- Замена лицензионного ключа
- Удаление лицензионного ключа
- Просмотр информации о добавленных лицензионных ключах в веб-интерфейсе Central Node
- Просмотр текста Лицензионного соглашения в веб-интерфейсе Central Node
- Просмотр текста Политики конфиденциальности в веб-интерфейсе Central Node
- Просмотр информации о стороннем коде, используемом в приложении
- Просмотр текста Лицензионного соглашения в веб-интерфейсе Sandbox
- Просмотр текста Лицензионного соглашения компонента Endpoint Agent
- Режимы работы приложения в соответствии с лицензией

Архитектура приложения
- Компонент Sensor
- Компонент Central Node
- Компонент Sandbox
- Компонент Endpoint Agent

Принцип работы приложения

Распределенное решение и мультитенантность
- Сценарий перехода в режим распределенного решения и мультитенантности
- Изменения в параметрах приложения при переходе в режим распределенного решения и мультитенантности
- Назначение серверу роли PCN
- Назначение серверу роли SCN
- Обработка запросов на подключение SCN к PCN
- Просмотр информации о тенантах, серверах PCN и SCN
- Добавление тенанта на сервере PCN
- Удаление тенанта на сервере PCN
- Изменение названия тенанта на сервере PCN
- Восстановление подключения SCN к PCN
- Отключение SCN от PCN
- Изменения в параметрах приложения при отключении SCN от PCN

Руководство по масштабированию
- Типовые схемы развертывания и установки компонентов приложения
  - Схема развертывания на два сервера
  - Схема развертывания на три сервера
  - Схема развертывания на четыре и более сервера
  - Схема развертывания функциональности KEDR с компонентом Sandbox
  - Схема развертывания функциональности KEDR без компонента Sandbox
- Калькулятор масштабирования
  - Расчеты для компонента Sensor
  - Расчеты для компонента Central Node при использовании функциональности KATA
  - Расчеты для компонента Central Node при использовании функциональности KEDR
  - Расчеты для компонента Central Node при использовании функциональности KATA и KEDR
  - Расчеты для компонента Central Node при использовании функциональности KATA и NDR

Расчеты для компонента Central Node при использовании функциональности KATA, KEDR и NDR
Расчеты для компонента Central Node при наличии интегрированных внешних систем
Расчеты для компонента Central Node при интеграции с Kaspersky Secure Mail Gateway
Расчеты для компонента Central Node при использовании функциональности ICAP
Расчеты для компонента Central Node в режиме распределенного решения и мультитенантности
Расчеты для компонента Central Node, развернутого в виде кластера
Расчеты для малых конфигураций решения
Расчет объема базы событий и Хранилища для настройки параметров масштабирования приложения
Расчеты для компонента Sandbox
Установка и первоначальная настройка приложения
Подготовка к установке компонентов приложения
Подготовка IT-инфраструктуры к установке компонентов приложения
Подготовка IT-инфраструктуры к интеграции с почтовым сервером для приема сообщений по протоколу POP3
Подготовка IT-инфраструктуры к интеграции с почтовым сервером для отправки сообщений по протоколу SMTP
Подготовка виртуальной машины к установке компонента Sandbox
Подготовка установочного образа диска с компонентами Central Node, Sensor и Sandbox
Порядок установки и настройки компонентов приложения
Установка компонента Sandbox
Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности
Шаг 2. Выбор диска для установки компонента Sandbox
Шаг 3. Настройка минимальной длины пароля администратора Sandbox
Шаг 4. Создание учетной записи администратора Sandbox
Шаг 5. Настройка управляющего сетевого интерфейса
Шаг 6. Назначение имени хоста и добавление адресов DNS-серверов
Шаг 7. Настройка статического сетевого маршрута
Развертывание компонента Central Node со встроенным Sensor в виде кластера
Развертывание сервера хранения данных
Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности
Шаг 2. Выбор роли сервера
Шаг 3. Выбор режима развертывания
Шаг 4. Выбор диска для установки компонента
Шаг 5. Выбор маски сети для адресации серверов
Шаг 6. Выбор маски сети для адресации компонентов приложения
Шаг 7. Выбор кластерного сетевого интерфейса
Шаг 8. Выбор внешнего сетевого интерфейса
Шаг 9. Выбор способа получения IP-адресов для сетевых интерфейсов
Шаг 10. Создание учетной записи администратора и аутентификация сервера в кластере
Создание учетной записи администратора
Аутентификация сервера в кластере
Шаг 11. Добавление адресов DNS-серверов
Шаг 12. Настройка синхронизации времени с NTP-сервером
Шаг 13. Выбор дисков для Ceph-хранилища
Развертывание обрабатывающего сервера
Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности
Шаг 2. Выбор роли сервера
Шаг 3. Выбор диска для установки компонента
Шаг 4. Выбор маски сети для адресации серверов кластера

Шаг 5. Выбор маски сети для адресации компонентов приложения
Шаг 6. Выбор кластерного сетевого интерфейса
Шаг 7. Выбор внешнего сетевого интерфейса
Шаг 8. Выбор способа получения IP-адресов для сетевых интерфейсов
Шаг 9. Аутентификация сервера в кластере
Шаг 10. Выбор языка локализации функциональности NDR и настройка получения зеркалированного трафика со SPAN-портов
Выбор языка локализации функционала NDR
Настройка получения зеркалированного трафика со SPAN-портов
Очистка жестких дисков на серверах хранения
Установка компонента Central Node со встроенным Sensor на сервере
Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности
Шаг 2. Выбор роли сервера
Шаг 3. Выбор диска для установки компонента
Шаг 4. Выделение диска для базы данных компонента Targeted Attack Analyzer
Шаг 5. Выбор маски сети для адресации серверов
Шаг 6. Выбор маски сети для адресации компонентов приложения
Шаг 7. Выбор внешнего сетевого интерфейса
Шаг 8. Выбор способа получения IP-адресов для сетевых интерфейсов
Шаг 9. Создание учетной записи администратора
Шаг 10. Выбор языка локализации функционала NDR
Шаг 11. Добавление адресов DNS-серверов
Шаг 12. Настройка синхронизации времени с NTP-сервером
Установка компонента Sensor на отдельном сервере
Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности
Шаг 2. Выбор роли сервера
Шаг 3. Выбор диска для установки компонента
Шаг 4. Выбор маски сети для адресации серверов
Шаг 5. Выбор маски сети для адресации компонентов приложения
Шаг 6. Выбор внешнего сетевого интерфейса
Шаг 7. Выбор способа получения IP-адресов для сетевых интерфейсов
Шаг 8. Создание учетной записи администратора
Шаг 9. Добавление адресов DNS-серверов
Шаг 10. Настройка синхронизации времени с NTP-сервером
Оптимизация настроек сетевых интерфейсов для компонента Sensor
Подключение и настройка внешнего хранилища для компонента Sensor
Настройка параметров масштабирования приложения
Настройка правил сетевого экрана
Порты, используемые на компьютерах с установленными компонентами Kaspersky Anti Targeted Attack Platform
Порты, используемые сервисами Kaspersky Anti Targeted Attack Platform в кластерной конфигурации
Порты, используемые сервисами Central Node, установленного на сервере
Порты, используемые сервисами в конфигурации с компонентом Sensor, установленным на отдельном сервере
Порты для взаимодействия между сервисами анализа трафика сети
Управление параметрами MTU в iptables
Настройка интеграции компонента Endpoint Agent с функциональным блоком KEDR
Настройка доверенного соединения с приложением Kaspersky Endpoint Security
Скачивание TLS-сертификата сервера Central Node на компьютер

- Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Anti Targeted Attack Platform
- Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Anti Targeted Attack Platform
- Включение проверки TLS-сертификата компонента Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform
- Генерация TLS-сертификата компонента Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и скачивание криптоконтейнера
- Загрузка самостоятельно подготовленного TLS-сертификата компонента Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform
- Просмотр таблицы TLS-сертификатов компонента Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform
- Фильтрация и поиск TLS-сертификатов компонента Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform
- Удаление TLS-сертификатов компонента Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform
- Настройка перенаправления трафика от компонента Endpoint Agent на сервер Sensor

Настройка интеграции компонента Endpoint Agent с функциональным блоком NDR

- Сценарий подготовки к получению данных от компонента Endpoint Agent
- Таблица серверов интеграции
- Добавление сервера интеграции
- Создание файла свертки для клиентов сервера интеграции
- Включение и выключение сервера интеграции
- Изменение параметров сервера интеграции
- Удаление сервера интеграции

Интеграция с почтовыми сенсорами

Начало работы с приложением

- Начало работы в веб-интерфейсе приложения под учетной записью администратора
- Начало работы в меню администратора приложения
- Начало работы с приложением в режиме Technical Support Mode

Управление учетными записями администраторов и пользователей приложения

- Создание учетной записи администратора веб-интерфейса приложения
- Создание учетной записи пользователя веб-интерфейса приложения
- Настройка отображения таблицы учетных записей
- Просмотр таблицы учетных записей
- Фильтрация учетных записей
- Сброс фильтра учетных записей
- Изменение прав доступа учетной записи к данным PCN и SCN
- Включение и отключение учетной записи
- Изменение пароля учетной записи
- Изменение пароля своей учетной записи

Аутентификация с помощью доменных учетных записей

- Создание keytab-файла
- Настройка интеграции с Active Directory
- Отключение интеграции с Active Directory

Участие в Kaspersky Security Network и использование Kaspersky Private Security Network

- Просмотр Положения о KSN и настройка участия в KSN
- Включение использования KPSN
- Настройка подключения к локальной репутационной базе KPSN

Настройка сохранения информации в локальную репутационную базу KPSN
Отказ от участия в KSN и использования KPSN
Работа с компонентом Sandbox через веб-интерфейс
Обновление баз компонента Sandbox
Запуск обновления баз вручную
Выбор источника обновления баз
Обновление баз компонента с помощью Kaspersky Update Utility
Скачивание пакетов обновлений с помощью Kaspersky Update Utility
Включение и отключение использования прокси-сервера для обновления баз
Настройка параметров соединения с прокси-сервером для обновления баз
Настройка соединения компонентов Sandbox и Central Node
Обработка запросов на подключение от серверов Central Node в веб-интерфейсе Sandbox
Настройка сетевых интерфейсов компонента Sandbox
Настройка параметров DNS
Настройка параметров управляющего сетевого интерфейса
Настройка параметров сетевого интерфейса для доступа обрабатываемых объектов в интернет
Добавление, изменение и удаление статических сетевых маршрутов
Политики аутентификации на Sandbox
Завершение неактивных сессий на Sandbox
Информирование о неуспешных попытках аутентификации на Sandbox
Установка даты и времени системы Sandbox
Подготовка виртуальных машин к работе
Работа с образами операционных систем и приложений в Хранилище Sandbox
Просмотр таблицы образов операционных систем и приложений в Хранилище Sandbox
Загрузка образов операционных систем и приложений в Хранилище
Активация образов операционных систем и приложений в Хранилище Sandbox
Удаление образов операционных систем и приложений из Хранилища Sandbox
Работа с шаблонами виртуальных машин
Создание шаблона виртуальной машины
Просмотр таблицы шаблонов
Включение и выключение шаблона
Редактирование шаблона
Настройка операционной системы и программного обеспечения
Устранение уязвимостей типа Spectre и Meltdown
Удаление Защитника Windows
Экспорт шаблона
Импорт шаблона
Удаление шаблона
Управление виртуальными машинами
Создание виртуальной машины
Создание виртуальной машины в разделе Виртуальные машины
Создание виртуальной машины в таблице шаблонов
Создание виртуальной машины в окне просмотра шаблона
Создание и установка виртуальной машины через командную строку
Просмотр таблицы преднастроенных виртуальных машин
Просмотр таблицы пользовательских виртуальных машин
Установка виртуальной машины

Удаление виртуальной машины
Загрузка отладочных символов
Установка максимального количества одновременно запускаемых виртуальных машин
Изменение количества лицензионных ключей для пользовательской виртуальной машины
Экспорт параметров Sandbox
Импорт параметров Sandbox
Перезагрузка сервера Sandbox
Выключение сервера Sandbox
Изменение пароля учетной записи администратора Sandbox
Администратору: работа в веб-интерфейсе приложения
Интерфейс Kaspersky Anti Targeted Attack Platform
Мониторинг работы приложения
О виджетах и схемах расположения виджетов
Выбор тенанта и сервера для работы в разделе Мониторинг
Добавление виджета на текущую схему расположения виджетов
Перемещение виджета на текущей схеме расположения виджетов
Изменение отображения данных в виджетах NDR
Удаление виджета с текущей схемы расположения виджетов
Сохранение схемы расположения виджетов в PDF
Настройка периода отображения данных на виджетах
Мониторинг приема и обработки входящих данных
Мониторинг очередей обработки данных модулями и компонентами приложения
Мониторинг обработки данных компонентом Sandbox
Просмотр состояния работоспособности модулей и компонентов приложения
Работа с информацией о серверах с компонентами Central Node и Sensor
Просмотр информации о серверах с компонентами Central Node и Sensor
Просмотр информации о сетевых интерфейсах
Определение Ethernet-порта, связанного с сетевым интерфейсом
Управление серверами Central Node, PCN или SCN с помощью веб-интерфейса приложения
Настройка даты и времени сервера
Генерация или загрузка TLS-сертификата сервера
Скачивание TLS-сертификата сервера на компьютер
Назначение FQDN-имени сервера
Настройка параметров DNS
Настройка параметров сетевого интерфейса
Настройка сетевого маршрута для использования по умолчанию
Настройка параметров соединения с прокси-сервером
Настройка параметров соединения с почтовым сервером
Управление параметрами сохранения трафика
Управление параметрами сохранения файлов дампа трафика
Управление компонентом Sensor
Подключение компонента Sensor к Central Node
Подключение компонента Sensor с помощью файла свертки
Добавление и подключение компонента Sensor автоматически по сети
Удаление компонента Sensor
Изменение параметров Sensor, установленного отдельно от Central Node
Подготовка к изменению параметров Sensor, установленного отдельно от Central Node

- Управление сертификатом сервера Sensor
  - Генерация TLS-сертификата сервера Sensor в меню администратора сервера Sensor
  - Загрузка самостоятельно подготовленного TLS-сертификата через меню администратора сервера Sensor
  - Скачивание TLS-сертификата сервера Sensor на компьютер
- Изменение имени сервера
- Управление точками мониторинга
  - Добавление точки мониторинга
  - Переименование точки мониторинга
  - Включение точек мониторинга
  - Выключение точек мониторинга
  - Удаление точки мониторинга
- Настройка максимального размера проверяемого файла
- Настройка записи содержимого HTTP-пакета
- Настройка интеграции с почтовым сервером по протоколу SMTP
- Настройка интеграции с прокси-сервером по протоколу ICAP
  - Включение и отключение интеграции с прокси-сервером по протоколу ICAP
  - Включение и отключение проверки ICAP-трафика в режиме реального времени
  - Настройка параметров проверки ICAP-трафика в режиме реального времени
  - Настройка отображения страниц уведомлений
- Настройка записи зеркалированного трафика со SPAN-портов
  - Выбор сетевых протоколов для получения зеркалированного трафика со SPAN-портов
  - Настройка параметров записи зеркалированного трафика со SPAN-портов
- Настройка интеграции с почтовым сервером по протоколу POP3

Политики аутентификации
- Обязательная смена пароля после первой успешной аутентификации
- Обязательная смена пароля по истечении заданного периода
- Завершение неактивных сессий
- Информирование о неуспешных попытках аутентификации

Управление кластером
- Просмотр таблицы серверов кластера
- Добавление сервера в кластер
- Увеличение дискового пространства сервера хранения
- Перезагрузка серверов кластера
- Вывод серверов из эксплуатации
  - Удаление сервера из кластера
- Включение и выключение кластера

Уведомления о максимальной загрузке центрального процессора и оперативной памяти серверов Central Node и Sensor
- Настройка максимального допустимого значения загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor

Настройка соединения по протоколу SNMP
- Описание объектов MIB Kaspersky Anti Targeted Attack Platform

Работа с информацией о хостах с компонентом Endpoint Agent
- Выбор тенанта для работы в разделе Endpoint Agents
- Просмотр таблицы хостов с компонентом Endpoint Agent на отдельном сервере Central Node
- Просмотр информации о хосте
- Фильтрация и поиск хостов с компонентом Endpoint Agent по имени хоста

Фильтрация и поиск хостов с компонентом Endpoint Agent, изолированных от сети
Фильтрация и поиск хостов с компонентом Endpoint Agent по именам серверов PCN и SCN
Фильтрация и поиск хостов с компонентом Endpoint Agent по IP-адресу компьютера
Фильтрация и поиск хостов с компонентом Endpoint Agent по версии операционной системы на компьютере
Фильтрация и поиск хостов с компонентом Endpoint Agent по версии компонента
Фильтрация и поиск хостов с компонентом Endpoint Agent по их активности
Быстрое создание фильтра хостов с компонентом Endpoint Agent
Сброс фильтра хостов с компонентом Endpoint Agent
Настройка показателей активности компонента Endpoint Agent
Удаление хостов с компонентом Endpoint Agent
Автоматическое удаление неактивных хостов
Настройка интеграции с компонентом Sandbox
Просмотр таблицы серверов с компонентом Sandbox
Создание запроса на подключение к серверу с компонентом Sandbox
Включение и отключение соединения с компонентом Sandbox
Удаление соединения с компонентом Sandbox
Выбор операционных систем для проверки объектов в Sandbox
Ручная отправка файлов с хостов с компонентом Endpoint Agent на проверку в Sandbox
Включение и отключение ручной отправки файлов с хостов Endpoint Agent на проверку в Sandbox
Настройка интеграции с внешними системами
Просмотр таблицы внешних систем
Обработка запроса от внешней системы
Удаление внешней системы из списка разрешенных к интеграции
Настройка приоритета обработки трафика от почтовых сенсоров
Настройка интеграции с Kaspersky Managed Detection and Response
Включение интеграции с MDR
Отключение интеграции с MDR
Замена конфигурационного файла MDR
Настройка интеграции с SIEM-системой
Включение и отключение записи информации в удаленный журнал
Настройка основных параметров интеграции с SIEM-системой
Загрузка TLS-сертификата
Включение и отключение TLS-шифрования соединения с SIEM-системой
Содержание и свойства syslog-сообщений об обнаружениях
Управление коннекторами
Об управляемых и неуправляемых коннекторах
Об отправке событий, сообщений приложения и записей аудита в сторонние системы
Об автоматическом управлении сетевым доступом устройств с помощью коннекторов типа Cisco Switch
Добавление коннектора
Просмотр таблицы коннекторов
Включение и выключение коннектора
Изменение параметров коннектора
Создание нового файла свертки для коннектора
Удаление коннектора

Добавление и удаление типов коннекторов
Просмотр таблицы типов коннекторов
Добавление типа коннектора
Удаление типа коннектора
Управление секретами с учетными данными для удаленных подключений
Добавление секрета
Просмотр таблицы секретов
Защита от компрометации секретов при удаленных подключениях к устройствам
Изменение параметров секрета
Удаление секретов
Обновление баз приложения
Выбор источника обновления баз
Запуск обновления баз вручную
Обновление баз приложения с помощью Kaspersky Update Utility
Скачивание пакетов обновлений с помощью Kaspersky Update Utility
Обновление сертификата для подключения к Central Node через API
Интеграция со средствами для раскрытия зашифрованного SSL/TLS-трафика
Сотруднику службы безопасности: работа в веб-интерфейсе приложения
Интерфейс Kaspersky Anti Targeted Attack Platform
Выбор тенанта для работы в веб-интерфейсе приложения
Мониторинг работы приложения
О виджетах и схемах расположения виджетов
Добавление виджета на текущую схему расположения виджетов
Перемещение виджета на текущей схеме расположения виджетов
Изменение отображения данных в виджетах NDR
Удаление виджета с текущей схемы расположения виджетов
Сохранение схемы расположения виджетов в PDF
Настройка периода отображения данных на виджетах
Настройка масштаба отображения виджетов
Основные принципы работы с виджетами типа "Алерты"
Информация в виджете Устройства
Информация в виджете События
Просмотр состояния работоспособности модулей и компонентов приложения
Управление технологиями
Включение и выключение технологий
Настройка режима работы технологии Обнаружение активности устройств
Управление наследованием технологий
Просмотр таблицы алертов
Настройка отображения таблицы алертов
Фильтрация, сортировка и поиск алертов
Фильтрация алертов по наличию статуса VIP
Фильтрация и поиск алертов по времени
Фильтрация алертов по степени важности
Фильтрация и поиск алертов по категориям обнаруженных объектов
Фильтрация и поиск алертов по полученной информации
Фильтрация и поиск алертов по адресу источника
Фильтрация и поиск алертов по адресу назначения

Фильтрация и поиск алертов по имени сервера
Фильтрация и поиск алертов по названию технологии
Фильтрация и поиск алертов по состоянию их обработки пользователем
Фильтрация и поиск алертов по имени пользователя, которому они назначены
Сортировка алертов в таблице
Быстрое создание фильтра алертов
Сохранение фильтров
Сброс фильтра алертов
Рекомендации по обработке алертов
Рекомендации по обработке AM-алертов
Рекомендации по обработке TAA-алертов
Рекомендации по обработке SB-алертов
Рекомендации по обработке IOC-алертов
Рекомендации по обработке YARA-алертов
Рекомендации по обработке IDS-алертов
Рекомендации по обработке NDR:IDS- и AA-алертов
Просмотр алертов
Просмотр информации об алерте
Общая информация об алерте любого типа
Информация в блоке Информация об объекте
Информация в блоке Детали алерта
Информация в блоке Сведения о проверке технологиями NDR
Информация в блоке Результаты проверки
Информация в блоке Правило IDS
Информация в блоке URL
Информация в блоке IP устройств, связанных с обнаружением
Информация в блоке Сетевое событие
Результаты проверки в Sandbox
Результаты IOC-проверки
Информация в блоке Хосты
Информация в блоке Журнал изменений
Отправка данных об алерте
Просмотр связей алерта
Действия пользователей с алертами
Назначение алертов определенному пользователю
Отметка о завершении обработки одного алерта
Отметка о завершении обработки алертов
Изменение статуса VIP алертов
Добавление комментария к алерту
Мониторинг событий в трафике сети
Оценки и уровни критичности событий NDR
Технологии регистрации событий NDR
Статусы событий NDR
Таблица зарегистрированных событий NDR
Настройка таблицы зарегистрированных событий
Просмотр событий, вложенных в агрегирующее событие
Просмотр подробных данных о событии NDR

- Изменение статусов событий NDR
- Установка меток
- Копирование событий NDR в текстовый редактор
- Загрузка трафика для событий
- Создание директории для экспорта событий на сетевой ресурс

Поиск угроз по базе событий

- Поиск событий в режиме конструктора
- Поиск событий в режиме исходного кода
- Конвертация в запрос для поиска событий в режиме исходного кода
- Критерии для поиска событий
- Операторы
- Сортировка событий в таблице
- Изменение условий поиска событий
- Поиск событий типа Обнаружение и Результат обработки обнаружения
- Поиск событий по условиям, заданным в файле формата IOC и YAML
- Создание правила TAA (IOA) на основе условий поиска событий

Информация о событиях

- Рекомендации по обработке событий
  - Выполнение рекомендации по изоляции хоста
  - Выполнение рекомендации по запрету запуска файла
  - Выполнение рекомендации по созданию задачи
- Информация о событиях в дереве событий
  - Просмотр информации о родительском процессе в дереве событий
  - Просмотр информации о событиях, инициированных родительским процессом, в дереве событий
  - Просмотр информации о хосте в дереве событий
- Просмотр таблицы событий
- Настройка отображения таблицы событий
- Просмотр информации о событии
- Информация о событии Запущен процесс
- Информация о событии Завершен процесс
- Информация о событии Загружен модуль
- Информация о событии Удаленное соединение
- Информация о событии Правило запрета
- Информация о событии Заблокирован документ
- Информация о событии Изменен файл
- Информация о событии Журнал событий ОС
- Информация о событии Изменение в реестре
- Информация о событии Прослушан порт
- Информация о событии Загружен драйвер
- Информация о событии DNS
- Информация о событии LDAP
- Информация о событии Именованный канал
- Информация о событии WMI
- Информация о событии Обнаружение
- Информация о событии Результат обработки обнаружения
- Информация о событии Интерпретированный запуск файла
- Информация о событии AMSI-проверка

Информация о событии Интерактивный ввод команд в консоли
Информация о событии Внедрение кода
Информация о событии Доступ к процессу
Информация о событии USB-устройство
Проверка цепочек событий по правилам TAA (IOA) "Лаборатории Касперского"
Включение и выключение проверки цепочек событий по правилам TAA (IOA) "Лаборатории Касперского"
Просмотр событий, отмеченных правилом TAA (IOA) "Лаборатории Касперского"
Управление активами
Просмотр таблицы устройств
Просмотр информации об устройстве
Автоматическое добавление и обновление устройств
Добавление устройств вручную
Добавление устройства при работе с таблицей устройств
Добавление устройства при работе с топологической картой
Добавление устройства на основе узла неизвестного устройства на карте сетевых взаимодействий
Добавление устройства на основе неуправляемого коммутатора на топологической карте
Автоматическое присвоение статусов устройств
Автоматическая группировка устройств по заданному критерию
Автоматическая группировка устройств по заданному критерию, начиная с верхнего уровня иерархии в дереве групп
Автоматическая группировка устройств в выбранной группе устройств
Распределение устройств по группам вручную
Включение одного устройства в группу
Включение нескольких устройств в группу
Исключение одного устройства из группы
Исключение нескольких устройств из групп
Перемещение серверов с компонентами и групп в другие группы на карте сетевых взаимодействий
Дерево групп устройств
Формирование дерева групп устройств вручную
Добавление группы
Переименование группы
Удаление групп
Перемещение группы
Поиск групп
Обновление дерева
Установка и удаление меток для устройств
Установка меток для одного устройства
Установка меток для нескольких устройств
Удаление меток для одного устройства
Очистка списков меток для нескольких устройств
Реагирование
Контроль пользователей на устройствах
Контроль запусков исполняемых файлов на устройствах
Задания активных опросов устройств
Добавление задания активного опроса
Изменение задания активного опроса
Просмотр таблицы заданий активных опросов

Запуск и остановка заданий активных опросов
Просмотр общих сведений о выполнении запусков заданий активных опросов
Просмотр отчета о выполнении задания активного опроса
Удаление заданий активных опросов
Настройка адресных пространств
О правилах адресных пространств
О подсетях адресных пространств
Добавление адресного пространства
Формирование списка подсетей для контроля активов
Добавление подсети
Изменение параметров подсети
Удаление подсетей
Просмотр сведений об устройствах с IP-адресами из выбранных подсетей
Изменение адресного пространства
Удаление адресного пространства
Работа с картой сетевых взаимодействий
Узлы на карте сетевых взаимодействий
Группы устройств на карте сетевых взаимодействий
Соединения на карте сетевых взаимодействий
Просмотр подробных сведений об объектах
Изменение масштаба карты сетевых взаимодействий
Позиционирование карты сетевых взаимодействий
Закрепление и открепление узлов и групп
Изменение местоположения узлов и групп вручную
Автоматическое распределение узлов и групп
Поиск узлов на карте сетевых взаимодействий
Фильтрация объектов на карте сетевых взаимодействий
Комплексная фильтрация узлов и соединений
Фильтрация с помощью периода на временной шкале
Фильтрация по зарегистрированным событиям
Фильтрация узлов
Фильтрация узлов по статусам устройств
Фильтрация узлов по состояниям безопасности устройств
Фильтрация узлов по категориям устройств
Включение и выключение отображения узлов, связанных с отфильтрованными узлами
Фильтрация соединений
Фильтрация соединений по значениям оценок критичности соединений
Фильтрация соединений по протоколам взаимодействий
Фильтрация соединений по уровням модели OSI
Сброс параметров фильтрации
Сохранение и загрузка параметров отображения карты сетевых взаимодействий
Добавление нового вида с сохранением текущих параметров отображения карты сетевых взаимодействий
Обновление вида с сохранением текущих параметров отображения карты сетевых взаимодействий
Переименование вида карты сетевых взаимодействий
Удаление вида карты сетевых взаимодействий
Применение на карте сетевых взаимодействий параметров, сохраненных в виде

Мониторинг сетевых сеансов
- Таблица сетевых сеансов
- Просмотр сведений о сетевом сеансе
- Скачивание трафика сетевых сеансов
- Поиск по сетевым пакетам
- Преднастроенные правила поиска по сетевым пакетам
- Протоколы, определяемые Kaspersky Anti Targeted Attack Platform

Контроль рисков
- О рисках категории Уязвимость
- Сценарий реализации для процесса непрерывного управления рисками
- Просмотр таблицы рисков
- Просмотр сведений о риске
- Изменение статусов рисков вручную
- Просмотр сведений о рисках при работе с таблицей устройств

Настройка типов событий NDR
- Просмотр таблицы типов событий
- Изменение параметров системного типа события
- Настройка автоматического сохранения трафика для системных типов событий
- Настройка передачи событий через коннекторы
- Общие переменные для подстановки значений в Kaspersky Anti Targeted Attack Platform
- Технологии регистрации событий NDR
- Системные типы событий в Kaspersky Anti Targeted Attack Platform
  - Системные типы событий по технологии Обнаружение вторжений
  - Системные типы событий по технологии Контроль активов
  - Системные типы событий по технологии Внешние системы
  - Системные типы событий по технологии Защита конечных устройств

Настройка типов рисков
- Просмотр таблицы типов рисков
- Изменение базовой оценки для типа риска
- Управление параметрами хранения рисков

Работа с информацией о хостах с компонентом Endpoint Agent
- Просмотр таблицы хостов с компонентом Endpoint Agent
- Настройка отображения таблицы хостов с компонентом Endpoint Agent
- Просмотр информации о хосте
- Фильтрация и поиск хостов с компонентом Endpoint Agent по имени хоста
- Фильтрация и поиск хостов с компонентом Endpoint Agent, изолированных от сети
- Фильтрация и поиск хостов с компонентом Endpoint Agent по именам серверов PCN и SCN
- Фильтрация и поиск хостов с компонентом Endpoint Agent по IP-адресу компьютера
- Фильтрация и поиск хостов с компонентом Endpoint Agent по версии операционной системы на компьютере
- Фильтрация и поиск хостов с компонентом Endpoint Agent по версии компонента
- Фильтрация и поиск хостов с компонентом Endpoint Agent по их активности
- Быстрое создание фильтра хостов с компонентом Endpoint Agent
- Сброс фильтра хостов с компонентом Endpoint Agent
- Удаление хостов с компонентом Endpoint Agent
- Ограничение объема телеметрии от Endpoint Agent

Сетевая изоляция хостов с компонентом Endpoint Agent
Создание правила сетевой изоляции
Добавление исключения из правила сетевой изоляции
Удаление правила сетевой изоляции
Ограничения, действующие при сетевой изоляции
Автоматическая отправка файлов с хостов с компонентом Endpoint Agent на проверку в Sandbox по правилам TAA (IOA) "Лаборатории Касперского"
Включение и отключение автоматической отправки файлов с хостов с компонентом Endpoint Agent на проверку компоненту Sandbox
Выбор операционных систем для проверки объектов в Sandbox
Просмотр таблицы серверов с компонентом Sandbox
Выбор операционных систем для проверки объектов в Sandbox
Работа с задачами
Просмотр таблицы задач
Просмотр информации о задаче
Создание задачи получения файла
Создание задачи сбора форензики
Создание задачи получения ключа реестра
Создание задачи получения метафайлов NTFS
Создание задачи получения дампа памяти процесса
Создание задачи получения образа диска
Конвертация файла из формата RAW в формат EWF
Создание задачи получения дампа оперативной памяти
Создание задачи завершения процесса
Создание задачи проверки хостов с помощью правил YARA
Создание задачи управления службами
Создание задачи выполнения приложения
Создание задачи удаления файла
Создание задачи помещения файла на карантин
Создание задачи восстановления файла из карантина
Создание копии задачи
Удаление задач
Фильтрация задач по времени создания
Фильтрация задач по типу
Фильтрация задач по имени
Фильтрация задач по имени и пути к файлу
Фильтрация задач по описанию
Фильтрация задач по имени сервера
Фильтрация задач по имени пользователя, создавшего задачу
Фильтрация задач по состоянию обработки
Сброс фильтра задач
Работа с политиками (правилами запрета)
Просмотр таблицы правил запрета
Настройка отображения таблицы правил запрета
Просмотр правила запрета
Создание правила запрета
Импорт правил запрета

- Включение и отключение правила запрета
- Включение и отключение предустановок
- Удаление правил запрета
- Фильтрация правил запрета по имени
- Фильтрация правил запрета по типу
- Фильтрация правил запрета по хешу файла
- Фильтрация правил запрета по имени сервера
- Сброс фильтра правил запрета

Работа с пользовательскими правилами

- Об использовании индикаторов компрометации (IOC) и атаки (IOA) для поиска угроз
- Работа с пользовательскими правилами TAA (IOA)
  - Просмотр таблицы правил TAA (IOA)
  - Создание правила TAA (IOA) на основе условий поиска событий
  - Импорт правил TAA (IOA)
  - Просмотр информации о правиле TAA (IOA)
  - Поиск алертов и событий, в которых сработали правила TAA (IOA)
  - Фильтрация и поиск правил TAA (IOA)
  - Сброс фильтра правил TAA (IOA)
  - Включение и отключение использования правил TAA (IOA)
  - Изменение правила TAA (IOA)
  - Удаление правил TAA (IOA)
- Работа с пользовательскими правилами IOC
  - Просмотр таблицы IOC-файлов
  - Просмотр информации об IOC-файле
  - Загрузка IOC-файла
  - Скачивание IOC-файла на компьютер
  - Включение и отключение автоматического использования IOC-файла при проверке хостов
  - Удаление IOC-файла
  - Поиск алертов по результатам IOC-проверки
  - Поиск событий по IOC-файлу
  - Фильтрация и поиск IOC-файлов
  - Сброс фильтра IOC-файлов
  - Настройка расписания IOC-проверки
- Работа с пользовательскими правилами обнаружения вторжений
  - Просмотр таблицы правил обнаружения вторжений
  - Настройка отображения таблицы правил обнаружения вторжений
  - Дополнительные методы обнаружения вторжений
  - Включение и выключение наборов правил обнаружения вторжений
  - Загрузка и замена пользовательских наборов правил обнаружения вторжений
  - Удаление пользовательских наборов правил обнаружения вторжений
- Работа с пользовательскими правилами YARA
  - Просмотр таблицы правил YARA
  - Настройка отображения таблицы правил YARA
  - Импорт правил YARA
  - Просмотр информации о правиле YARA
  - Фильтрация и поиск правил YARA
  - Сброс фильтра правил YARA

Включение и отключение использования правил YARA
Удаление правил YARA
Работа с объектами в Хранилище и на карантине
Просмотр таблицы объектов, помещенных в Хранилище
Просмотр информации об объекте, загруженном в Хранилище через веб-интерфейс
Просмотр информации об объекте, помещенном в Хранилище по задаче получения файла
Просмотр информации об объекте, помещенном в Хранилище по задаче получения данных
Скачивание объектов из Хранилища
Загрузка объектов в Хранилище
Отправка объектов из Хранилища на проверку
Удаление объектов из Хранилища
Фильтрация объектов в Хранилище по типу объекта
Фильтрация объектов в Хранилище по описанию объекта
Фильтрация объектов в Хранилище по результатам проверки
Фильтрация объектов в Хранилище по имени сервера Central Node, PCN или SCN
Фильтрация объектов в Хранилище по источнику объекта
Фильтрация объектов по времени помещения в Хранилище
Сброс фильтра объектов в Хранилище
Просмотр таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent
Просмотр информации об объекте на карантине
Восстановление объекта из карантина
Получение копии объекта на карантине на сервер Kaspersky Anti Targeted Attack Platform
Удаление информации об объекте, помещенном на карантин, из таблицы
Фильтрация информации об объектах, помещенных на карантин, по типу объекта
Фильтрация информации об объектах, помещенных на карантин, по описанию объекта
Фильтрация информации об объектах, помещенных на карантин, по имени хоста
Фильтрация информации об объектах, помещенных на карантин, по времени
Сброс фильтра информации об объектах на карантине
Работа с отчетами
Работа с общими отчетами
Просмотр таблицы шаблонов и отчетов
Создание шаблона
Создание отчета по шаблону
Просмотр отчета
Скачивание отчета на локальный компьютер
Изменение шаблона
Фильтрация шаблонов по имени
Фильтрация шаблонов по имени пользователя, создавшего шаблон
Фильтрация шаблонов по времени создания
Сброс фильтра шаблонов
Удаление шаблона
Фильтрация отчетов по времени создания
Фильтрация отчетов по имени
Фильтрация отчетов по имени сервера с компонентом Central Node
Фильтрация отчетов по имени пользователя, создавшего отчет
Сброс фильтра отчетов
Удаление отчета

- Работа с отчетами NDR
  - Просмотр таблицы шаблонов отчетов NDR
  - Просмотр сведений о шаблоне отчета NDR
  - Просмотр таблицы отчетов NDR
  - Формирование отчета NDR по шаблону вручную
  - Дублирование шаблона отчета NDR
  - Изменение шаблона отчета NDR
  - Экспорт отчета NDR в файл
  - Удаление шаблона отчета NDR
  - Удаление отчета NDR
  - Отмена формирования отчета NDR
  - Управление параметрами хранения файлов отчетов
- Работа с правилами присвоения алертам статуса VIP
  - Просмотр таблицы правил присвоения статуса VIP
  - Создание правила присвоения статуса VIP
  - Удаление правила присвоения статуса VIP
  - Изменение правила присвоения статуса VIP
  - Импорт списка правил присвоения статуса VIP
  - Экспорт списка данных, исключенных из проверки
  - Фильтрация и поиск по типу правила присвоения статуса VIP
  - Фильтрация и поиск по значению правила присвоения статуса VIP
  - Фильтрация и поиск по описанию правила присвоения статуса VIP
  - Сброс фильтра правил присвоения статуса VIP
- Работа с разрешающими правилами для событий NDR
  - Просмотр таблицы разрешающих правил
  - Создание разрешающего правила с изначально пустыми значениями или со значениями из шаблона
  - Создание разрешающего правила на основе зарегистрированного события
  - Копирование разрешающего правила
  - Изменение параметров разрешающего правила
  - Включение и выключение разрешающих правил
  - Удаление разрешающих правил
- Работа со списком исключений из проверки
  - Просмотр таблицы данных, исключенных из проверки
  - Добавление правила исключения из проверки
  - Удаление правила исключения из проверки
  - Изменение правила, добавленного в исключения из проверки
  - Экспорт списка данных, исключенных из проверки
  - Фильтрация правил в списке исключений из проверки по критерию
  - Поиск правил в списке исключений из проверки по значению
  - Сброс фильтра правил в списке исключений из проверки
- Работа с исключениями из правил обнаружения вторжений
  - Просмотр таблицы правил обнаружения вторжений, добавленных в исключения
  - Добавление правила обнаружения вторжений в исключения
  - Редактирование описания правила обнаружения вторжений, добавленного в исключения
  - Удаление правил обнаружения вторжений из исключений

Работа с TAA-исключениями
Просмотр таблицы правил TAA (IOA), добавленных в исключения
Добавление правила TAA (IOA) в исключения
Просмотр правила TAA (IOA), добавленного в исключения
Удаление правил TAA (IOA) из исключений
Работа с ICAP-исключениями
Просмотр таблицы ICAP-исключений
Добавление правила в ICAP-исключения
Удаление правил из ICAP-исключений
Изменение и выключение правила в списке ICAP-исключений
Фильтрация правил в списке ICAP-исключений по критерию
Фильтрация правил в списке ICAP-исключений по значению
Фильтрация правил в списке ICAP-исключений по состоянию
Сброс условий фильтрации правил в списке ICAP-исключений
Работа с зеркалированным трафиком со SPAN-портов
Создание списка паролей для архивов
Работа с информацией о серверах с компонентами Central Node и Sensor
Просмотр параметров сервера
Просмотр таблицы серверов с компонентом Sandbox
Просмотр параметров набора операционных систем для проверки объектов в Sandbox
Просмотр таблицы внешних систем
Работа с пользовательскими правилами Sandbox
Просмотр таблицы пользовательских правил Sandbox
Настройка отображения таблицы правил Sandbox
Фильтрация и поиск правил Sandbox
Сброс фильтра правил Sandbox
Просмотр информации о пользовательском правиле Sandbox
Создание пользовательского правила Sandbox для проверки файлов
Создание пользовательского правила Sandbox для проверки URL-адреса
Копирование пользовательского правила Sandbox
Импорт пользовательских правил Sandbox для проверки файлов
Изменение пользовательского правила Sandbox
Включение и отключение пользовательских правил Sandbox
Экспорт пользовательских правил Sandbox для проверки файлов
Удаление пользовательских правил Sandbox
Список расширений для категорий файлов
Подготовка данных для передачи в систему ГосСОПКА
Запуск утилиты для подготовки данных к передаче в систему ГосСОПКА
Отправка уведомлений
Просмотр таблицы правил для отправки уведомлений
Создание правила для отправки уведомлений об обнаружениях
Создание правила для отправки уведомлений о работе компонентов приложения
Включение и отключение правила для отправки уведомлений
Изменение правила для отправки уведомлений
Удаление правила для отправки уведомлений
Фильтрация и поиск правил отправки уведомлений по типу правила
Фильтрация и поиск правил отправки уведомлений по теме уведомлений

Фильтрация и поиск правил отправки уведомлений по адресу электронной почты
Фильтрация и поиск правил отправки уведомлений по их состоянию
Сброс фильтра правил отправки уведомлений
Управление журналами
Управление журналом активности пользователей приложения
Включение и отключение записи информации в журнал активности
Скачивание файла журнала активности
Записи в журнале активности пользователей приложения
Управление журналом активности пользователей NDR
Управление параметрами хранения журналов
Включение и выключение аудита действий пользователей
Просмотр записей аудита действий пользователей
Настройка максимального объема хранения журналов трассировки
Настройка максимального объема хранения журналов статистики
Журнал активности пользователей Sensor
Записи о действиях пользователей в меню администратора компонента Sensor
Журналы Sandbox
Скачивание системного журнала Sandbox
Скачивание журнала активности пользователей Sandbox
Записи в журнале активности пользователей Sandbox
Скачивание журналов Kaspersky Anti Targeted Attack Platform
Просмотр сообщений приложения
Настройка срока хранения системных журналов и обнаружений Kaspersky Anti Targeted Attack Platform
Просмотр информации о файлах, поступавших на проверку в Kaspersky Anti Targeted Attack Platform
Управление приложением Kaspersky Endpoint Security для Windows
Управление приложением Kaspersky Endpoint Security для Linux
Управление приложением Kaspersky Endpoint Security для Mac
Резервное копирование и восстановление данных
Резервное копирование и восстановление данных сервера Central Node
Резервное копирование и восстановление данных сервера Central Node в виде кластера
Резервное копирование и восстановление данных сервера Central Node в режиме распределенного решения и мультитенантности
Состав экспортируемых данных
Ограничения, действующие во время создания резервной копии
Восстановление работы встроенного Sensor после восстановления приложения из резервной копии
Обновление Kaspersky Anti Targeted Attack Platform
Обновление Central Node, установленного на сервере
Очистка диска сервера Central Node
Обновление Central Node, установленного в виде кластера
Обновление Central Node с версии 7.1 до версии 7.1.1 или 7.1.2
Обновление Central Node с версии 7.1.1 или 7.1.2 до версии 7.1.3
Обновление Central Node с версии 7.1.3 до версии 7.1.7
Обновление Sensor, установленного на отдельном сервере
Восстановление данных на внешнем хранилище, подключенном к компоненту Sensor
Состав и объем данных, сохраняемых при обновлении приложения Kaspersky Anti Targeted Attack Platform

Управление компонентами приложения через меню администратора
Меню администратора Central Node
Меню администратора Sensor
Меню администратора Sandbox
Использование KATA и KEDR API
Интеграция внешней системы с Kaspersky Anti Targeted Attack Platform
API для проверки объектов внешних систем
Запрос на проверку объектов
Запрос на получение результатов проверки
Запрос на удаление результатов проверки
Запрос на вывод ограничений приложения на проверку объектов
API для получения внешними системами информации об алертах
Запрос на вывод информации об алертах
Состав передаваемых данных
Данные об обнаруженных объектах
Данные о найденных угрозах
Данные об окружении обнаруженных объектов
API для получения внешними системами информации о событиях приложения
Запрос на вывод информации о событиях
Язык запросов для фильтрации событий
Поля для фильтрации событий
API для управления действиями по реагированию на угрозы
Запрос на получение списка хостов с компонентом Endpoint Agent
Запрос на получение информации о сетевой изоляции и наличии правил запрета для хостов с компонентом Endpoint Agent
Управление сетевой изоляцией хостов
Запрос на включение сетевой изоляции
Запрос на отключение сетевой изоляции
Запрос на добавление исключения в правило сетевой изоляции
Управление правилами запрета
Запрос на создание правила запрета
Запрос на удаление правила запрета
Управление задачей запуска приложения
Запрос на получение информации о задаче
Запрос на создание задачи
Запрос на удаление задачи
Использование NDR API
Обеспечение безопасного взаимодействия при использовании Kaspersky Anti Targeted Attack Platform API
Создание и использование коннекторов для Kaspersky Anti Targeted Attack Platform API
Источники информации о приложении
Обращение в Службу технической поддержки
Способы получения технической поддержки
Техническая поддержка через Kaspersky CompanyAccount
Глоссарий
Advanced persistent threat (APT)
Anti-Malware Engine
Backdoor-программа

Central Node

CSRF-атака

End User License Agreement

ICAP-данные

ICAP-клиент

Intrusion Detection System

IOA

IOC

IOC-файл

Kaspersky Anti Targeted Attack Platform

Kaspersky Private Security Network

Kaspersky Secure Mail Gateway

Kaspersky Security Network (KSN)

Kaspersky Threat Intelligence Portal

KATA

KEDR

Kerberos-аутентификация

Keytab-файл

MIB (Management Information Base)

MITM-атака

NTP-сервер

OpenIOC

Sandbox

Sensor

SIEM-система

SPAN

Syslog

Targeted Attack Analyzer

TLS-шифрование

YARA

Алерт

Альтернативный поток данных

Атака "нулевого дня"

Вредоносные веб-адреса

Дамп

Зеркалированный трафик

Имя субъекта-службы (SPN)

Компонент Endpoint Agent

Локальная репутационная база KPSN

Мультитенантность

Обнаружение

Правила YARA

Правило TAA (IOA)

Пропускная способность канала связи

Распределенное решение

Сигнатура

Статус VIP

- Тенант
- Техника MITRE
- Трассировка
- Угрозы нового поколения
- Уязвимость "нулевого дня"
- Фишинговые URL-адреса
- Целевая атака

Информация о стороннем коде

Уведомления о товарных знаках

Справка Kaspersky Anti Targeted Attack Platform

Новые функции

- Что нового в Kaspersky Anti Targeted Attack Platform

Аппаратные и программные требования

- Аппаратные и программные требования
- Совместимость Kaspersky Anti Targeted Attack Platform с Kaspersky Endpoint Security для Windows, Linux и Mac

Лицензирование

- Лицензирование Kaspersky Anti Targeted Attack Platform

Начало работы

- Распределенное решение и мультитенантность
- Масштабирование Kaspersky Anti Targeted Attack Platform
- Установка и первоначальная настройка Kaspersky Anti Targeted Attack Platform
- Настройка интеграции Kaspersky Anti Targeted Attack Platform с компонентом Endpoint Agent

Работа в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

- Работа в веб-интерфейсе приложения – Администратору
- Работа в веб-интерфейсе приложения – Сотруднику службы безопасности

Дополнительные возможности

- Работа с компонентом Sandbox через веб-интерфейс
- Взаимодействие с внешними системами по API

Обновление

- Обновление предыдущей версии Kaspersky Anti Targeted Attack Platform

Обращение в Службу технической поддержки

- Способы получения технической поддержки

О Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform – решение (далее также "приложение"), предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как *атаки "нулевого дня"*, *целевые атаки* и сложные целевые атаки *advanced persistent threats* (далее также "*APT*").
Решение разработано для корпоративных пользователей.

Решение Kaspersky Anti Targeted Attack Platform включает в себя три функциональных блока:

- Kaspersky Anti Targeted Attack (далее также "KATA"), обеспечивающий защиту периметра IT-инфраструктуры предприятия.
- Kaspersky Endpoint Detection and Response (далее также "KEDR"), обеспечивающий защиту компьютеров локальной сети организации.
- Network Detection and Response (далее также "NDR"), обеспечивающий защиту внутренней сети предприятия.

Решение может получать и обрабатывать данные следующими способами:

- Интегрироваться в локальную сеть, получать и обрабатывать *зеркалированный SPAN-, ERSPAN- и RSPAN-трафик* и извлекать объекты и метаинформацию HTTP-, HTTP2, FTP-, SMTP- и DNS-, SMB- и NFS-протоколов.
- Подключаться к прокси-серверу по протоколу ICAP, получать и обрабатывать данные HTTP-, HTTP2- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на прокси-сервере.
- Подключаться к почтовому серверу по протоколам POP3(S) и SMTP, получать и обрабатывать копии сообщений электронной почты.
- Интегрироваться с приложениями "Лаборатории Касперского" Kaspersky Secure Mail Gateway и Kaspersky Security для Linux Mail Server, получать и обрабатывать копии сообщений электронной почты.
- Принимать и обрабатывать копии сетевого трафика, которые отправляются с удаленного объекта с помощью приложения "Лаборатории Касперского" Kaspersky SD-WAN. Эта функциональность обеспечивает расширенную гибкость в обнаружении и контроле сетевой активности, позволяя анализировать трафик из различных точек сети и принимать соответствующие меры по обеспечению безопасности сети.

  Вы можете получить подробную информацию о Kaspersky Secure Mail Gateway, Kaspersky Security для Linux Mail Server и Kaspersky SD-WAN из документации к этим приложениям.
- Интегрироваться с приложением Kaspersky Endpoint Security и получать данные (*события*) с отдельных компьютеров, входящих в IT-инфраструктуру организации и работающих под управлением операционных систем Microsoft® Windows®, Linux® и Mac®. Приложения осуществляют постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.
- Интегрироваться с внешними системами с помощью интерфейса REST API и проверять файлы на этих системах.

Решение использует следующие средства анализа угроз (Threat Intelligence):

- Инфраструктуру облачных служб Kaspersky Security Network (далее также "KSN"), предоставляющую доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

- Интеграцию с приложением "Лаборатории Касперского" Kaspersky Private Security Network (далее также "KPSN"), предоставляющую пользователю возможность получать доступ к репутационным базам KSN, а также другим статистическим данным, не отправляя данные в KSN со своих компьютеров.

- Интеграцию с информационной системой "Лаборатории Касперского" Kaspersky Threat Intelligence Portal, которая содержит и отображает информацию о репутации файлов и URL-адресов.

- Индикаторы IOC (Indicator of Compromise, или индикатор компрометации). Kaspersky Anti Targeted Attack Platform использует IOC-файлы открытого стандарта описания индикаторов компрометации OpenIOC. IOC-файлы содержат набор индикаторов, при совпадении с которыми приложение считает событие алертом.

- Индикаторы IOA (Indicator of Attack, или индикатор атаки). Kaspersky Anti Targeted Attack Platform проверяет базу событий приложения и отмечает события или цепочки событий, которые совпадают с поведением, описанным в правилах TAA (IOA).

Решение может обнаружить следующие события, происходящие внутри IT-инфраструктуры организации:

- На компьютер локальной сети организации был загружен файл или была предпринята попытка загрузки файла.

- На адрес электронной почты пользователя локальной сети организации был отправлен файл.

- На компьютере локальной сети организации была открыта ссылка на веб-сайт.

- IP-адрес или доменное имя компьютера локальной сети организации были замечены в сетевой активности.

- На компьютере локальной сети организации были запущены процессы.

Приложение может предоставлять пользователю результаты своей работы и анализа угроз следующими способами:

- Отображать результаты работы в веб-интерфейсе серверов Central Node, Primary Central Node (далее также PCN) или Secondary Central Node (далее также SCN).

- Публиковать алерты в SIEM-систему, которая уже используется в вашей организации, по протоколу Syslog.

- Интегрироваться с внешними системами с помощью интерфейса REST API и по запросу отправлять данные об алертах и событиях решения во внешние системы.

- Публиковать информацию об алертах компонента Sandbox в локальную репутационную базу Kaspersky Private Security Network.

Пользователи с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут выполнять следующие действия в приложении:

- Осуществлять мониторинг работы компонентов решения.
- Просматривать таблицу обнаруженных признаков целевых атак и вторжений в IT-инфраструктуру организации, осуществлять фильтрацию и поиск алертов, просмотр и работу с каждым алертом, выполнять рекомендации по оценке и расследованию инцидентов.
- Просматривать таблицу событий, происходящих на компьютерах и серверах, входящих в IT-инфраструктуру организации, осуществлять поиск угроз, фильтрацию, просмотр и работу с каждым событием, выполнять рекомендации по оценке и расследованию инцидентов.
- Выполнять задачи на компьютерах с Kaspersky Endpoint Security: запускать приложения и останавливать процессы, скачивать и удалять файлы, помещать объекты на карантин на компьютерах с приложением Kaspersky Endpoint Security, копии файлов в Хранилище Kaspersky Anti Targeted Attack Platform, а также восстанавливать файлы из карантина.
- Настраивать политики запрета запуска файлов и процессов, которые они считают небезопасными, на выбранных компьютерах с приложением Kaspersky Endpoint Security.
- Изолировать отдельные компьютеры с приложением Kaspersky Endpoint Security от сети.
- Работать с правилами TAA (IOA) для классификации и анализа событий.
- Работать с пользовательскими правилами Targeted Attack Analyzer TAA (IOA), YARA, Sandbox и правилами обнаружения вторжений: загружать правила, по которым приложение будет проверять события и создавать алерты.
- Работать с файлами открытого стандарта описания индикаторов компрометации OpenIOC (IOC-файлы) для поиска признаков целевых атак, зараженных и возможно зараженных объектов на хостах с компонентом Endpoint Agent и в базе алертов.
- Добавлять правила TAA (IOA) и правила IDS, предоставленные специалистами "Лаборатории Касперского", в исключения из проверки.
- Работать с объектами на карантине и копиями объектов в Хранилище.
- Управлять отчетами о работе приложения и отчетами об алертах.
- Настраивать отправку уведомлений об алертах и о проблемах в работе приложения на адреса электронной почты пользователей.
- Работать со списком алертов со статусом VIP, со списком данных, исключенных из проверки, наполнять локальную репутационную базу KPSN.
- Сохранять и выгружать копии сырого сетевого трафика для анализа во внешних системах.

Пользователи с ролью **Аудитор** могут выполнять следующие действия в приложении:

- Осуществлять мониторинг работы компонентов решения.
- Просматривать таблицу обнаруженных признаков целевых атак и вторжений в IT-инфраструктуру организации, осуществлять фильтрацию и поиск алертов, просматривать данные каждого алерта.

- Просматривать таблицу событий, происходящих на компьютерах и серверах, входящих в IT-инфраструктуру организации, осуществлять поиск угроз, фильтрацию, просмотр каждого события.
- Просматривать список хостов с компонентом Endpoint Agent и информацию о выбранных хостах.
- Просматривать пользовательские правила Targeted Attack Analyzer TAA (IOA), YARA, Sandbox и правила обнаружения вторжений.
- Просматривать исключенные из проверки правила TAA (IOA) и правила IDS, предоставленные специалистами "Лаборатории Касперского".
- Просматривать отчеты о работе приложения и отчеты об алертах.
- Просматривать список алертов со статусом VIP, список данных, исключенных из проверки.
- Просматривать все настройки, производимые в веб-интерфейсе приложения.
- Сохранять и выгружать копии сырого сетевого трафика для анализа во внешних системах.

Пользователи с ролью **Администратор** могут выполнять следующие действия в приложении:

- Настраивать параметры работы приложения.
- Настраивать серверы для работы в режиме распределенного решения и мультитенантности.
- Производить интеграцию приложения с другими приложениями и системами.
- Работать с TLS-сертификатами и настраивать доверенное соединение сервера Central Node с сервером Sandbox, а также серверов Kaspersky Anti Targeted Attack Platform с компонентом Endpoint Agent и с внешними системами.
- Управлять учетными записями пользователей приложения.
- Осуществлять мониторинг работоспособности приложения.

Что нового

В Kaspersky Anti Targeted Attack Platform 7.1.7 появились следующие изменения:

1. Исправлена ошибка, возникавшая при извлечении из трафика объектов, переданных по протоколу HTTP/2.
2. Исправлены ошибки, возникавшие при интеграции с KPSN версии 4.0.
3. Исправлена ошибка, возникавшая при отображении данных в разделе **Поиск угроз** за выбранный период.
4. Исправлена ошибка отображения данных, возникавшая при поиске всех событий, связанных с алертом, из карточки алерта.
5. Улучшена работа ICAP-интеграции: исправлены ошибки и повышена стабильность.

В Kaspersky Anti Targeted Attack Platform 7.1.3 появились следующие изменения:

1. Исправлены ошибки, возникавшие при обновлении Kaspersky Anti Targeted Attack Platform.
2. Исправлены ошибки, возникавшие при резервном копировании и восстановлении данных.
3. Исправлена ошибка, возникавшая при отображении данных в разделе **Поиск угроз**.
4. Исправлена ошибка, возникавшая при отправке уведомлений об алертах типа AA (Aggregated Alerts).

В Kaspersky Anti Targeted Attack Platform 7.1.1 и 7.1.2 появились следующие изменения:

1. Исправлены уязвимости операционной системы.
2. Исправлены ошибки, возникавшие при обновлении Kaspersky Anti Targeted Attack Platform.
3. Исправлена ошибка регистрации событий в трафике сети и соответствующих им алертов.
4. Если в результате проверки электронного письма с несколькими URL-адресами создается алерт, в нем отображается информация по каждому URL-адресу.
5. Исправлена ошибка, возникающая при выгрузке данных для системы ГосСОПКА.

В Kaspersky Anti Targeted Attack Platform 7.1 появились следующие изменения:

1. Улучшена производительность Kaspersky Anti Targeted Attack Platform.
2. Улучшена проверка ICAP-трафика в режиме реального времени:
   - Увеличена скорость обработки запросов.
   - Улучшен сбор статистики.
   - Оптимизировано взаимодействие с сетью Kaspersky Security Network (KSN).
   - Добавлена проверка файлов в POST-запросах (REQMOD).
   - Добавлена дедупликация запросов на проверку объектов.
   - В стандартной проверке ICAP-трафика в режиме реального времени произошли следующие изменения:
     - Во время проверки файла скорость его загрузки снижается. Если по истечении указанного времени файл не удастся проверить, загрузка продолжается с обычной скоростью.

       В связи с реализацией этого функционала в веб-интерфейсе приложения упразднена возможность настроить страницы уведомлений **Проверка файла** и **Истек срок хранения файла**.
     - Мультимедийные файлы исключаются из проверки.
   - В усиленной проверке ICAP-трафика в режиме реального времени произошли следующие изменения:
     - Для оптимизации нагрузки приложение может временно переключаться из режима усиленной проверки ICAP-трафика в режим стандартной проверки. При этом в разделе **Мониторинг** веб-интерфейса приложения отображается предупреждение о переходе в режим стандартной проверки.

3. Улучшен интерфейс для работы с пользовательскими правилами обнаружения вторжений.

4. Поддержана возможность использовать систему Storage Area Network (SAN) в качестве диска для хранения данных компонента Central Node, установленного на сервере.

5. Поддержано получение зеркалированного трафика с использованием технологии ERSPAN (Encapsulated Remote SPAN) – для этого сервер с компонентом Central Node или Sensor должен выступать в роли конечной точки назначения для создаваемых туннелей по протоколу GRE (Generic Routing Encapsulation).

   Для передачи ERSPAN-трафика между компонентами вам требуется нужно настроить параметры MTU в iptables таким образом, чтобы размер MTU составлял 1900.

6. Добавлен новый тип события – **USB-устройство**.

7. Добавлена возможность выбрать период **Последние 7 дней** при поиске событий в разделе **Поиск угроз**.

8. Реализованы новые возможности по управлению политиками аутентификации:

   - Отслеживание неудачных попыток аутентификации в веб-интерфейсе или консоли управления компонентов Central Node и Sandbox.

   - Завершение неактивных пользовательских сессий в веб-интерфейсе или консоли управления компонентов Central Node, Sensor и Sandbox по истечении заданного периода.

9. Реализована возможность при добавлении правила обнаружения вторжений от "Лаборатории Касперского" в исключение указать условия его применения. Например, чтобы применять исключения только для выбранных узлов сети.

10. Реализована выгрузка информации об алертах и событиях в трафике сети (событиях NDR) в систему ГосСОПКА.

11. Расширен функционал журналов приложения:

    - Для компонента Sandbox реализованы журналы активности, в которые записывается информация о действиях пользователей в веб-интерфейсе и меню администратора компонента.

    - Для компонента Sensor реализован журнал активности, в который записывается информация о действиях пользователей в меню администратора компонента.

    - Расширен состав событий, которые записываются в журнал активности пользователей приложения.

    - Добавлена возможность настроить срок хранения журналов и данных обнаружений в базе данных компонента Central Node, а также срок хранения журналов компонентов Sensor и Sandbox.

12. Добавлена возможность ограничить объем телеметрии от компонента Endpoint Agent (при интеграции с функциональным блоком KEDR).

13. В веб-интерфейсе приложения произошли следующие изменения:

    - Добавлен новый язык локализации приложения – традиционный китайский.

    - Задача **Выполнить приложение** переименована на **Запустить программу**.

14. Упразднен доступ к веб-интерфейсу компонента Sensor.

Изменения в Kaspersky Endpoint Security 12.9 для Windows

Вы можете посмотреть список изменений в Kaspersky Endpoint Security 12.9 для Windows в справке Kaspersky Endpoint Security для Windows.

Изменения в Kaspersky Endpoint Security 12.2 для Linux

Вы можете посмотреть список изменений в Kaspersky Endpoint Security 12.2 для Linux в справке Kaspersky Endpoint Security для Linux.

Изменения в Kaspersky Endpoint Security 12.1 для Mac

Вы можете посмотреть список изменений в Kaspersky Endpoint Security 12.1 для Mac в справке Kaspersky Endpoint Security для Mac.

Исправленные проблемы

Таблица ниже содержит информацию о проблемах, обнаруженных в текущей версии Kaspersky Anti Targeted Attack Platform и исправленных обновлениями.

Дата выпуска обновления	Номер версии обновления	Версия приложения, в которой проблема появилась впервые	Описание проблемы				
7.04.2026	7.1.7	7.1.3	[9403837] Исправлена проблема, при которой недоступна кнопка **Сохранить** в параметрах соединения с прокси-сервером, если в поле **Сервер** введен IP-адрес с одной цифрой в последнем октете.				
		7.1.1	[9047903] Исправлена проблема, при которой в веб-интерфейсе Kaspersky Secure Mail Gateway вместо результатов проверки объекта в Kaspersky Anti Targeted Attack Platform отображается ошибка. [9458080] Добавлена проверка IP-адреса PCN в параметрах подключения SCN к PCN. [9159104] Исправлена проблема, из-за которой при поиске событий из карточки алерта в результатах отображаются не все связанные события. [9109119] Исправлена ошибка *Ошибки обработки файлов компонентом Sensor*, которая отображается в разделе **Мониторинг** при обработке файлов, полученных по протоколу HTTP2.	7.1	[8971563] Исправлена проблема, при которой события, созданные за указанный период, не отображаются в результатах поиска с фильтрацией по дате. [9169778] Исправлено появление ошибки *Проверка SPAN-трафика по технологии IDS работает некорректно* в разделе **Мониторинг** при включении приема зеркалированного SPAN-трафика на Central Node со встроенным Sensor (Embedded Sensor).		
						7.0	[8705844] Исправлена проблема исключения из проверки по таймауту сообщений электронной почты, которые поступили от Kaspersky Secure Mail Gateway и содержат в теле письма URL-адрес.

Использование Kaspersky Threat Intelligence Portal

Для получения дополнительной информации о файлах, которые вы считаете подозрительными, вы можете перейти на веб-сайт приложения "Лаборатории Касперского" Kaspersky Threat Intelligence Portal, которое анализирует каждый файл на наличие вредоносного кода и отображает информацию о репутации этого файла.

Доступ к приложению Kaspersky Threat Intelligence предоставляется на коммерческой основе. Для авторизации на веб-сайте приложения на вашем компьютере в хранилище сертификатов должен быть установлен сертификат доступа к приложению. Кроме того, у вас должны быть имя пользователя и пароль доступа к приложению.

Подробнее о приложении Kaspersky Threat Intelligence Portal см. веб-сайт "Лаборатории Касперского".

Комплект поставки

В комплект поставки Kaspersky Anti Targeted Attack Platform входят следующие файлы:

- Образ диска (файл с расширением iso) с установочными файлами операционной системы Ubuntu Server 22.04 и компонентов Sensor, Central Node, Sandbox.
- Архив с расширением .tar.gz компонентов Sensor, Central Node для создания iso-образа на базе операционной системы Astra Linux Special Edition 1.8.1.
- Архив с расширением tar.gz компонента Sandbox для создания iso-образа на базе операционной системы Astra Linux Special Edition 1.8.1.
- Образы дисков (файлы с расширением iso) операционных систем, в которых компонент Sandbox будет запускать файлы.
- Утилита (файл с расширением tar) для создания iso-образа на базе операционной системы Astra Linux Special Edition 1.8.1.
- Утилита для подготовки данных к передаче в систему ГосСОПКА (gossopka_alert_exporter.tar.gz).
- Пакет с обновлением для компонентов Central Node и Sensor на базе операционной системы Ubuntu.
- Пакет с обновлением для компонентов Central Node и Sensor на базе операционной системы Astra Linux .
- Файл с информацией о стороннем коде, используемом в Kaspersky Anti Targeted Attack Platform.

Аппаратные и программные требования

Программные требования к виртуальным платформам для установки Kaspersky Anti Targeted Attack Platform

Вы можете развернуть компоненты приложения на следующих виртуальных платформах:

- Central Node и Sensor:
  - VMware ESXi™ 6.7.0 или 7.0.
  - KVM.
  - ПК СВ "Брест" 3.3.
  - "РЕД Виртуализация" 7.3.
  - zVirt Node 4.2.
  - Nutanix Acropolis Operating System (Nutanix AOS) версии 7.3.1.2 и гипервизор Acropolis Hypervisor (AHV) версии 10.3.1.2.
- Sandbox:
  - VMware ESXi™ 6.7.0 или 7.0.
  - ПК СВ "Брест" 3.3.
  - "РЕД Виртуализация" 7.3.
  - zVirt Node 4.2.

Для развертывания приложения на виртуальной платформе VMware ESXI необходимо установить для гипервизора актуальный пакет обновления.

Если вы хотите развернуть приложение на базе операционной системы Astra Linux в гипервизоре VMware ESXI, вам требуется обеспечить совместимость используемого вами серверного оборудования с операционной системой Astra Linux. Полный список поддерживаемого серверного оборудования см. на сайте разработчика ОС Astra Linux.

Аппаратные требования к компонентам Central Node, Sensor и Sandbox приведены в Руководстве по масштабированию.

При развертывании приложения на виртуальных платформах могут действовать ограничения. Мы рекомендуем ознакомиться с ними перед установкой приложения.

Аппаратные и программные требования к компьютерам для установки компонента Endpoint Agent

Аппаратные и программные требования к компоненту Endpoint Agent соответствуют аппаратным и программным требованиям к компьютерам для приложений, которые выступают в роли компонента Endpoint Agent, и отражены в документации этих приложений:

- Kaspersky Endpoint Security для Windows.
- Kaspersky Endpoint Security для Linux.
- Kaspersky Endpoint Security для Mac.

Начиная с этой версии Kaspersky Anti Targeted Attack Platform больше не поддерживает интеграцию с приложением Kaspersky Endpoint Agent.

Если при работе с предыдущими версиями приложения вы использовали Kaspersky Endpoint Agent, вам требуется заменить это приложение на Kaspersky Endpoint Security для Windows. Вы можете использовать Kaspersky Endpoint Security для Windows в следующих режимах:

- EDR-агент.

  Этот режим рекомендуется, если ранее вы использовали Kaspersky Endpoint Agent без интеграции с EPP-приложениями.

- Легкий агент.

  Этот режим рекомендуется, если ранее вы использовали интеграцию Kaspersky Endpoint Agent с Kaspersky Security для виртуальных сред Легкий агент.

Подробнее о режимах работы приложения Kaspersky Endpoint Security для Windows вы можете посмотреть в разделе *Режимы работы приложения: Стандартный, EDR-агент, Легкий агент* онлайн-справки приложения Kaspersky Endpoint Security для Windows.

Аппаратные и программные требования к компьютерам для работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Для настройки и работы с приложением через веб-интерфейс на компьютерах должен быть установлен один из следующих браузеров:

- Mozilla™ Firefox™ для Linux.
- Mozilla Firefox для Windows.
- Google™ Chrome™ для Windows.
- Google Chrome для Linux.

- Edge (Windows).
- Safari (Mac).

Минимально возможное разрешение экрана для работы в веб-интерфейсе: 1366x768 пикселей.

Программные требования к прокси-серверу при настройке интеграции по протоколу ICAP

При настройке интеграции с прокси-сервером по протоколу ICAP мы рекомендуем в качестве прокси-сервера использовать следующие приложения:

- Ideco NGFW версии 14 (сборка 14.13.4).
- Squid версии 5.9.
- User Gate.

Совместимость версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать Kaspersky Endpoint Security в качестве компонента Endpoint Agent.

Информация о совместимости версий Kaspersky Endpoint Security с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Совместимость версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform

Версия Kaspersky Endpoint Security	Совместимость с KATA 4.0	Совместимость с KATA 4.1	Совместимость с KATA 5.0	Совместимость с KATA 5.1	Совместимость с KATA 6.0	Совместимость с KATA 6.1	Совместимость с KATA 7.0
Kaspersky Endpoint Security 12.1, 12.2	Нет	Да	Да	Да	Да	Нет	Есть ограничения
Kaspersky Endpoint Security 12.3, 12.4	Нет	Да	Да	Да	Да	Да	Есть ограничения
Kaspersky Endpoint Security 12.5, 12.6	Нет	Нет	Да	Да	Да	Да	Есть ограничения
Kaspersky Endpoint Security 12.7	Нет	Нет	Есть ограничения	Есть ограничения	Есть ограничения	Есть ограничения	Да
Kaspersky Endpoint Security 12.8, 12.9	Нет	Нет	Есть ограничения	Есть ограничения	Есть ограничения	Есть ограничения	Есть ограничения
Kaspersky Endpoint Security 12.10, 12.11	Нет	Нет	Да	Да	Да	Да	Да

Подробнее об ограничениях совместимости версий Kaspersky Endpoint Security с версиями Kaspersky Anti Targeted Attack Platform см. в разделе *Ограничения совместимости с Kaspersky Endpoint Security для Windows*.

Kaspersky Endpoint Security для Windows с версии 12.8 может использоваться в качестве компонента Легкий агент для Windows для приложения Kaspersky Security для виртуальных сред. Подробнее об интеграции см. в справке Kaspersky Security для виртуальных сред Легкий агент.

Совместимость версий Kaspersky Endpoint Security для Linux с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать Kaspersky Endpoint Security в качестве компонента Endpoint Agent.

Информация о совместимости версий Kaspersky Endpoint Security с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Совместимость версий Kaspersky Endpoint Security для Linux с версиями Kaspersky Anti Targeted Attack Platform

Версия Kaspersky Endpoint Security	Совместимость с KATA 4.0	Совместимость с KATA 4.1	Совместимость с KATA 5.0	Совместимость с KATA 5.1	Совместимость с KATA 6.0	Совместимость с KATA 6.1	Совместимость с KATA 7.0
Kaspersky Endpoint Security 11.4	Нет	Нет	Нет	Есть ограничения	Есть ограничения	Есть ограничения	Есть ограничения
Kaspersky Endpoint Security 12	Нет	Нет	Есть ограничения	Есть ограничения	Есть ограничения	Есть ограничения	Есть ограничения
Kaspersky Endpoint Security 12.1	Нет	Нет	Нет	Есть ограничения	Есть ограничения	Есть ограничения	Есть ограничения
Kaspersky Endpoint Security 12.2, 12.3	Нет	Нет	Нет	Нет	Есть ограничения	Есть ограничения	Есть ограничения

Подробнее об ограничениях совместимости версий Kaspersky Endpoint Security с версиями Kaspersky Anti Targeted Attack Platform см. в разделе *Ограничения совместимости с Kaspersky Endpoint Security для Linux*.

Kaspersky Endpoint Security для Linux с версии 12 может использоваться в качестве компонента Легкий агент для Linux для приложения Kaspersky Security для виртуальных сред. При использовании приложения Kaspersky Endpoint Security для Linux в качестве компонента Легкий агент для Linux интеграция Kaspersky Endpoint Security для Linux и Kaspersky Anti Targeted Attack Platform сохраняется.

Подробнее об интеграции см. в справке Kaspersky Security для виртуальных сред Легкий агент.

Совместимость Kaspersky Endpoint Security для Mac с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать Kaspersky Endpoint Security для Mac в качестве компонента Endpoint Agent.

Информация о совместимости версий Kaspersky Endpoint Security для Mac с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Совместимость версий Kaspersky Endpoint Security для Mac с версиями Kaspersky Anti Targeted Attack Platform

Версия Kaspersky Endpoint Security	Совместимость с KATA 4.0	Совместимость с KATA 4.1	Совместимость с KATA 5.0	Совместимость с KATA 5.1	Совместимость с KATA 6.0	Совместимость с KATA 6.1	Совместимость с KATA 7.0
Kaspersky Endpoint Security 12, 12.1, 12.2	Нет	Нет	Нет	Нет	Есть ограничения	Есть ограничения	Есть ограничения

Подробнее об ограничениях совместимости версий Kaspersky Endpoint Security с версиями Kaspersky Anti Targeted Attack Platform см. в разделе *Ограничения совместимости с Kaspersky Endpoint Security для Mac*.

Совместимость версий KUMA с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать KUMA в качестве SIEM-системы.

Информация о совместимости версий KUMA с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Совместимость версий KUMA с версиями Kaspersky Anti Targeted Attack Platform

Версия KUMA	Совместимость с KATA 4.1	Совместимость с KATA 5.0	Совместимость с KATA 5.1	Совместимость с KATA 6.0	Совместимость с KATA 6.1	Совместимость с KATA 7.0	Совместимость с KATA 7.1
KUMA 2.0	Да	Да	Нет	Нет	Нет	Нет	Нет
KUMA 2.1	Нет	Да	Да	Да	Нет	Нет	Нет
KUMA 3.0.2	Нет	Нет	Нет	Да	Да	Нет	Нет
KUMA 3.0.3	Нет	Нет	Нет	Да	Да	Нет	Нет
KUMA 3.2	Нет	Нет	Нет	Да	Да	Нет	Да
KUMA 3.3	Нет	Нет	Нет	Нет	Нет	Да	Нет
KUMA 3.4	Нет	Нет	Нет	Нет	Нет	Да	Да

Совместимость версий XDR с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать XDR в качестве SIEM-системы.

Информация о совместимости версий XDR с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Совместимость версий XDR с версиями Kaspersky Anti Targeted Attack Platform

Версия XDR	Совместимость с KATA 4.1	Совместимость с KATA 5.0	Совместимость с KATA 5.1	Совместимость с KATA 6.0	Совместимость с KATA 6.1	Совместимость с KATA 7.0	Совместимость с KATA 7.1
XDR 1.0	Нет	Нет	Да	Нет	Нет	Нет	Нет
XDR 1.1	Нет	Нет	Нет	Да	Да	Нет	Нет
XDR 1.2	Нет	Нет	Нет	Нет	Нет	Да	Нет
XDR 1.3	Нет	Нет	Нет	Нет	Нет	Да	Есть ограничения

Совместимость версий KPSN с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать Kaspersky Private Security Network (KPSN) вместо Kaspersky Security Network (KSN), чтобы не использовать отправку данных вашей организации за пределы локальной сети организации.

Информация о совместимости версий KPSN с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Совместимость версий KPSN с версиями Kaspersky Anti Targeted Attack Platform

Версия KPSN	Совместимость с KATA 4.1	Совместимость с KATA 5.0	Совместимость с KATA 5.1	Совместимость с KATA 6.0	Совместимость с KATA 6.1	Совместимость с KATA 7.0	Совместимость с KATA 7.1
KPSN 3.3	Да	Да	Да	Да	Да	Нет	Нет
KPSN 3.4	Нет	Нет	Нет	Да	Да	Да	Да
KPSN 3.5	Нет	Нет	Нет	Да	Да	Да	Да
KPSN 4.0	Нет	Нет	Нет	Нет	Да	Да	Да

Совместимость Kaspersky Anti Targeted Attack Platform с VK Cloud

Kaspersky Anti Targeted Attack Platform поддерживает развертывание на облачной платформе VK Cloud.

При развертывании приложения вы можете подключить к компоненту Central Node компоненты Sandbox.

Ограничения при развертывании Kaspersky Anti Targeted Attack Platform для работы с VK Cloud:

- Поддерживается работа только функционального блока KATA.
- Поддерживается работа только сертифицированной версии приложения на базе операционной системы Astra Linux.
- Поддерживается работа только неотказоустойчивой версии приложения.

- Вы можете настроить интеграцию только с внешней системой KSMG. Подробнее об интеграции см. справку KSMG.
- Вы можете использовать режим распределенного решения, только используя интеграцию с KSMG.

Для функционирования компонента Sandbox необходимо выполнить следующие требования:

- На виртуальной машине должна быть включена вложенная виртуализация.
- Должны быть корректно настроены параметры сетевого интерфейса для доступа обрабатываемых объектов в интернет.

  Активация образов операционной системы Windows возможна только при корректной настройке сетевого интерфейса.

- Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть изолирован от локальной сети вашей организации.
- Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть подключен к подсети, не совпадающей с подсетью, к которой подключен управляющий интерфейс.
- Не рекомендуется использовать статический публичный IP-адрес для сетевого интерфейса, обрабатывающего доступ объектов в интернет.

Ограничения

Известные ограничения Kaspersky Anti Targeted Attack Platform

Для Kaspersky Anti Targeted Attack Platform 7.1.3 и 7.1.7 известны следующие ограничения:

1. При обновлении приложения до версии 7.1.3 или 7.1.7 правила обнаружения вторжений не переносятся автоматически. Вам необходимо добавить пользовательские правила обнаружения вторжений самостоятельно.
2. После восстановления данных пользовательские правила YARA и IOC восстанавливаются в неработоспособном состоянии.

   Мы рекомендуем скачать неработающее правило, удалить это правило в веб-интерфейсе и загрузить сохраненное правило заново.
3. После восстановления данных в режиме распределенного решения и мультитенантности в таблице алертов могут не отображаться новые алерты, созданные в результате проверки технологией AM. Вы можете проверить наличие ограничения и при необходимости устранить его. См. подробнее раздел *Резервное копирование и восстановление данных сервера Central Node в режиме распределенного решения и мультитенантности*.

4. Kaspersky Anti Targeted Attack Platform обрабатывает сетевые события и создает соответствующие им IDS-алерты без задержек при объеме до 1 000 000 алертов в сутки. При превышении этого порога приложение создает алерты с задержкой: отставание в 100 000 алертов устраняется за 1 час.

5. Корректная работа соединения между Central Node, Sensor, PCN и SCN возможна только при размещении серверов с установленными компонентами в одной подсети. Использование Network Address Translation (NAT) не поддерживается. Ограничение не распространяется на компоненты Endpoint Agent: они могут располагаться в отдельной от Central Node подсети.

Для Kaspersky Anti Targeted Attack Platform 7.1.1 и 7.1.2 известны следующие ограничения:

1. Не поддерживаются Sigma-правила, ориентированные на источники данных, отличные от System Monitor (Sysmon) и Журнала событий Windows.

2. Не поддерживаются корреляционные Sigma-правила.

3. В рамках интеграции с функциональным блоком NDR к одному компоненту Central Node можно подключить до 2000 компонентов Endpoint Agent.

4. В файловом алерте, созданном по результатам проверки копии веб-трафика, не заполняется поле **Имя пользователя**, если пользователь аутентифицировался на прокси-сервере с базовой аутентификацией.

5. Если дата на сервере, на котором установлен компонент Central Node, отстает от текущей более чем на 30 дней, приложение Kaspersky Anti Targeted Attack Platform становится неработоспособным. Мы рекомендуем перед установкой приложения убедиться, что дата на сервере, на который вы хотите установить компонент приложения, актуальна.

6. При проверке репутации файла в Kaspersky Security Network в журнал не записывается информация о производителе доверенной подписи.

7. Kaspersky Anti Targeted Attack Platform корректно обрабатывает ERSPAN-трафик, полученный через виртуальный интерфейс со скоростью до 2 Гбит\с. Подача ERSPAN-трафика с большей скоростью приведет к потере данных.

8. Kaspersky Anti Targeted Attack Platform обрабатывает сетевые события и создает соответствующие им IDS-алерты без задержек при объеме до 1 000 000 алертов в сутки. При превышении этого порога приложение создает алерты с задержкой: отставание в 100 000 алертов устраняется за 1 час.

9. Корректная работа соединения между Central Node, Sensor, PCN и SCN возможна только при размещении серверов с установленными компонентами в одной подсети. Использование Network Address Translation (NAT) не поддерживается. Ограничение не распространяется на компоненты Endpoint Agent: они могут располагаться в отдельной от Central Node подсети.

Для Kaspersky Anti Targeted Attack Platform 7.1 известны следующие ограничения:

1. Не поддерживаются Sigma-правила, ориентированные на источники данных, отличные от System Monitor (Sysmon) и Журнала событий Windows.

2. Не поддерживаются корреляционные Sigma-правила.

3. В рамках интеграции с функциональным блоком NDR к одному компоненту Central Node можно подключить до 2000 компонентов Endpoint Agent.

4. В файловом алерте, созданном по результатам проверки копии веб-трафика, не заполняется поле **Имя пользователя**, если пользователь аутентифицировался на прокси-сервере с базовой аутентификацией.

5. Если дата на сервере, на котором установлен компонент Central Node, отстает от текущей более чем на 30 дней, приложение Kaspersky Anti Targeted Attack Platform становится неработоспособным. Мы рекомендуем перед установкой приложения убедиться, что дата на сервере, на который вы хотите установить компонент приложения, актуальна.

6. Размер полезного блока данных одного пакета (англ. maximum transmission unit, MTU) на канале связи между серверами Central Node и Sensor, а также PCN и SCN по умолчанию составляет 1500. Если вам известно, что провайдер ограничивает размер MTU на каналах связи между компонентами решения, вам нужно настроить параметры MTU таким образом, чтобы его размер не превышал значение, разрешенное провайдером.

7. При проверке репутации файла в Kaspersky Security Network в журнал не записывается информация о производителе доверенной подписи.

8. Kaspersky Anti Targeted Attack Platform корректно обрабатывает ERSPAN-трафик, полученный через виртуальный интерфейс со скоростью до 2 Гбит\с. Подача ERSPAN-трафика с большей скоростью приведет к потере данных.

9. Обновление Central Node, установленного на сервере, может завершиться ошибкой "Upgrade task " (MoveVolumesDataTask)" completed with an error", если под базу данных компонента Targeted Attack Analyzer был выделен диск объемом 2 ТБ и более.

   Порядок действий при возникновении ошибки "Upgrade task "(MoveVolumesDataTask)" completed with an error"

   1. Войдите в консоль управления сервера Central Node, на котором вы хотите выполнить обновление, по протоколу SSH или через терминал.

   2. В директории /data/upgrade создайте файл wa.sh со следующим содержимым:

      ```
      set -e
      rsync -ah /data/storage/volumes/clickhouse/ /data/volumes/clickhouse/
      rm -rf /data/storage/volumes/clickhouse/
      docker volume rm -f kata_product_edr_synchronizer_storage_1 kata_product_agent_server_storage_1 \
      kata_product_ksn_proxy_storage_1 kata_product_prometheus_volume_1
      kata_product_nta_database_storage_1 \
      kata_product_postfix_storage_1 kata_product_response_actions_processor_volume_1
      kata_product_siem_proxy_storage_1 \
      kata_product_updater_storage_1 kata_product_zookeeper_data_volume_1
      kata_product_clickhouse_storage_1
      sed -i 's/"current_task_index":[[:space:]]*25/"current_task_index": 26/' /data/upgrade/upgrade_config.json
      ./run_kata_upgrade.py
      ```

   3. Установите разрешение на запуск скрипта, выполнив команду:

      ```
      chmod +x wa.sh
      ```

   4. Запустите скрипт, выполнив команду:

      ```
      ./wa.sh
      ```

   Процесс обновления возобновится.

10. Для корректной работы компонента Central Node, установленного на сервере с операционной системой Astra Linux, требуется больше свободного места на диске по сравнению с версией приложения 7.0.3. Если на сервере Central Node недостаточно свободного места, установка пакета обновления завершается ошибкой. Приложение при этом остается работоспособным.

    Вы можете освободить место на диске. См. подробнее раздел *Обновление Central Node, установленного на сервере*.

11. Корректная работа соединения между Central Node, Sensor, PCN и SCN возможна только при размещении серверов с установленными компонентами в одной подсети. Использование Network Address Translation (NAT) не поддерживается. Ограничение не распространяется на компоненты Endpoint Agent: они могут располагаться в отдельной от Central Node подсети.

Ограничения в Kaspersky Endpoint Security 12.9 для Windows

Вы можете посмотреть список ограничений в Kaspersky Endpoint Security 12.9 для Windows в справке Kaspersky Endpoint Security для Windows.

Ограничения в Kaspersky Endpoint Security 12.2 для Linux

Вы можете посмотреть список ограничений в Kaspersky Endpoint Security 12.2 для Linux в документе Kaspersky Endpoint Security для Linux Release Notes.

Ограничения в Kaspersky Endpoint Security 12.1 для Mac

Вы можете посмотреть список ограничений в Kaspersky Endpoint Security 12.1 для Mac в справке Kaspersky Endpoint Security для Mac.

Общие ограничения

Для правильной работы Kaspersky Anti Targeted Attack Platform должны выполняться следующие требования:

1. Размер полезного блока данных одного пакета (англ. maximum transmission unit, MTU) на канале связи между серверами Central Node и Sensor, а также PCN и SCN по умолчанию составляет 1500. Если вам известно, что провайдер ограничивает размер MTU на каналах связи между компонентами решения, вам нужно настроить параметры MTU таким образом, чтобы его размер не превышал значение, разрешенное провайдером.

2. Не поддерживается изменение имени сервера Central Node через командную строку.

3. Если вы хотите установить компонент Endpoint Agent на виртуальную машину, мы настоятельно не рекомендуем создавать эту виртуальную машину путем клонирования эталонного образа, включающего Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux. При клонировании образа у виртуальной машины остается неизменным уникальный идентификатор, из-за чего Kaspersky Anti Targeted Attack Platform впоследствии может определять несколько виртуальных машин как одно устройство. В результате функции, которые входят в функциональный блок KEDR, например, поиск угроз по базе событий или сетевая изоляция, будут работать некорректно. Вы можете устранить это ограничение, установив Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux на виртуальную машину после того, как она будет развернута.

Развертывание Central Node в виде кластера

При развертывании компонента Central Node в виде кластера действуют следующие ограничения:

1. Кластер должен включать минимум 4 сервера: 2 сервера хранения и 2 обрабатывающих сервера. Вы можете масштабировать кластер для увеличения количества обрабатываемого трафика или количества подключенных компьютеров в соответствии с руководством по масштабированию.

2. Кластер является отказоустойчивым, но не высокопроизводительным. Добавление в кластер большего количества обрабатывающих серверов, чем рекомендуется в руководстве по масштабированию, не обеспечивает бесконечный рост количества принимаемой телеметрии и/или обрабатываемого трафика.

3. При выходе из строя некоторых серверов кластера работоспособность кластера восстанавливается только в том случае, если в рабочем состоянии находятся хотя бы два сервера с ролью manager в Docker swarm.

4. Рекомендуется добавлять в кластер серверы с одинаковой аппаратной конфигурацией. В противном случае пропорциональное увеличение производительности не гарантируется.

5. Добавление в кластер дополнительного сервера не ускоряет обработку объектов, которые уже находятся в очереди на проверку.

6. Веб-интерфейс приложения может быть недоступен некоторое время при отказе сервера, на котором он расположен.

7. При отказе обрабатывающего сервера возможна потеря полученных по протоколам ICAP, POP3 и SMTP данных трафика и копий сообщений электронной почты, которые ждут обработки, и обнаружений, связанных с ними.

8. Если для обрабатывающего сервера настроено получение зеркалированного трафика со SPAN-портов, то при выходе из строя этого сервера SPAN-трафик не обрабатывается.

9. Компонент Sensor можно подключить только к обрабатывающему серверу кластера. Для этого сервера должно быть **настроено получение зеркалированного трафика со SPAN-портов**.

   Вы можете включить получение зеркалированного трафика при установке компонента. Если вы отказались от получения трафика на этапе установки, выполните шаги инструкции ниже.

   Чтобы включить получение зеркалированного трафика со SPAN-портов:

   1. Если Central Node установлен на сервере, войдите в консоль управления этим сервером по протоколу SSH или через терминал.

   2. Если Central Node развернут в виде кластера, войдите в консоль управления любым из обрабатывающих серверов кластера по протоколу SSH или через терминал.

   3. Выполните команду:

      ```
      kata-enable-span
      ```

      Получение зеркалированного трафика со SPAN-портов будет включено.

10. Возможна временная рассинхронизация данных в базе событий при отказе одного из серверов кластера или временной потере связи между сервером и компонентом Endpoint Agent, подключенным к функциональному блоку KEDR.

11. При изменении конфигурации серверов кластера возможно временное замедление обработки трафика и событий с компьютеров, на которых установлен компонент Endpoint Agent, подключенный к функциональному блоку KEDR.

12. При установке Kaspersky Anti Targeted Attack Platform в виде кластера или при обновлении кластерной конфигурации возможна ситуация, когда не запускается встроенный Sensor (Embedded Sensor).

    В этом случае мы рекомендуем сделать следующее:

    - Если Sensor не подключен, вам нужно удалить его через веб-интерфейс приложения, затем в режиме Technical Support Mode выполнить **последовательность команд для запуска Sensor**.

      1. `kata-sensor-tool reset`
      2. `kata-sensor-tool reset-core`
      3. `kata-sensor-tool init-embedded-sensor`

    - Если Sensor не запущен, вам нужно в режиме Technical Support Mode выполнить **последовательность команд для запуска Sensor**.

      1. `kata-sensor-tool reset`
      2. `kata-sensor-tool reset-core`
      3. `kata-sensor-tool init-embedded-sensor`

Через некоторое время Sensor появится в веб-интерфейсе.

13. Не поддерживается установка Kaspersky Anti Targeted Attack Platform в виде кластера на виртуальных платформах zVirt Node, "РЕД Виртуализация", KVM, VMware ESXi.

Ограничения Sensor

Для компонента Sensor действуют следующие ограничения:

1. Для захвата сетевого трафика на максимальной скорости 10 Гбит/с могут использоваться только компоненты Sensor, установленные на отдельных серверах.

2. При захвате FTP-трафика на максимальной скорости 10 Гбит/с возможен высокий уровень потерь.

3. Настройку параметров проверки ICAP-трафика в режиме реального времени на отдельных серверах с установленным компонентом Sensor возможно выполнить только в режиме Technical Support Mode.

Ограничения Sandbox

Для компонента Sandbox действуют следующие ограничения:

1. Поддерживается установка пользовательских образов операционных систем следующих версий:

   - Windows 7.

   - Windows 8.1 64-разрядная.

   - Windows 10 64-разрядная (до версии 1909).

2. Для пользовательских образов операционных систем полностью поддерживаются следующие локализации: русский, английский, упрощенный китайский (simplified), арабский, испанский (Mexico).

3. Лицензионные ключи для активации операционных систем и программного обеспечения не предоставляются.

4. Если в наборе операционных систем на сервере с компонентом Central Node выбраны операционные системы, не установленные на сервере с компонентом Sandbox, Kaspersky Anti Targeted Attack Platform не отправляет объекты на проверку компоненту Sandbox. При подключении к компоненту Central Node нескольких серверов с компонентом Sandbox приложение отправляет объекты на проверку тем серверам, на которых установлены операционные системы, соответствующие выбранному на Central Node набору.

Развертывание приложения на платформах виртуализации

zVirt Node, "РЕД Виртуализация", KVM, VMware ESXi

Не поддерживается развертывание отказоустойчивой версии приложения (кластера Central Node) на виртуальных платформах zVirt Node, "РЕД Виртуализация", KVM, VMware ESXi.

ПК СВ "Брест", zVirt Node, "РЕД Виртуализация"

Если вы планируете использовать компонент Sandbox на виртуальной платформе ПК СВ "Брест", zVirt Node или "РЕД Виртуализация", вам потребуется дополнительно настроить время проверки объектов компонентом, чтобы повысить вероятность обнаружения. Для настройки обратитесь в Службу технической поддержки.

Nutanix

Если вы используете кластер Nutanix и планируете использовать Central Node в кластерной конфигурации на этой платформе, все серверы кластера Central Node требуется развернуть на одном хосте кластера Nutanix. Это необходимо для корректной маршрутизации пакетов через внутренний виртуальный коммутатор.

Использование приложения в режиме распределенного решения и мультитенантности

При использовании приложения в режиме распределенного решения и мультитенантности действуют следующие ограничения:

1. На сервере PCN на вкладке **Активы** → **Устройства** отображаются только те хосты, которые подключены к этому серверу PCN.

2. Смена пароля для учетных записей доступна только на сервере PCN.

3. Отключение SCN от PCN необратимо. Повторное подключение SCN к какому-либо серверу PCN не предусмотрено.

Ограничения совместимости с Kaspersky Endpoint Security для Windows

Ограничения совместимости версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform

- Интеграция Kaspersky Endpoint Security 12.1 - 12.6 с Kaspersky Anti Targeted Attack Platform 7.0.

  Объем передаваемых Kaspersky Endpoint Security данных ограничен:

  - Не передаются данные о событиях **DNS**, **Внедрение кода**, **Именованный канал**, **WMI**, **LDAP**.
  - Для события **Изменен файл** не обрабатываются данные о подтипах **Прочитан файл**, **Создана жесткая ссылка**, **Символическая ссылка создана**.
  - Для события **Изменение в реестре** не обрабатываются данные о подтипах **Переименован ключ реестра**, **Сохранен ключ реестра**.
  - Для событий **Загружен модуль** и **Удаленное соединение** не расширен состав полей.

- Интеграция Kaspersky Endpoint Security 12.1 - 12.6 с Kaspersky Anti Targeted Attack Platform 7.1.

  Объем передаваемых Kaspersky Endpoint Security данных ограничен:

  - Не передаются данные событий **Именованный канал**, **WMI**, **LDAP**, **DNS**, **Внедрение кода**, **USB-устройство**.
  - Для события **Изменен файл** не обрабатываются данные о подтипах **Прочитан файл**, **Создана жесткая ссылка**, **Символическая ссылка создана**.
  - Для события **Изменение в реестре** не обрабатываются данные о подтипах **Переименован ключ реестра**, **Сохранен ключ реестра**.
  - Для событий **Загружен модуль** и **Удаленное соединение** не расширен состав полей.

- Интеграция Kaspersky Endpoint Security 12.7 с Kaspersky Anti Targeted Attack Platform 5.0-6.1.

  Сервер этих версий Kaspersky Anti Targeted Attack Platform воспринимает ограниченный объем данных от приложения Kaspersky Endpoint Security:

  - Не обрабатываются данные событий **Именованный канал**, **WMI**, **LDAP**, **DNS**, **Внедрение кода**.
  - Для события **Изменен файл** не обрабатываются данные о подтипах **Прочитан файл**, **Создана жесткая ссылка**, **Символическая ссылка создана**.
  - Для события **Изменение в реестре** не обрабатываются данные о подтипах **Переименован ключ реестра**, **Сохранен ключ реестра**.
  - Для событий **Загружен модуль** и **Удаленное соединение** не расширен состав полей.

- Интеграция Kaspersky Endpoint Security 12.7 с Kaspersky Anti Targeted Attack Platform 7.1.

  Объем передаваемых Kaspersky Endpoint Security данных ограничен: не обрабатываются данные события **USB-устройство**.

- Интеграция Kaspersky Endpoint Security 12.8, 12.9 с Kaspersky Anti Targeted Attack Platform 5.0-6.1.

  Сервер этих версий Kaspersky Anti Targeted Attack Platform воспринимает ограниченный объем данных от приложения Kaspersky Endpoint Security:

  - Не обрабатываются данные событий **Именованный канал**, **WMI**, **LDAP**, **DNS**, **Внедрение кода**, **USB-устройство**.
  - Для события **Изменен файл** не обрабатываются данные о подтипах **Прочитан файл**, **Создана жесткая ссылка**, **Символическая ссылка создана**.
  - Для события **Изменение в реестре** не обрабатываются данные о подтипах **Переименован ключ реестра**, **Сохранен ключ реестра**.
  - Для событий **Загружен модуль** и **Удаленное соединение** не расширен состав полей.

- Интеграция Kaspersky Endpoint Security 12.8, 12.9 с Kaspersky Anti Targeted Attack Platform 7.0.

  Сервер этой версии Kaspersky Anti Targeted Attack Platform не обрабатывает данные события **USB-устройство**.

Ограничения совместимости с Kaspersky Endpoint Security для Linux

Ограничения совместимости версий Kaspersky Endpoint Security для Linux с версиями Kaspersky Anti Targeted Attack Platform

- Интеграция Kaspersky Endpoint Security 11.4 с Kaspersky Anti Targeted Attack Platform 5.1 - 6.1.

  Объем передаваемых Kaspersky Endpoint Security данных ограничен:

  - Не поддерживается создание правил сетевой изоляции.
  - Не поддерживается создание правил запрета.
  - Не поддерживается поиск индикаторов компрометации на компьютерах с помощью IOC-файлов.
  - Список передаваемых событий ограничен следующими типами: **Запущен процесс**, **Изменен файл**, **Журнал событий ОС**, **Обнаружение**, **Результат обработки обнаружения**.
  - Список задач ограничен следующими типами: **Получить файл**, **Запустить программу**.

- Интеграция Kaspersky Endpoint Security 12, 12.1 с Kaspersky Anti Targeted Attack Platform 5.1.

Объем передаваемых Kaspersky Endpoint Security данных ограничен:

- Не поддерживается создание правил запрета.
- Список передаваемых событий ограничен следующими типами: **Запущен процесс**, **Изменен файл**, **Журнал событий ОС**, **Обнаружение**, **Результат обработки обнаружения**.
- Список задач ограничен следующими типами: **Получить файл**, **Запустить программу**, **Удалить файл**, **Завершить процесс**.

- Интеграция Kaspersky Endpoint Security 12, 12.1 с Kaspersky Anti Targeted Attack Platform 6.0 - 7.1.

  Объем передаваемых Kaspersky Endpoint Security данных ограничен:

  - Список передаваемых событий ограничен следующими типами: **Завершен процесс**, **Правило запрета**, **Заблокирован документ**.
  - Список задач ограничен следующими типами: **Получить файл**, **Запустить программу**, **Удалить файл**, **Завершить процесс**.

- Интеграция Kaspersky Endpoint Security 12.2, 12.3 с Kaspersky Anti Targeted Attack Platform 6.0, 6.1.

  Объем передаваемых Kaspersky Endpoint Security данных ограничен:

  - Список передаваемых событий ограничен следующими типами: **Завершен процесс**, **Правило запрета**, **Заблокирован документ**.
  - Список задач ограничен следующими типами: **Получить файл**, **Запустить программу**, **Удалить файл**, **Завершить процесс**, **Поместить файл на карантин**, **Восстановить файл из карантина**.

- Интеграция Kaspersky Endpoint Security 12.2, 12.3 с Kaspersky Anti Targeted Attack Platform 7.0, 7.1.

  Объем передаваемых Kaspersky Endpoint Security данных ограничен:

  - Список передаваемых событий ограничен следующими типами: **Завершен процесс**, **Правило запрета**, **Заблокирован документ**, **Внедрение кода**, **DNS**.
  - Список задач ограничен следующими типами: **Получить файл**, **Запустить программу**, **Удалить файл**, **Завершить процесс**, **Поместить файл на карантин**, **Восстановить файл из карантина**.

Ограничения совместимости с Kaspersky Endpoint Security для Mac

Ограничения совместимости версий Kaspersky Endpoint Security для Mac с версиями Kaspersky Anti Targeted Attack Platform

- Интеграция Kaspersky Endpoint Security 12, 12.1, 12.2 с Kaspersky Anti Targeted Attack Platform 6.0 - 7.1.

  Объем передаваемых Kaspersky Endpoint Security данных ограничен:

  - Не поддерживается создание правил сетевой изоляции.
  - Не поддерживается создание правил запрета.

- Не поддерживается поиск индикаторов компрометации на компьютерах с помощью IOC-файлов.
- Список передаваемых событий ограничен следующими типами: **Запущен процесс**, **Завершен процесс**, **Изменен файл**, **Обнаружение**, **Результат обработки обнаружения**.
- Список задач ограничен следующими типами: **Получить файл**, **Запустить программу**.

Ограничения совместимости с XDR

Ограничения совместимости версий XDR с Kaspersky Anti Targeted Attack Platform

Объем данных, передаваемых Kaspersky Anti Targeted Attack Platform 7.1 при интеграции с XDR 1.3, ограничен: не передаются данные активов.

Интеграция с прокси-сервером по протоколу ICAP

При интеграции с прокси-сервером по протоколу ICAP действуют следующие ограничения:

1. Настройка интеграции по протоколу ICAP с сервисом SQUID версии 5.9 и ниже недоступна.
2. Количество одновременных подключений к приложению через прокси-сервер не должно превышать 20 000. Рекомендуемое значение – 1000.

Предоставление данных

Для работы некоторых компонентов Kaspersky Anti Targeted Attack Platform необходима обработка данных на стороне "Лаборатории Касперского". Компоненты не отправляют данные без согласия администратора Kaspersky Anti Targeted Attack Platform.

Вы можете ознакомиться с перечнем данных и условиями их использования, а также дать согласие на обработку данных в следующих соглашениях между вашей организацией и "Лабораторией Касперского":

- В Лицензионном соглашении (например, при установке приложения).

  Согласно условиям Лицензионного соглашения, вы соглашаетесь в автоматическом режиме предоставлять "Лаборатории Касперского" информацию, перечисленную в Лицензионном соглашении в пункте Предоставление информации. Лицензионное соглашение входит в комплект поставки приложения.

- В Положении о KSN (например, при установке приложения или в меню администратора приложения после установки).

  При участии в Kaspersky Security Network в "Лабораторию Касперского" автоматически передается информация, полученная в результате работы Kaspersky Anti Targeted Attack Platform. Перечень передаваемых данных указан в Положении о KSN. Пользователь Kaspersky Anti Targeted Attack Platform самостоятельно принимает решение об участии в KSN. Положение о KSN входит в комплект поставки приложения.

  Перед тем, как данные KSN-статистики отправляются в "Лабораторию Касперского", они накапливаются в кеше на серверах с компонентами Kaspersky Anti Targeted Attack Platform.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

При использовании Kaspersky Private Security Network в "Лабораторию Касперского" не передается информация о работе Kaspersky Anti Targeted Attack Platform, но данные KSN-статистики накапливаются в кеше на серверах с компонентами Kaspersky Anti Targeted Attack Platform в том же составе, что и при использовании Kaspersky Security Network. Эти накопленные данные KSN-статистики могут передаваться за пределы вашей организации в том случае, если сервер с приложением Kaspersky Private Security Network находится за пределами вашей организации.

Администратору Kaspersky Private Security Network необходимо обеспечить безопасность этих данных самостоятельно.

Служебные данные приложения

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Anti Targeted Attack Platform не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлено приложение, к персональным данным других пользователей любыми системными средствами на его усмотрение.

Информация о служебных данных Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Служебные данные Kaspersky Anti Targeted Attack Platform

Тип данных	Место и срок хранения
• Данные об учетных записях пользователей. • Данные компонента Central Node. • Данные о тенантах. • Данные о подключенных к компоненту Central Node компьютерах, на которых установлен компонент Endpoint Agent. • Данные о предустановках и правилах запрета. • Данные о задачах, назначенных на компьютеры с компонентом Endpoint Agent. • Данные о пользовательских схемах расположения виджетов. • Данные о пользовательских правилах TAA (IOA). • Данные о пользовательских правилах IDS. • Данные о пользовательских правилах IOC. • Данные о правилах сетевой изоляции. • Данные об исключениях из проверки. • Данные об отчетах и шаблонах отчетов. • Данные о сертификатах компонента Endpoint Agent.	Данные хранятся бессрочно на сервере с компонентом Central Node в директории `/data`, если компонент Central Node установлен на сервере. При установке компонента Central Node на кластер данные хранятся бессрочно на серверах хранения.

Тип данных	Место и срок хранения
Информация об интеграции с MDR, KSN, KPSN.	Данные хранятся бессрочно на сервере с компонентом Central Node в директории `/data`.
Данные об используемых лицензионных ключах или кодах активации.	
Настройки Endpoint Agent.	
Настройки почтового сервера, используемого для отправки уведомлений: • IP-адрес и порт сервера. • Цифровой отпечаток сертификата. • Логин и хеш пароля пользователя, от имени которого происходит авторизация на сервере. • Имя секрета, который используется в качестве ключа расшифровки. • Используется ли шифрование.	
Имя текущего сервера.	
Адреса серверов, подключенных к текущему серверу, и данные о сертификатах, используемых для взаимной аутентификации с ними.	
Настройки коннекторов: • Адрес узла размещения коннектора. • Адрес сервера сторонней системы, с которой взаимодействует коннектор.	
Данные о секретах и данные учетных записей пользователей Central Node.	
Адрес точки мониторинга.	
Данные об ICAP-исключениях.	

Тип данных	Место и срок хранения
Настройки интеграции Sensor с ICAP: • Состояние (включено или выключено). • Максимальное количество подключений. • Адрес подключения в режиме REQMOD. • Адрес подключения в режиме RESPMOD. • Заголовок запроса ICAP, который содержит IP-адрес клиента, отправившего HTTP запрос, при получении этого запроса через прокси-сервер. • Заголовок запроса ICAP, который содержит порт клиента, отправившего HTTP запрос, при получении этого запроса через прокси-сервер. • Имя пользователя. • Заголовок запроса ICAP, который содержит имя пользователя клиента, отправившего HTTP запрос, при получении этого запроса через прокси-сервер. • Использовано ли декодирование base64. • Режим работы. • Таймаут проверки. • Важность обнаружения. • Страница, возвращаемая пользователю при блокировке файла • Страница, возвращаемая пользователю при блокировке URL • Прослушиваемые интерфейсы.	
Настройки отправки пользовательских правил обнаружения вторжений в KSN.	
Данные о состоянии и именах Keytab-файлов, используемых в Kerberos-аутентификации.	
Информация о приоритете проверки сообщений электронной почты KSMG.	
Настройки уведомлений о загрузке ЦП и ОЗУ: • Пороги использования центрального процессора, жесткого диска и оперативной памяти. • Интервал обновления статистики.	
Информация о сертификатах, используемых для взаимной аутентификации Sensor и Central Node.	

Тип данных	Место и срок хранения
Настройки интеграции Sensor с POP3: • IP-адрес и порт сервера POP3. • Логин и хеш пароля пользователя, от имени которого происходит авторизация на сервере POP3. • Имя секрета, который используется в качестве ключа расшифровки. • Политика проверки сертификатов. • Сертификаты клиентов.	
Настройки прокси-сервера: • IP-адрес и порт прокси-сервера. • Логин и хеш пароля пользователя, от имени которого происходит авторизация на прокси-сервере. • Имя секрета, который используется в качестве ключа расшифровки. • Состояние прокси-сервера.	
Настройки серверов хранения: • Размер хранилища. • Срок хранения данных.	
Настройки серверов с компонентом Sandbox: • IP-адрес и имя сервера. • Состояние сервера. • Цифровой отпечаток сертификата.	
Настройки Sandbox: • Список образов виртуальных машин. • Состояние синхронизации Sandbox.	
Настройки безопасности: • Период смены и сброса пароля. • Счетчик неудачных попыток аутентификации. • Максимальное время бездействия пользователя. • Состояние блокировки раздела **Мониторинг** при отсутствии активности со стороны пользователя.	
Настройки серверов с компонентом Sensor: максимальный размер файла, отправляемого на сканирование.	

Тип данных	Место и срок хранения
Настройки SIEM: • Состояние локальных и удаленных журналов обновлений и действий. • Состояние TLS-шифрования. • Адреса и порты серверов SIEM • Используемый сетевой протокол. • ID хоста, отправляющего данные в SIEM. • Сертификат шифрования TLS.	
Настройки интеграции Sensor с SMTP: • Сертификаты, используемые для взаимной аутентификации. • Имена доменнов и поддоменов. • Клиентские сети и подсети SMTP. • Уровень безопасности TLS. • Состояние запроса клиентского TLS сертификата • Состояние SMTP.	
Настройки соединения по протоколу SNMP: • Логин. • Хеш пароля. • Имя секрета, который используется в качестве ключа расшифровки. • Версия протокола. • Состояние SNMP.	
Настройки интеграции Sensor со SPAN: • Прослушиваемые интерфейсы. • Состояние сохранения HTTP-заголовков. • Состояние SPAN. • Сертификаты клиентов.	
Настройки хранилища зеркалированного трафика со SPAN-портов: • Состояние и размер хранилища. • Используемая директория. • Максимальное количество файлов.	
Настройки поиска угроз: • Используются ли правила TAA для проверки цепочек событий. • Используемая версия модели данных.	
Настройки часового пояса.	
Настройки обновлений: • Тип сервера обновлений. • Пользовательский URL-адрес сервера обновлений.	Данные хранятся бессрочно на сервере с компонентом Central Node в директории `/data`.
Журнал событий ОС.	Файлы журнала ОС хранятся бессрочно в директории `/var/log` на сервере с компонентом Central Node.

Тип данных	Место и срок хранения
Журнал с информацией о работе приложения.	Файл журнала хранится бессрочно в директории /data на сервере с компонентом Central Node, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.
Очередь файлов на проверку.	Файлы хранятся на сервере с компонентом Central Node в директории /data, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных. Данные хранятся до выполнения проверки.
Файлы, полученные с компьютеров с компонентом Endpoint Agent.	Файлы хранятся на сервере с компонентом Central Node в директории /data, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных. Данные ротируются при заполнении места на диске.
Файлы с правилами YARA и IDS (пользовательские и от "Лаборатории Касперского").	Файлы хранятся бессрочно в директории /data на сервере с компонентом Central Node, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.
Файлы с данными о переданных во внешние системы обнаружениях.	Файлы хранятся бессрочно на сервере с компонентом Central Node в директории /data, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.
Артефакты компонента Sandbox.	Файлы хранятся на сервере с компонентом Central Node в директории /data, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных. Данные ротируются при заполнении места на диске.
Файлы, для которых были созданы обнаружения компонентом Sandbox.	Файлы хранятся на сервере с компонентом Central Node в директории /data, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных. Данные ротируются при заполнении места на диске.
Файлы сертификатов, которые используются для аутентификации компонентов приложения.	Файлы хранятся бессрочно в директории /data на сервере с компонентом Central Node, PCN, SCN, Sensor или на компьютере с компонентом Endpoint Agent.
Ключи шифрования, которые передаются между компонентами приложения.	Файлы хранятся бессрочно в директории /data на сервере с компонентом Central Node, PCN, SCN, Sensor или на компьютере с компонентом Endpoint Agent.
Копии зеркалированного трафика со SPAN-портов.	Файлы хранятся в хранилище, примонтированном к серверу с компонентом Sensor. Данные удаляются по мере заполнения места на диске.

Тип данных	Место и срок хранения
Фильтры ICAP-исключений.	Файлы хранятся бессрочно на сервере с компонентом Central Node в директории /data, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.
• Данные о сетевых сессиях. • Данные устройств. • Телеметрия при интеграции с компонентом Endpoint Agent. • События в трафике сети. • Данные учетных записей пользователей. • Данные об исполняемых файлах. • Дампы трафика, относящегося к зарегистрированным событиям. • Дампы трафика, относящегося к сетевым сеансам.	Данные хранятся на сервере с компонентом Central Node в директории /data/storage/volumes/nta_database. Данные ротируются по мере заполнения места на диске.
• Идентификатор учетной записи. • Имя учетной записи. • Доменное имя пользователя. • Роль учетной записи. • Статус учетной записи. • Дата и время последней смены пароля учетной записи.	Файлы хранятся бессрочно на сервере с компонентом Central Node в директории /data, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.
Данные о конфигурациях виртуальных машин: • IP-адрес сервера с компонентом Sandbox. • Список виртуальных машин.	

Тип данных	Место и срок хранения
Данные об учетных записях: • Идентификатор учетной записи. • Имя учетной записи. • Имя компьютера, на котором авторизован пользователь.	Данные хранятся на сервере с компонентом Central Node в директории /data/storage/volumes/nta_database. Данные ротируются по мере заполнения места на диске.
Данные сетевых сессий: • Имена участников сетевого взаимодействия. • IP- и MAC-адреса участников сетевого взаимодействия.	
Данные об устройствах, зарегистрированных в приложении: • Имена устройств. • IP- и MAC-адреса устройств.	
Данные, сохраняемые при интеграции с компонентом Endpoint Agent в рамках функциональности NDR: • IP- и MAC-адреса компьютера с компонентом Endpoint Agent. • Имя компьютера с компонентом Endpoint Agent. • Имя учетной записи, зарегистрированной на компьютере с компонентом Endpoint Agent. • Используемая на компьютере операционная система. • User Agent.	
Данные о событиях в трафике сети: IP- и MAC-адреса устройств.	
Данные об исполняемых файлах на компьютерах с компонентом Endpoint Agent, подключенных в рамках функциональности NDR: • Имя файла. • Путь к файлу. • Версия файла. • MD5- и SHA256-хеш файла.	
Данные дампов трафика, относящегося к зарегистрированным сетевым сеансам и событиям: • Имена участников сетевого взаимодействия. • IP- и MAC-адреса участников сетевого взаимодействия. • Имена устройств. • IP- и MAC-адреса устройств. • Имя учетной записи пользователя. • Идентификатор учетной записи. • Используемая на компьютере операционная система. • User Agent. • Имя исполняемого файла. • Путь к исполняемому файлу. • Версия исполняемого файла. • MD5- и SHA256-хеш исполняемого файла.	
Журнал аудита действий пользователей, относящийся к функциональности NDR.	

Данные компонентов Central Node и Sensor

В этом разделе содержится следующая информация о данных пользователей, хранящихся на сервере с компонентом Central Node и на сервере с компонентом Sensor:

- состав хранимых данных;
- место хранения;
- срок хранения;
- доступ пользователей к данным.

Данные трафика компонента Sensor

Данные трафика компонента Sensor хранятся на сервере с компонентом Sensor или на сервере с компонентами Sensor и Central Node, если Sensor и Central Node установлены на одном сервере или развернуты в виде кластера.

Данные трафика записываются и хранятся в последовательно создаваемых файлах. Приложение перестает записывать данные в один файл и начинает записывать в следующий файл в следующих случаях:

- при достижении максимального размера файла (вы можете настроить этот параметр);
- по окончании заданного в настройках промежутка времени (вы можете настроить этот параметр);
- при перезагрузке службы сохранения трафика или всего приложения Kaspersky Anti Targeted Attack Platform.

По мере накопления данных трафика, Kaspersky Anti Targeted Attack Platform фильтрует данные и оставляет только следующую информацию:

- информацию, связанную с обнаружениями, созданными в результате проверки технологией Targeted Attack Analyzer;
- PCAP-файлы, в которых:
  - IP-адрес источника или назначения совпадают каким-либо IP-адресом из обнаружения;
  - данные трафика относятся ко времени, отстоящему от времени создания обнаружения не более, чем на 15 минут.

Отфильтрованные данные трафика переносятся в отдельный раздел. Все остальные данные трафика (не отвечающие условиям фильтрации), удаляются.

Данные отфильтрованного трафика сохраняются в последовательно создаваемых файлах. Приложение перестает записывать данные в один файл и начинает записывать в следующий файл в следующих случаях:

- при достижении максимального размера файла;
- по окончании заданного в настройках промежутка времени.

Данные отфильтрованного трафика хранятся за последние сутки. Более старые данные удаляются.

Данные в обнаружениях

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Anti Targeted Attack Platform не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлено приложение, к персональным данным других пользователей любыми системными средствами на его усмотрение.

Информация о данных, которые могут сохраняться при создании обнаружений, приведена в таблице ниже.

Тип данных	Место и срок хранения
Для всех обнаружений на сервере хранятся следующие данные: • Дата и время создания обнаружения. • Дата и время изменения обнаружения. • Категория обнаруженного объекта. • Имя обнаруженного файла. • Тип обнаруженного файла. • Источник обнаруженного объекта. • Обнаруженный URL-адрес. • MD5-, SHA256-хеш обнаруженного файла. • Комментарии пользователя, добавленные в детали алерта, связанного с обнаружением. • Идентификатор правила TAA(IOA), в соответствии с которым было создано обнаружение. • IP-адрес и имя компьютера, на котором выполнено обнаружение. • Идентификатор компьютера, на котором выполнено обнаружение. • User agent. • Учетная запись пользователя, которому был назначен алерт, связанный с обнаружением. • Список файлов. • Важность обнаружения в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского". • Технология, по которой было выполнено обнаружение. • Статус алерта, связанного с обнаружением. • Имя пользователя, которому назначен алерт, связанный с обнаружением. • Идентификатор события (при использовании функциональности NDR). • Идентификаторы устройств (при использовании функциональности NDR).	Если Central Node установлен на сервере, информация об обнаружениях хранится на сервере Central Node в директории /data. Если Central Node установлен в виде кластера, информация об обнаружениях хранится в хранилище ceph. Данные ротируются, когда количество записей об обнаружениях, созданных в результате проверки одной технологией, достигает 1 000 000.
При изменении алерта, связанного с обнаружением, на сервере хранится следующая информация: • Учетная запись пользователя, который изменил алерт. • Учетная запись пользователя, которому был назначен алерт. • Дата и время изменения алерта. • Статус алерта. • Пользовательский комментарий.	
Если обнаружение создано в результате проверки файла, на сервере может храниться следующая информация: • Полное имя обнаруженного файла. • MD5-, SHA256-хеш обнаруженного файла. • Размер обнаруженного файла. • Информация о подписи файла.	
Если обнаружение создано в результате проверки FTP-трафика, на сервере может храниться следующая информация: • URI FTP-запроса.	
Если обнаружение создано в результате проверки HTTP-трафика, на сервере может храниться следующая информация: • URI HTTP-запроса. • URI источника запроса. • User agent. • Информация о прокси-сервере.	

Тип данных	Место и срок хранения
Если обнаружение создано в результате проверки технологией Intrusion Detection System, на сервере может храниться следующая информация: • Имя компьютера, с которого были отправлены данные. • Имя компьютера, получившего данные. • IP-адрес компьютера, с которого были отправлены данные. • IP-адрес компьютера, получившего данные. • Переданные данные. • Время передачи данных. • URL-адрес, извлеченный из файла с трафиком, User Agent, метод. • Файл с трафиком, в котором произошло обнаружение. • Категория объекта по базе IDS. • Название пользовательского правила IDS, по которому было выполнено обнаружение. • Тело HTTP-запроса. • Список обнаруженных объектов.	
Если обнаружение создано в результате проверки технологией URL Reputation, на сервере может храниться следующая информация: • Имя компьютера, с которого были отправлены данные. • Имя компьютера, получившего данные. • IP-адрес компьютера, с которого были отправлены данные. • IP-адрес компьютера, получившего данные. • URI переданного ресурса. • Информация о прокси-сервере. • Уникальный идентификатор сообщения электронной почты. • Адреса электронной почты отправителя и получателей сообщения (включая получателей копии и скрытой копии сообщения). • Тема сообщения электронной почты. • Дата и время поступления сообщения в Kaspersky Anti Targeted Attack Platform, с точностью до секунд. • Список обнаруженных объектов. • Время сетевого соединения. • URL-адрес сетевого соединения. • User agent.	
Если обнаружение создано в результате проверки компонентом Sandbox, на сервере может храниться следующая информация: • Версия баз приложения, с помощью которых было выполнено обнаружение. • Категория обнаруженного объекта. • Имена обнаруженных объектов. • MD5-хеши обнаруженных объектов. • Информация об обнаруженных объектах.	
Если обнаружение создано в результате проверки технологией Anti-Malware Engine, на сервере может храниться следующая информация: • Версии баз компонентов Kaspersky Anti Targeted Attack Platform, с помощью которых было выполнено обнаружение. • Категория обнаруженного объекта. • Список обнаруженных объектов. • MD5-хеш обнаруженных объектов. • Дополнительная информация об обнаружении.	
Если обнаружение создано в результате обнаружения DNS-активности, на сервере может храниться следующая информация: • Данные DNS-запроса. • Содержание ответа DNS-сервера на запрос. • Список запрашиваемых хостов.	

Тип данных	Место и срок хранения
Если обнаружение создано в результате проверки в соответствии с пользовательскими правилами IOC или TAA (IOA), на сервере может храниться следующая информация: • Дата и время выполнения проверки. • Идентификаторы компьютеров, на которых выполнено обнаружение. • Имя правила TAA (IOA). • Имя IOC-файла. • Информация об обнаруженных объектах. • Список хостов с компонентом Endpoint Agent.	
Если обнаружение создано при проверке с помощью правил YARA, на сервере может храниться следующая информация: • Версия правил YARA, с помощью которых было выполнено обнаружение. • Категория обнаруженного объекта. • Имя обнаруженного объекта. • MD5-хеш обнаруженного объекта. • Дата и время обнаружения объекта. • Дополнительная информация об алерте.	
Если обнаружение создано в результате проверки сообщения электронной почты, на сервере может храниться следующая информация: • Адреса электронной почты отправителя и получателей сообщения, копии и скрытой копии сообщения. • Тема сообщения электронной почты. • Дата и время поступления сообщения в Kaspersky Anti Targeted Attack Platform, с точностью до секунд. • Все служебные заголовки сообщения (так, как они выглядят в сообщении).	Если Central Node установлен на сервере, информация об обнаружениях хранится на сервере Central Node в директории /data. Если Central Node установлен в виде кластера, информация об обнаружениях хранится в хранилище ceph. Данные хранятся бессрочно.
Если обнаружение создано в результате повторного сканирования, на сервере может храниться следующая информация: • Имя файла.	

Данные в событиях

Данные пользователя могут содержаться в событиях. Если Central Node установлен на сервере, информация о произошедших событиях хранится в директории `/data`. Если Central Node установлен в виде кластера, информация хранится в хранилище ceph.

Данные ротируются по мере заполнения диска.

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Anti Targeted Attack Platform не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлено приложение, к персональным данным других пользователей любыми системными средствами на его усмотрение.

Данные о событиях могут содержать следующую информацию:

- Имя компьютера, на котором произошло событие.
- Уникальный идентификатор компьютера с компонентом Endpoint Agent.
- Имя пользователя, под учетной записью которого произошло событие.

- Имя группы, в которую входит пользователь.
- Тип события.
- Время события.
- Информация о файле, для которого записано событие: имя, путь, полное имя.
- MD5- и SHA256-хеш файла.
- Время создания файла.
- Время изменения файла.
- Флаги прав доступа к файлу.
- Переменные окружения процесса.
- Параметры командной строки.
- Текст команды, введенный в командную строку.
- Локальный IP-адрес адаптера.
- Локальный порт.
- Имя удаленного хоста.
- IP-адрес удаленного хоста.
- Порт на удаленном хосте.
- URL- и IP-адреса посещенных веб-сайтов, а также ссылки с этих веб-сайтов.
- Протокол сетевого соединения.
- Метод HTTP-запроса.
- Заголовок HTTP-запроса.
- Информация о переменных реестра Windows: путь к переменной, имя переменной, значение переменной.
- Содержание скрипта или двоичного файла, переданного на AMSI-проверку.
- Информация о событии в журнале Windows: тип события, идентификатор типа события, идентификатор события, пользователь, под учетной записью которого событие записано в журнал, полный текст события из журнала событий Windows в формате XML.

Данные в отчетах

Если компонент Central Node установлен на сервере, данные отчетов хранятся в директории `/data` бессрочно. Если Central Node установлен в виде кластера, информация хранится в хранилище ceph бессрочно.

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Anti Targeted Attack Platform не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлено приложение, к персональным данным других пользователей любыми системными средствами на его усмотрение.

В отчетах может содержаться следующая информация:

- Дата создания отчета.
- Период, за который сформирован отчет.
- Идентификатор учетной записи пользователя, сформировавшего отчет.
- Статус отчета.
- Компоненты Central Node, по которым был сформирован отчет.
- Текст отчета в виде HTML-кода.
- Описание отчета.
- Имя шаблона, на основе которого создан отчет.
- Идентификатор тенанта.

Если используется функциональность NDR, в отчетах может содержаться следующая информация:

- Имя шаблона, на основе которого создан отчет.
- Дата создания отчета.
- Идентификатор учетной записи пользователя, сформировавшего отчет.
- Текст отчета в виде HTML-кода.

Данные об объектах в Хранилище и на карантине

Если компонент Central Node установлен на сервере, данные об объектах в Хранилище и на карантине хранятся в директории /data бессрочно. Если Central Node установлен в виде кластера, информация хранится в хранилище ceph бессрочно.

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Anti Targeted Attack Platform не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлено приложение, к персональным данным других пользователей любыми системными средствами на его усмотрение.

Данные об объектах в Хранилище и на карантине могут содержать следующую информацию:

- Имя объекта.
- Путь к объекту на компьютере с компонентом Endpoint Agent.
- MD5-, SHA256-хеш файла.
- Размер файла.
- Идентификатор пользователя, поместившего объект на карантин.
- Идентификатор пользователя, поместившего объект в Хранилище.
- IP-адрес компьютера, на котором хранится объект, помещенный на карантин.
- Имя компьютера, на котором хранится объект, помещенный на карантин.
- Уникальный идентификатор компьютера, на котором хранится объект, помещенный на карантин.
- Идентификатор правила TAA (IOA), в соответствии с которым было выполнено обнаружение.
- Категория обнаруженного объекта.
- Результаты проверки объекта с помощью отдельных модулей и технологий приложения.
- Время загрузки файла.
- Метаинформация о проверенных файлах и источниках получения.
- Результирующий статус об объекте в Хранилище.

Данные компонента Sandbox

На время обработки тело переданного компонентом Central Node файла сохраняется в открытом виде на сервере с компонентом Sandbox. Во время обработки доступ к переданному файлу может получить администратор сервера в режиме Technical Support Mode. Проверенный файл удаляется специальным скриптом по расписанию. По умолчанию один раз в 60 минут.

Информация о данных, хранящихся на сервере с компонентом Sandbox, приведена в таблице ниже.

Данные, хранящиеся на сервере с компонентом Sandbox

Состав данных	Место хранения	Срок хранения	Доступ
Проверяемые файлы	`/var/opt/kaspersky/sandbox/library/`	После получения компонентом Central Node результатов проверки или до автоматического удаления, но не более 24 часов.	Доступ пользовател администратором с операционной систе
Результат проверки файлов	• `/var/opt/kaspersky/sandbox/library/` • `/tmp/`	После получения компонентом Central Node результатов проверки или до автоматического удаления, но не более 24 часов.	Доступ пользовател администратором с операционной систе
Параметры задач	• `/var/opt/kaspersky/sandbox/library/` • база данных компонента Sandbox	После получения компонентом Central Node результатов проверки или до автоматического удаления, но не более 24 часов в директории `/var/opt/kaspersky/sandbox/library/`. В базе данных компонента Sandbox до 90 дней.	Доступ пользовател `/var/opt/kaspersk` определяется адми помощью средств о Для аутентификации данных требуется па базы данных имеют т от имени которых за базы данных, и польз root. Доступ осуществляе шифрованному кана
Файлы трассировки	`/var/log/kaspersky/sandbox/`	До 21 дня.	Доступ пользовател администратором с операционной систе Действия с файлами доступны только для пользователей. Информация о дейст трассировки сохран событий приложени
Настройки источника обновлений	`/var/opt/kaspersky/apt-updater`	До изменения или удаления.	Доступ пользовател администратором с операционной систе
Настройки минимальной длины пароля	`/var/opt/kaspersky/apt-config-ram-common/validator.conf`	До изменения или удаления.	Доступ пользовател администратором с операционной систе
Виртуальные машины	`/vm`	До изменения или удаления.	Доступ пользовател администратором с операционной систе
Загруженные образы операционных систем и приложений в формате iso	`/var/opt/kaspersky/sandbox/custom_images/iso`	До изменения или удаления.	Доступ пользовател администратором с операционной систе

Данные, пересылаемые между компонентами приложения

Central Node и компонент Endpoint Agent

Приложения, которые выступают в роли компонента Endpoint Agent, отправляют на компонент Central Node отчеты о выполнении задач, информацию о событиях и обнаружениях, произошедших на компьютерах с этими приложениями, а также информацию о терминальных сессиях.

Если связь с компонентом Central Node отсутствует, все данные, предназначенные для отправки, накапливаются до тех пор, пока они не будут отправлены на компонент Central Node или приложение, которое выступает в роли компонента Endpoint Agent, не будет удалено с компьютера, но не более 21 дня.

Общие сведения для всех событий

Если событие произошло на компьютере пользователя, приложения отправляют следующие данные в базу событий:

- Тип события.
- Время события.
- Идентификатор события.
- Версия схемы события.
- Время обработки события сервером Central Node.
- Учетная запись пользователя, от имени которой было совершено событие.
- Имя хоста, на котором произошло событие.
- IP-адрес хоста.
- Тип операционной системы, установленной на хосте.
- Семейство ОС.
- Имя ОС.
- Версия ОС.

- IP-адрес сетевого адаптера, через который приложение, используемое в роли компонента Endpoint Agent, подключается к серверу Central Node или Sensor.
- Версия приложения, которое используется в роли компонента Endpoint Agent.
- Дата последнего обновления баз KBD.
- Дата последнего обновления баз SW.
- Дата индекса.
- При разметке событий по правилам TAA(IOA) передается следующая информация:
  - Идентификатор сработавшего индикатора атаки.
  - Заключение сработавшего индикатора атаки.
  - Источник сработавшего индикатора атаки.
  - Версия сработавшего индикатора атаки.
  - Код техники MITRE.
  - Код тактики MITRE.
  - Важность обнаружения в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".
  - Надежность обнаружения в зависимости от вероятности ложных срабатываний правила.

Central Node и Kaspersky Endpoint Security для Windows

Если событие произошло на компьютере пользователя, приложение отправляет следующие данные в базу событий:

1. Событие изменения файла.
   - Сведения о процессе, создавшем файл: имя файла процесса, MD5-, SHA256-хеш файла процесса.
   - Сведения о созданном или измененном файле: имя, путь, полное имя, тип, MD5-хеш, SHA256-хеш, дата создания, дата изменения, атрибуты, дата изменения атрибутов, размер, атрибуты,идентификатор зоны, имя приложения файла, производитель, имя организации, выпустившей цифровой сертификат, описание, результат проверки цифровой подписи, время цифровой подписи, исходное имя, имя до изменения, путь до изменения, полное имя до изменения.
   - Сведения о файле, на который была создана ссылка: MD5-хеш, SHA256-хеш, дата создания, дата изменения, атрибуты, дата изменения атрибутов, размер, тип, идентификатор зоны, имя приложения файла, исходное имя, имя организации, выпустившей цифровой сертификат, описание, субъект подписи, результат проверки цифровой подписи, время цифровой подписи, полное имя файла-ссылки.

2. Событие мониторинга реестра.

- Сведения о процессе, изменившем реестр: ID процесса, имя файла процесса, MD5-, SHA256-хеш файла процесса.
- Путь к ключу реестра.
- Имя параметра реестра.
- Значение параметра реестра.
- Тип параметра реестра.
- Предыдущий путь к ключу реестра.
- Предыдущее значение параметра реестра.
- Предыдущий тип параметра реестра.
- Тип операции с реестром.
- Путь к файлу, в который был сохранен ключ реестра.

3. Событие загрузки драйвера.

- Имя файла.
- Исходное имя файла.
- Путь к файлу.
- Полное имя файла.
- MD5-, SHA256-хеш файла.
- Размер файла.
- Дата создания и изменения файла.
- Дата изменения атрибутов файла.
- Размер файла.
- Тип файла.
- Атрибуты файла.
- Идентификатор зоны файла.
- Производитель файла.
- Описание файла.
- Имя организации, выпустившей цифровой сертификат.

- Субъект подписи.
- Результат проверки цифровой подписи.
- Время цифровой подписи.
- URL-адрес, с которого был получен файл.
- Мета-данные о письме, из которого был получен файл.

4. Событие открытия порта на прослушивание.

- Сведения о процессе, открывшем порт на прослушивание: имя файла процесса, MD5-, SHA256-хеш файла процесса.
- Номер порта.
- IP-адрес адаптера.
- Статус операции.

5. Событие удаленного соединения.

- Сведения о локальном компьютере: IP-адрес, номер порта.
- Сведения об удаленном компьютере: IP-адрес, порт, номер порта, FQDN.
- Сведения о TLS-шифровании соединения: версия протокола, SNI, зашифрованный SNI, MD5-хеш файла сертификата, SHA1-хеш файла сертификата, имя издателя сертификата, серийный номер сертификата, результат проверки сертификата, срок действия сертификата, Ja3, Ja3s, MD5-хеш Ja3, MD5-хеш Ja3s, тип разъема (socket).
- Номер LANA.
- HTTP-метод.
- URL-адрес, по которому был совершен переход.
- Статус процесса.
- Направление соединения.

6. Событие DNS-поиска.

- IP-адрес запрашиваемого DNS-сервера в формате IPv4.
- Бинарная маска выполняемого DNS-запроса.
- Код ошибки DNS-ответа.
- Идентификатор типа DNS-запроса.
- Имя домена, для которого требуется разрешить запись DNS.
- Дата DNS-ответа.

7. Событие LDAP.

   - Область поиска.
   - Фильтр поискового запроса.
   - Атрибуты, заданные в запросе в качестве возвращаемых.
   - Путь к LDAP-контейнеру, в котором будет производиться поиск.

8. Событие запуска процесса.

   Сведения о файлах родительского и прародительского процессов, процессов-загрузчиков, процессов-создателей, запущенных процессах: имя, путь, полное имя, MD5-хеш, SHA256-хеш, дата и время создания, дата и время изменения, атрибуты, дата и время изменения атрибутов, размер, идентификатор зоны,производитель, имя организации, выпустившей цифровой сертификат, описание, исходное имя, субъект цифровой подписи, результат проверки цифровой подписи, дата и время цифровой подписи, версия файла, тип входа в систему, идентификатор сессии входа, тип учетной записи, имя пользователя, идентификатор учетной записи, IP-адрес компьютера, с которого был совершен вход, уровень целостности, идентификатор процесса, текущая директория.

9. Событие остановки процесса.

   - Сведения о файле процесса: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, время завершения процесса.
   - Уникальный идентификатор процесса.
   - Параметры запуска процесса.
   - Сведения о родительском процессе: путь к файлу, UniquePID, MD5- и SHA256-хеш, параметры запуска.

10. Событие доступа к процессу.

    - Тип операции.
    - Права доступа к процессу.
    - Стек вызовов.
    - Сведения о файле процесса-реципиента и файле процесса, из которого был продублирован дескриптор: имя, путь, полный путь, MD5-и SHA256-хеш, дата и время создания, дата и время изменения, дата и время изменения атрибутов, размер, уникальный идентификатор, системный идентификатор, параметры командной строки, URL-адрес, с которого был получен файл, мета-данные о письме, из которого был получен файл.

11. Событие загрузки модуля.

    - Сведения о файле, загрузившем модуль: UniquePID, имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла.
    - Имя DLL.
    - Путь к DLL.
    - Полное имя DLL.

- MD5-, SHA256-хеш DLL.
- Размер DLL.
- Атрибуты DLL.
- Идентификатор зоны DLL.
- Имя приложения DLL.
- Исходное имя DLL.
- Дата создания и изменения DLL.
- Имя организации, выпустившей цифровой сертификат DLL.
- Результат проверки цифровой подписи DLL.
- Дата цифровой подписи DLL.
- Путь к замененной DLL.
- Тип файла DLL.
- URL-адрес. с которого был получен файл.
- Мета-данные об электронном письме, из которого был получен файл.
- Имя сборки .NET.
- Флаги сборки .NET.
- Флаги модуля .NET.

12. Событие блокирования запуска процесса.

    - Сведения о файле, который пытались выполнить: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, дата создания и изменения файла.
    - Параметры командной строки.

13. Событие блокирования запуска файла.

    - Сведения о файле, который пытались открыть: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, тип контрольной суммы, по которой произведена блокировка, размер файла (0 – MD5, !=0 – SHA256, для поиска не используется), URL-адрес сайта, с которого был скачан запускаемый файл, метаданные о письме, из вложения которого был скачан файл.
    - Сведения об исполняемом файле: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, дата создания и изменения файла.
    - Сведения о родительском процессе: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, PID, UniquePID.

14. Событие открытия именованного канала и подключения к нему.

- Имя файла процесса, создавшего именованный канал или подключившегося к нему.
- Тип операции с каналом.

15. Событие обнаружения угрозы и результата обработки обнаружения.

- Имя обнаруженного объекта.
- MD5-хеш обнаруженного объекта.
- SHA256-хеш обнаруженного объекта.
- Тип обнаруженного объекта.
- Результат проверки.
- Идентификатор записи в базах приложения.
- Версия баз приложения, с помощью которых было выполнено обнаружение.
- Режим обработки объекта.
- Категория обнаруженного объекта (например, название вируса).
- Протокол.
- IP-адрес локального компьютера в формате IPv4 или IPv6.
- Номер локального порта.
- IP-адрес удаленного компьютера в формате IPv4 или IPv6.
- Номер удаленного порта.
- URL-адрес, с которого был получен файл.
- Электронный адрес отправителя, если файл был получен из электронного письма.
- Полное имя, MD5-, SHA256-хеш загрузчика файла.
- Уникальный идентификатор процесса.
- PID процесса, отображаемый в диспетчере задач Windows.
- Командная строка запуска процесса.
- Причина ошибки при обработке объекта.
- Содержание и тип скрипта, проверенного с помощью AMSI.

16. Событие операции с USB-устройством:

- Тип операции с устройством.
- Тип подключенного устройства
- ID подключенного устройства.
- Имя подключенного устройства.
- Путь к подключенному устройству.
- Является ли подключенное устройство системным диском.

17. Событие запуска службы WMI.

- Тип операции.
- Признак удаленного запуска службы WMI.
- Имя компьютера, на котором была запущена служба WMI.
- Имя пользователя, под учетной записью которого была запущена служба WMI.
- Пространство имен WMI.
- Имя фильтра потребителя событий.
- Имя созданного потребителя событий.
- Исходный код потребителя событий.

18. Событие AMSI-проверки.

- Содержание скрипта, проверенного с помощью AMSI.
- Тип содержимого, переданного на проверку скрипта.
- Имя переданного на проверку скрипта.
- MD5-хеш файла скрипта.
- SHA256-хеш файла скрипта.

19. Событие внедрения кода.

- Сведения о процессе-реципиенте: имя приложения, полное имя приложения, путь к приложению, MD5-хеш файла, SHA256-хеш файла, URL-адрес, с которого был скачан файл, метаданные о письме, из вложения которого был скачан файл, уникальный идентификатор приложения, системный идентификатор приложения, командная строка запуска, имя DLL процесса, путь к DLL процесса, адрес процесса в адресном пространстве.
- Метод внедрения.
- Измененная командная строка запуска процесса.

- Параметры системного вызова.
- Стек API-вызовов на момент перехвата функции, связанной с внедрением.

20. Событие интерпретированного запуска файла.

    Сведения об интерпретированном файле: имя, путь, полное имя, MD5, SHA256, дата и время создания файла, дата и время изменения файла, размер, тип, атрибуты, дата и время изменения атрибутов, оригинальное имя, описание, идентификатор зоны, имя организации, выпустившей цифровой сертификат, результат проверки цифровой подписи, дата и время цифровой подписи, субъект цифровой подписи, URL-адрес, с которого был получен файл, метаданные о письме, из вложения которого был скачан файл.

21. Событие в журнале ОС.

    - Время события, хост, на котором произошло событие, имя учетной записи пользователя.
    - ID события.
    - Имя журнала/канала.
    - ID события в журнале.
    - Имя провайдера.
    - Подтип события аутентификации.
    - Имя домена.
    - Удаленный IP-адрес.

- Поля заголовка события: ProviderName, EventId, Version, Level, Task, Opcode, Keywords, TimeCreatedSystemTime, EventRecordId, CorellationActivityId, ExecutionProcessID, ThreadID, Channel, Computer.

- Поля тела события: AccessList, AccessFiles mask, AccountExpires, AllowedToDelegateTo, Application, AuditPolicyChanges, AuthenticationPackageName, CategoryId, CommandLine, DisplayName, Dummy, ElevatedToken, EventCode, EventProcessingFailure, FailureReason, FilterRTID, HandleId, HomeDirectory, HomePath, ImpersonationLevel, IpAddress, IpPort, KeyLength, LayerName, LayerRTID, LmPackageName, LogonGuid, LogonHours, LogonProcessName, LogonType, MandatoryLabel, MemberName, MemberSid, NewProcessId, NewProcessName, NewUacValue, NewValue, NewValueType, ObjectName, ObjectServer, ObjectType, ObjectValueName, OldUacValue, OldValue, OldValueType, OperationType, PackageName, ParentProcessName, PasswordLastSet, PrimaryGroupId, PriviledgeList, ProcessId, ProcessName, ProfileChanged, ProfilePath, Protocol, PublisherId, ResourceAttributes, RestrictedAdminMode, SamAccountName, ScriptPath, ServiceAccount, ServiceFileName, ServiceName, ServiceStartType, ServiceType, SettingType, SettingValue, ShareLocalPath, ShareName, SidHistory, SourceAddress, SourcePort, Status, SubcategoryGuid, SubcategoryId, SubjectDomainName, SubjectLogonId, SubjectUserName, SubjectUserSid, SubStatus, TargetDomainName, TargetLinkedLogonId, TargetLogonId, TargetOutboundDomainName, TargetOutboundUserName, TargetUserName, TargetUserSid, TaskContent, TaskName, TokenElevationType, TransmittedServices, UserAccountControl, UserParameters, UserPrincipalName, UserWorkstations, VirtualAccount, Workstation, WorkstationName, System, SystemProvider, SystemProviderName, SystemProviderGuid, SystemProviderEventSourceName, SystemEventID, SystemEventIDQualifiers, SystemEventRecordID, SystemChannel, SystemTask, SystemOpcode, SystemVersion, SystemLevel, SystemKeywords, SystemTimeCreated, SystemTimeCreatedSystemTime, SystemCorrelation, SystemCorrelationActivityID, SystemExecution, SystemExecutionProcessID, SystemExecutionThreadID, SystemComputer, SystemSecurity, SystemSecurityUserID, UserData, UserDataEventProcessingFailure, UserDataEventProcessingFailureError, UserDataEventProcessingFailureErrorCode, UserDataEventProcessingFailureEventID, UserDataEventProcessingFailurePublisherID, UserDataLogFileCleared, UserDataLogFileClearedSubjectUserSid, UserDataLogFileClearedSubjectUserName, UserDataLogFileClearedSubjectDomainName, UserDataLogFileClearedSubjectLogonId, UserDataFileIsFull, UserDataOperationStartedOperationalProviderName, UserDataOperationStartedOperationalCode, UserDataOperationStartedOperationalHostProcess, UserDataOperationStartedOperationalProcessID, UserDataOperationStartedOperationalProviderPath, UserDataServiceShutdown, UserDataOperationClientFailure, UserDataOperationClientFailureId, UserDataOperationClientFailureClientMachine, UserDataOperationClientFailureUser, UserDataOperationClientFailureClientProcessId, UserDataOperationClientFailureComponent, UserDataOperationClientFailureOperation, UserDataOperationClientFailureResultCode, UserDataOperationClientFailurePossibleCause, EventData, EventDataData, EventDataDataTaskName, EventDataDataPrivilegeList, EventDataDataAttributeLDAPDisplayName, EventDataDataOperationType, EventDataDataObjectClass, EventDataDataAttributeValue, EventDataDataObjectDN, EventDataDataRelativeTargetName, EventDataDataWorkstationName, EventDataDataServiceName, EventDataDataAllowedToDelegateTo, EventDataDataUserAccountControl, EventDataDataProfileChanged, EventDataDataRuleId, EventDataDataRuleName, EventDataDataSubjectUserSid, EventDataDataSubjectUserName, EventDataDataSubjectDomainName, EventDataDataSubjectLogonId, EventDataDataPreviousTime, EventDataDataNewTime, EventDataDataProcessId, EventDataDataProcessName, EventDataDataObjectType, EventDataDataObjectName, EventDataDataAccessList, EventDataDataAccessMask, EventDataDataServiceFileName, EventDataDataServiceType, EventDataDataServiceStartType, EventDataDataServiceAccount, EventDataDataDomainName, EventDataDataDomainSid, EventDataDataTdoType, EventDataDataTdoDirection, EventDataDataTdoAttributes, EventDataDataSidFilteringEnabled, EventDataDataTargetSid, EventDataDataAccessGranted, EventDataDataTargetUserName, EventDataDataTargetDomainName, EventDataDataSamAccountName, EventDataDataSidHistory, EventDataDataDomainPolicyChanged, EventDataDataMinPasswordAge, EventDataDataMaxPasswordAge, EventDataDataForceLogoff, EventDataDataLockoutThreshold, EventDataDataLockoutObservationWindow, EventDataDataLockoutDuration, EventDataDataProperties, EventDataDataPasswordProperties, EventDataDataMinPasswordLength, EventDataDataPasswordHistoryLength, EventDataDataMachineAccountQuota, EventDataDataMixedDomainMode, EventDataDataDomainBehaviorVersion,

EventDataDataOemInformation, EventDataDataGroupTypeChange, EventDataDataLogonGuid,
EventDataDataTargetUserSid, EventDataDataTargetLogonId, EventDataDataTargetLogonGuid,
EventDataDataSidList, EventDataDataWorkstation, EventDataDataStatus, EventDataDataCallerProcessId,
EventDataDataCallerProcessName, EventDataDataForestRoot, EventDataDataForestRootSid,
EventDataDataOperationId, EventDataDataEntryType, EventDataDataFlags, EventDataDataTopLevelName,
EventDataDataDnsName, EventDataDataNetbiosName, EventDataDataAuditSourceName,
EventDataDataEventSourceId, EventDataDataErrorCode, EventDataDataGPOList,
EventDataDataDestinationDRA, EventDataDataSourceDRA, EventDataDataSourceAddr,
EventDataDataNamingContext, EventDataDataOptions, EventDataDataStatusCode,
EventDataDataSessionID, EventDataDataStartUSN, EventDataDataPackageName,
EventDataDataAuthenticationPackageName, EventDataDataFailureReason, EventDataDataSubStatus,
EventDataDataCategoryId, EventDataDataSubcategoryGuid, EventDataDataAuditPolicyChanges,
EventDataDataUserPrincipalName, EventDataDataHomeDirectory, EventDataDataHomePath,
EventDataDataScriptPath, EventDataDataProfilePath, EventDataDataUserWorkstations,
EventDataDataPasswordLastSet, EventDataDataAccountExpires, EventDataDataPrimaryGroupId,
EventDataDataOldUacValue, EventDataDataNewUacValue, EventDataDataUserParameters,
EventDataDataLogonHours, EventDataDataMemberName, EventDataDataMemberSid,
EventDataDataServiceSid, EventDataDataTicketOptions, EventDataDataTicketEncryptionType,
EventDataDataPreAuthType, EventDataDataCertIssuerName, EventDataDataCertSerialNumber,
EventDataDataCertThumbprint, EventDataDataSettingType, EventDataDataSettingValue,
EventDataDataShareName, EventDataDataShareLocalPath, EventDataDataApplication,
EventDataDataSourceAddress, EventDataDataSourcePort, EventDataDataProtocol,
EventDataDataFilterRTID, EventDataDataLayerName, EventDataDataLayerRTID, EventDataDataLogonType,
EventDataDataLogonProcessName, EventDataDataTransmittedServices, EventDataDataLmPackageName,
EventDataDataKeyLength, EventDataDataIpAddress, EventDataDataIpPort,
EventDataDataImpersonationLevel, EventDataDataRestrictedAdminMode,
EventDataDataTargetOutboundUserName, EventDataDataTargetOutboundDomainName,
EventDataDataVirtualAccount, EventDataDataTargetLinkedLogonId, EventDataDataElevatedToken,
EventDataDataTaskContentNew, EventDataDataTaskContentNewTask,
EventDataDataTaskContentNewTaskRegistrationInfo,
EventDataDataTaskContentNewTaskRegistrationInfoDate,
EventDataDataTaskContentNewTaskRegistrationInfoAuthor, EventDataDataTaskContentNewTaskTriggers,
EventDataDataTaskContentNewTaskPrincipals, EventDataDataTaskContentNewTaskPrincipalsPrincipal,
EventDataDataTaskContentNewTaskPrincipalsPrincipalid,
EventDataDataTaskContentNewTaskPrincipalsPrincipalRunLevel,
EventDataDataTaskContentNewTaskPrincipalsPrincipalUserId,
EventDataDataTaskContentNewTaskPrincipalsPrincipalLogonType,
EventDataDataTaskContentNewTaskSettings,
EventDataDataTaskContentNewTaskSettingsMultipleInstancesPolicy,
EventDataDataTaskContentNewTaskSettingsDisallowStartIfOnBatteries,
EventDataDataTaskContentNewTaskSettingsStopIfGoingOnBatteries,
EventDataDataTaskContentNewTaskSettingsAllowHardTerminate,
EventDataDataTaskContentNewTaskSettingsStartWhenAvailable,
EventDataDataTaskContentNewTaskSettingsRunOnlyIfNetworkAvailable,
EventDataDataTaskContentNewTaskSettingsIdleSettings,
EventDataDataTaskContentNewTaskSettingsIdleSettingsStopOnIdleEnd,
EventDataDataTaskContentNewTaskSettingsIdleSettingsRestartOnIdle,
EventDataDataTaskContentNewTaskSettingsAllowStartOnDemand,
EventDataDataTaskContentNewTaskSettingsEnabled,
EventDataDataTaskContentNewTaskSettingsHidden,
EventDataDataTaskContentNewTaskSettingsRunOnlyIfIdle,
EventDataDataTaskContentNewTaskSettingsWakeToRun,
EventDataDataTaskContentNewTaskSettingsExecutionTimeLimit,
EventDataDataTaskContentNewTaskSettingsPriority, EventDataDataTaskContentNewTaskActions,
EventDataDataTaskContentNewTaskActionsContext, EventDataDataTaskContentNewTaskActionsExec,
EventDataDataTaskContentNewTaskActionsExecCommand, EventDataDataOldSd, EventDataDataNewSd,
EventDataDataNotificationPackageName, EventDataDataSecurityPackageName, EventDataDataStopTime,
EventDataDataContextInfo, EventDataDataUserData, EventDataDataPayload,

EventDataDataOpCorrelationID, EventDataDataAppCorrelationID, EventDataDataDSName,
EventDataDataDSType, EventDataDataObjectGUID, EventDataDataFileName, EventDataDataLinkName,
EventDataDataTransactionId, EventDataDataOldObjectDN, EventDataDataNewObjectDN,
EventDataDatabcdCCID, EventDataDatabMaxSlotIndex, EventDataDatabVoltageSupport,
EventDataDatadwProtocols, EventDataDatadwDefaultClock, EventDataDatadwMaximumClock,
EventDataDatabNumClockSupported, EventDataDatadwDataRate, EventDataDatadwMaxDataRate,
EventDataDatabNumDataRateSupported, EventDataDatadwMaxIFSD, EventDataDatadwSyncProtocols,
EventDataDatadwMechanical, EventDataDatadwFeatures, EventDataDataObjectValueName,
EventDataDataHandleId, EventDataDataOldValueType, EventDataDataOldValue,
EventDataDataNewValueType, EventDataDataNewValue, EventDataDataSubjectUserDomainName,
EventDataDataObjectCollectionName, EventDataDataObjectIdentifyingProperties,
EventDataDataObjectProperties, EventDataDataparam, EventDataDataCVEID,
EventDataDataAdditionalDetails, EventDataDataObjectServer, EventDataDataTaskContent,
EventDataDataTaskContentTask, EventDataDataTaskContentTaskRegistrationInfo,
EventDataDataTaskContentTaskRegistrationInfoDate,
EventDataDataTaskContentTaskRegistrationInfoAuthor, EventDataDataTaskContentTaskTriggers,
EventDataDataTaskContentTaskPrincipals, EventDataDataTaskContentTaskPrincipalsPrincipal,
EventDataDataTaskContentTaskPrincipalsPrincipalid,
EventDataDataTaskContentTaskPrincipalsPrincipalRunLevel,
EventDataDataTaskContentTaskPrincipalsPrincipalUserId,
EventDataDataTaskContentTaskPrincipalsPrincipalLogonType, EventDataDataTaskContentTaskSettings,
EventDataDataTaskContentTaskSettingsMultipleInstancesPolicy,
EventDataDataTaskContentTaskSettingsDisallowStartIfOnBatteries,
EventDataDataTaskContentTaskSettingsStopIfGoingOnBatteries,
EventDataDataTaskContentTaskSettingsAllowHardTerminate,
EventDataDataTaskContentTaskSettingsStartWhenAvailable,
EventDataDataTaskContentTaskSettingsRunOnlyIfNetworkAvailable,
EventDataDataTaskContentTaskSettingsIdleSettings,
EventDataDataTaskContentTaskSettingsIdleSettingsStopOnIdleEnd,
EventDataDataTaskContentTaskSettingsIdleSettingsRestartOnIdle,
EventDataDataTaskContentTaskSettingsAllowStartOnDemand,
EventDataDataTaskContentTaskSettingsEnabled, EventDataDataTaskContentTaskSettingsHidden,
EventDataDataTaskContentTaskSettingsRunOnlyIfIdle,
EventDataDataTaskContentTaskSettingsWakeToRun,
EventDataDataTaskContentTaskSettingsExecutionTimeLimit,
EventDataDataTaskContentTaskSettingsPriority, EventDataDataTaskContentTaskActions,
EventDataDataTaskContentTaskActionsContext, EventDataDataTaskContentTaskActionsExec,
EventDataDataTaskContentTaskActionsExecCommand, EventDataDataOldTargetUserName,
EventDataDataNewTargetUserName, EventDataDataDeviceId, EventDataDataDeviceDescription,
EventDataDataClassId, EventDataDataClassName, EventDataDataVendorIds,
EventDataDataCompatibleIds, EventDataDataLocationInformation, EventDataDataAccountName,
EventDataDataAccountDomain, EventDataDataLogonID, EventDataDataSessionName,
EventDataDataClientName, EventDataDataClientAddress, EventDataDataMajorVersion,
EventDataDataMinorVersion, EventDataDataBuildVersion, EventDataDataQfeVersion,
EventDataDataServiceVersion, EventDataDataBootMode, EventDataDataStartTime,
EventDataDataOldRemark, EventDataDataNewRemark, EventDataDataOldMaxUsers,
EventDataDataNewMaxUsers, EventDataDataOldShareFlags, EventDataDataNewShareFlags,
EventDataDataOldSD, EventDataDataNewSD, EventDataDataTreeDelete, EventDataDataPuaCount,
EventDataDataPuaPolicyId, EventDataDataResourceAttributes, EventDataDataModifiedObjectProperties,
EventDataDataDisplayName, EventDataDataDnsHostName, EventDataDataServicePrincipalNames,
EventDataDataAttributeSyntaxOID, EventDataDataDummy, EventDataDataComputerAccountChange,
EventDataDataMessageNumber, EventDataDataMessageTotal, EventDataDataScriptBlockText,
EventDataDataScriptBlockId, EventDataDataPath, EventDataDataImagePath, EventDataDataStartType,
EventDataDataAppName, EventDataDataAppVersion, EventDataDataTerminationTime,
EventDataDataExeFileName, EventDataDataReportId, EventDataDataPackageFullName,
EventDataDataPackageRelativeAppId, EventDataDataHangType, EventDataDataAccessReason,
EventDataDataTargetServerName, EventDataDataTargetInfo, EventDataDataTargetProcessId,

EventDataDataTargetProcessName, EventDataDataKerberosPolicyChange, EventDataDataSubcategoryId, EventDataBinary.

Central Node и Kaspersky Endpoint Security для Linux

Если событие произошло на компьютере пользователя, приложение отправляет следующие данные в базу событий:

1. Событие изменения файла.

   - Сведения о процессе, создавшем файл: имя файла процесса, MD5-, SHA256-хеш файла процесса.
   - Сведения о созданном или измененном файле: имя, путь, полное имя, тип, MD5-хеш, SHA256-хеш, дата создания, дата изменения, атрибуты, дата изменения атрибутов, размер, атрибуты,идентификатор зоны, имя приложения файла, производитель, имя организации, выпустившей цифровой сертификат, описание, результат проверки цифровой подписи, время цифровой подписи, исходное имя, имя до изменения, путь до изменения, полное имя до изменения.
   - Сведения о файле, на который была создана ссылка: MD5-хеш, SHA256-хеш, дата создания, дата изменения, атрибуты, дата изменения атрибутов, размер, тип, идентификатор зоны, имя приложения файла, исходное имя, имя организации, выпустившей цифровой сертификат, описание, субъект подписи, результат проверки цифровой подписи, время цифровой подписи, полное имя файла-ссылки.
   - Тип файла.
   - Идентификатор владельца.
   - Идентификатор группы-владельца.
   - Имя пользователя-владельца.
   - Имя группы-владельца.
   - URL-адрес, с которого был получен файл.
   - Мета-данные об электронном письме, из которого был получен файл.
   - Запрашиваемые флаги доступа.
   - Признак того, что файл будет удален после перезагрузки.
   - Флаги доступа к файлу.

2. Событие в журнале ОС.

   - Время события.
   - Тип события.
   - Имя события.

- Результат операции.
- Сведения о родительском процессе: путь к файлу, UniquePID, MD5-, SHA256-хеш файла процесса, команда, с помощью которой был запущен процесс.

3. Событие запуска процесса.

   Сведения о файлах родительского и прародительского процессов, процессов-загрузчиков, процессов-создателей, запущенных процессах: имя, путь, полное имя, MD5-хеш, SHA256-хеш, дата и время создания, дата и время изменения, атрибуты, дата и время изменения атрибутов, размер, идентификатор зоны, производитель, имя организации, выпустившей цифровой сертификат, описание, исходное имя, субъект цифровой подписи, результат проверки цифровой подписи, дата и время цифровой подписи, версия файла, тип входа в систему, идентификатор сессии входа, тип учетной записи, имя пользователя, идентификатор учетной записи, IP-адрес компьютера, с которого был совершен вход, уровень целостности, идентификатор процесса, текущая директория, идентификатор владельца, идентификатор группы-владельца, имя пользователя-владельца, имя группы-владельца, настоящее имя пользователя, настоящее имя группы, действующее имя группы, действующее имя пользователя, флаги прав доступа к файлу, URL-адрес, с которого был скачан файл, мета-данные о письме, из которого был получен файл, переменные окружения процесса, параметры командной строки, тип процесса.

4. Событие остановки процесса.

   - Сведения о файле процесса: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, время завершения процесса.
   - UniquePID.
   - Параметры запуска процесса.
   - Сведения о родительском процессе: путь к файлу, UniquePID, MD5-, SHA256-хеш файла процесса, параметры запуска процесса.

5. Событие обнаружения и результата его обработки.

   - Результат проверки.
   - Название обнаруженного объекта.
   - Идентификатор записи в базах приложения.
   - Время выпуска баз приложения, с помощью которых было выполнено обнаружение.
   - Режим обработки объекта.
   - Категория обнаруженного объекта (например, название вируса).
   - MD5-хеш обнаруженного объекта.
   - SHA256-хеш обнаруженного объекта.
   - Уникальный идентификатор процесса.
   - PID процесса.
   - Командная строка запуска процесса.
   - Причина ошибки при обработке объекта.

6. Событие DNS-поиска.

   - IP-адрес запрашиваемого DNS-сервера в формате IPv4.
   - Бинарная маска выполняемого DNS-запроса.
   - Код ошибки DNS-ответа.
   - Идентификатор типа DNS-запроса.
   - Имя домена, для которого требуется разрешить запись DNS.
   - Дата DNS-ответа.

7. Событие внедрения кода.

   - Сведения о процессе-реципиенте: имя приложения, полное имя приложения, путь к приложению, MD5-хеш файла, SHA256-хеш файла, URL-адрес, с которого был скачан файл, метаданные о письме, из вложения которого был скачан файл, уникальный идентификатор приложения, системный идентификатор приложения, командная строка запуска, имя DLL процесса, путь к DLL процесса, адрес процесса в адресном пространстве.
   - Метод внедрения.
   - Измененная командная строка запуска процесса.
   - Параметры системного вызова.
   - Стек API-вызовов на момент перехвата функции, связанной с внедрением.

Central Node и Kaspersky Endpoint Security для Mac

Если событие произошло на компьютере пользователя, приложение отправляет следующие данные в базу событий:

1. Событие создания файла.

   - Сведения о процессе, создавшем файл: имя файла процесса, MD5-, SHA256-хеш файла процесса.
   - Имя файла.
   - Путь к файлу.
   - Полное имя файла.
   - Тип файла.
   - MD5-, SHA256-хеш файла.
   - Дата создания и изменения файла.
   - Размер файла.

2. Событие запуска процесса.

   Сведения о файлах родительского и прародительского процессов, процессов-загрузчиков, процессов-создателей, запущенных процессах: имя, путь, полное имя, MD5-хеш, SHA256-хеш, дата и время создания, дата и время изменения, атрибуты, дата и время изменения атрибутов, размер, идентификатор зоны, производитель, имя организации, выпустившей цифровой сертификат, описание, исходное имя, субъект цифровой подписи, результат проверки цифровой подписи, дата и время цифровой подписи, версия файла, тип входа в систему, идентификатор сессии входа, тип учетной записи, имя пользователя, идентификатор учетной записи, IP-адрес компьютера, с которого был совершен вход, уровень целостности, идентификатор процесса, текущая директория, идентификатор владельца, идентификатор группы-владельца, имя пользователя-владельца, имя группы-владельца, настоящее имя пользователя, настоящее имя группы, действующее имя группы, действующее имя пользователя, флаги прав доступа к файлу, URL-адрес, с которого был скачан файл, мета-данные о письме, из которого был получен файл, переменные окружения процесса, параметры командной строки, тип процесса.

3. Событие остановки процесса.

   - Сведения о файле процесса: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, время завершения процесса.
   - UniquePID.
   - Параметры запуска процесса.
   - Сведения о родительском процессе: путь к файлу, UniquePID, MD5-, SHA256-хеш файла процесса, параметры запуска процесса.

4. Событие обнаружения угрозы и результата обработки обнаружения.

   - Результат проверки.
   - Название обнаруженного объекта.
   - Идентификатор записи в базах приложения.
   - Время выпуска баз приложения, с помощью которых было выполнено обнаружение.
   - Режим обработки объекта.
   - Категория обнаруженного объекта (например, название вируса).
   - MD5-хеш обнаруженного объекта.
   - SHA256-хеш обнаруженного объекта.
   - Уникальный идентификатор процесса.
   - PID процесса.
   - Командная строка запуска процесса.
   - Причина ошибки при обработке объекта.

Central Node и Sandbox

Компонент Central Node отправляет на компонент Sandbox файлы и URL-адреса, выделенные из сетевого или почтового трафика. Перед передачей файлы никак не изменяются. Компонент Sandbox отправляет компоненту Central Node результаты проверки.

Central Node и Sensor

Приложение может пересылать между компонентами Central Node и Sensor следующие данные:

- Файлы и сообщения электронной почты.
- Данные об обнаружениях, выполненных технологиями Intrusion Detection System и URL Reputation.
- Информацию о лицензии.
- Список данных, исключенных из проверки.
- Данные приложений, выступающих в роли компонента Endpoint Agent, если настроена интеграция с прокси-сервером.
- Базы приложения, если настроено получение обновления баз от компонента Central Node.

Серверы с ролями PCN и SCN

Если приложение работает в режиме распределенного решения, то между PCN и подключенными SCN передаются следующие данные:

- Об алертах.
- О событиях.
- О задачах.
- О политиках.
- О проверке по пользовательским правилам IOC, TAA (IOA), IDS, YARA.
- О файлах в Хранилище.
- Об учетных записях пользователей.
- О лицензии.
- Список компьютеров с компонентом Endpoint Agent.

- Объекты, помещенные в Хранилище.
- Объекты, помещенные на карантин на компьютерах с компонентом Endpoint Agent.
- Файлы, прикрепленные к обнаружениям.
- IOC- и YARA-файлы.

Данные в файлах трассировки приложения

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Anti Targeted Attack Platform не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлено приложение, к персональным данным других пользователей любыми системными средствами на его усмотрение.

В файлы трассировки могут попасть любые персональные данные пользователя или конфиденциальные данные вашей организации. Файлы хранятся в директории `/var/log/kaspersky` бессрочно.

Данные Kaspersky Endpoint Security для Windows

Вы можете посмотреть подробную информацию о передаваемых Kaspersky Endpoint Security данных в справке приложения:

- Предоставление данных в рамках Лицензионного соглашения.
- Предоставление данных при использовании Kaspersky Security Network.
- Соответствие законодательству Европейского союза (GDPR).
- Предоставление данных при использовании решений Detection and Response → Kaspersky Anti Targeted Attack Platform (EDR).

Данные Kaspersky Endpoint Security для Linux

Вы можете посмотреть подробную информацию о передаваемых Kaspersky Endpoint Security данных в справке приложения.

Данные Kaspersky Endpoint Security для Mac

Вы можете посмотреть подробную информацию о передаваемых Kaspersky Endpoint Security данных в справке приложения.

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложения Kaspersky Anti Targeted Attack Platform.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать приложение.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с приложением.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Anti Targeted Attack Platform.
- Прочитав документ /EULA/License.<язык>.

  Этот документ включен в комплект поставки приложения.
- В веб-интерфейсе приложения в разделе **Параметры**, подразделе **Лицензия** по кнопке **Лицензионное соглашение**.
- В веб-интерфейсе компонента Sandbox в меню  по ссылке **Лицензионное соглашение**.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки приложения. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку приложения и не должны использовать приложение.

О Лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- идентификатор лицензии или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о приложении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение по предоставляемой лицензии);
- дата начала срока действия лицензии;

- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Anti Targeted Attack Platform, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Объем предоставляемых услуг и срок использования приложения зависят от типа лицензии, по которой было активировано приложение.

В Kaspersky Anti Targeted Attack Platform предусмотрены следующие типы лицензий:

- NFR (not for resale / не для перепродажи) – бесплатная лицензия на определенный период, предназначенная для ознакомления с приложением и тестовых развертываний приложения.
- Коммерческая – платная лицензия, предоставляемая при приобретении приложения.

По истечении срока действия лицензии приложение продолжает работу, но с ограниченной функциональностью. Чтобы использовать приложение в режиме полной функциональности, вам нужно приобрести коммерческую лицензию или продлить срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от угроз компьютерной безопасности.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) может быть недоступна в приложении на территории США.

В текущей версии Kaspersky Anti Targeted Attack Platform функциональность приложения также зависит от типа добавленного лицензионного ключа.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать приложение в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в приложение одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в приложение.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы приложения требуется добавить другой лицензионный ключ.

В текущей версии Kaspersky Anti Targeted Attack Platform функциональность приложения зависит от типа добавленного лицензионного ключа:

- **Лицензионные ключи KATA + NDR и KEDR**. Полная функциональность приложения.
- **Лицензионный ключ KEDR**. Ограничен прием и обработка данных из сетевого и почтового трафика.
- **Лицензионный ключ KATA + NDR**. Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **Пользовательские правила**, **Хранилище**, **Активы**.
- **Лицензионный ключ KATA**. Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **Пользовательские правила**, **Хранилище**, **Активы**, ограничена функциональность сохранения и выгрузки сетевого трафика в разделе **Обработка SPAN-трафика**.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего приложение.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Anti Targeted Attack Platform или после заказа Kaspersky Anti Targeted Attack Platform с типом лицензии NFR.

Чтобы активировать приложение с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" на основе имеющегося кода активации.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky Anti Targeted Attack Platform. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Anti Targeted Attack Platform или после заказа Kaspersky Anti Targeted Attack Platform с типом лицензии NFR.

Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если код активации был потерян после активации приложения, свяжитесь с партнером "Лаборатории Касперского", у которого вы приобрели лицензию.

О подписке

Подписка на Kaspersky Anti Targeted Attack Platform – это заказ на использование решения с выбранными параметрами (дата окончания подписки, количество защищаемых устройств).

Подписка является ограниченной (например, на один год). Для продолжения работы Kaspersky Anti Targeted Attack Platform после окончания ограниченной подписки вам нужно продлить ее. Если подписка не продлена, Kaspersky Anti Targeted Attack Platform продолжает работу в режиме ограниченной функциональности.

Чтобы использовать Kaspersky Anti Targeted Attack Platform по подписке, вам нужно ввести код активации. После применения кода активации добавляется лицензионный ключ, определяющий лицензию на использование приложения по подписке. Информация о лицензионном ключе отображается в веб-интерфейсе сервера Central Node.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Anti Targeted Attack Platform.

Добавление лицензионного ключа

В режиме распределенного решения замена ключа доступна только на сервере PCN.

Вы можете добавить лицензионный ключ в Kaspersky Anti Targeted Attack Platform одним из следующих способов:

- Ввести код активации.
- Загрузить файл ключа.

Чтобы добавить лицензионный ключ в Kaspersky Anti Targeted Attack Platform с помощью кода активации:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите **Ввести код активации** в области того функционального блока, который вы хотите активировать: KATA/NDR или KEDR.

   Отобразится окно активации.
3. Введите в поле код активации, который вы получили по указанному вами адресу электронной почты.

4. Ознакомьтесь с Положением о Kaspersky Security Network и выберите один из следующих вариантов:

   - **Я согласен участвовать в KSN**. если вы согласны с условиями Положения о KSN и хотите участвовать в KSN.
   - **Я не согласен участвовать в KSN**, если вы не согласны с условиями Положения о KSN и не хотите участвовать в KSN.

   Если вы не согласны с условиями Положения, использование Kaspersky Security Network не будет включено.

5. Нажмите на кнопку **Применить**.

Лицензионный ключ будет добавлен в приложение.

Чтобы добавить лицензионный ключ в Kaspersky Anti Targeted Attack Platform с помощью файла ключа:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите **Загрузить файл ключа** в области того функционального блока, который вы хотите активировать: KATA/NDR или KEDR.

   Отобразится окно активации.
3. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
4. Выберите файл ключа, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.
5. Ознакомьтесь с Положением о Kaspersky Security Network и выберите один из следующих вариантов:

   - **Я согласен участвовать в KSN**. если вы согласны с условиями Положения о KSN и хотите участвовать в KSN.
   - **Я не согласен участвовать в KSN**, если вы не согласны с условиями Положения о KSN и не хотите участвовать в KSN.

   Если вы не согласны с условиями Положения, использование Kaspersky Security Network не будет включено.

6. Нажмите на кнопку **Применить**.

Лицензионный ключ будет добавлен в приложение.

Замена лицензионного ключа

В режиме распределенного решения замена ключа доступна только на сервере PCN.

Вы можете заменить активный лицензионный ключ в Kaspersky Anti Targeted Attack Platform другим лицензионным ключом одним из следующих способов:

- Заменить с помощью кода активации.
- Заменить с помощью файла ключа.

Чтобы заменить активный лицензионный ключ в Kaspersky Anti Targeted Attack Platform с помощью кода активации:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите **Заменить** в области того функционального блока, который вы хотите активировать: KATA/NDR или KEDR. В отобразившемся раскрывающемся списке выберете **Замена с помощью кода активации**.

   Отобразится окно замены лицензионного ключа.
3. Введите в поле код активации, который вы получили по указанному вами адресу электронной почты.
4. Ознакомьтесь с Положением о Kaspersky Security Network и выберите один из следующих вариантов:
   - **Я согласен участвовать в KSN**. если вы согласны с условиями Положения о KSN и хотите участвовать в KSN.
   - **Я не согласен участвовать в KSN**, если вы не согласны с условиями Положения о KSN и не хотите участвовать в KSN.

     Если вы не согласны с условиями Положения, использование Kaspersky Security Network не будет включено.
5. Нажмите на кнопку **Применить**.

Лицензионный ключ будет заменен.

Чтобы добавить лицензионный ключ в Kaspersky Anti Targeted Attack Platform с помощью файла ключа:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите **Заменить** в области того функционального блока, который вы хотите активировать: KATA/NDR или KEDR. В отобразившемся раскрывающемся списке выберете **Замена с помощью файла ключа**.

   Отобразится окно замены лицензионного ключа.
3. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
4. Выберите файл ключа, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

5. Ознакомьтесь с Положением о Kaspersky Security Network и выберите один из следующих вариантов:

   - **Я согласен участвовать в KSN**. если вы согласны с условиями Положения о KSN и хотите участвовать в KSN.
   - **Я не согласен участвовать в KSN**, если вы не согласны с условиями Положения о KSN и не хотите участвовать в KSN.

   > Если вы не согласны с условиями Положения, использование Kaspersky Security Network не будет включено.

6. Нажмите на кнопку **Применить**.

Лицензионный ключ будет заменен.

Удаление лицензионного ключа

> В режиме распределенного решения удаление лицензионного ключа доступна только на сервере PCN.

Вы можете удалить добавленный лицензионный ключ в Kaspersky Anti Targeted Attack Platform. После удаления лицензионного ключа приложение перейдет в режим ограниченной функциональности.

Чтобы удалить лицензионный ключ, выполните следующие действия:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите на кнопку **Удалить** в области того функционального блока, лицензионный ключ которого вы хотите удалить: KATA/NDR или KEDR.

   Отобразится окно подтверждения удаления лицензионного ключа.
3. Нажмите на кнопку **Да**.

   Окно подтверждения удаления ключа закроется.

Лицензионный ключ будет удален.

Просмотр информации о добавленных лицензионных ключах в веб-интерфейсе Central Node

В режиме распределенного решения и мультитенантности вы можете просматривать информацию о лицензии и добавленных ключах в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью администратора или пользователей веб-интерфейса приложения.

Чтобы просмотреть информацию о добавленных лицензионных ключах,

в веб-интерфейсе сервера с компонентом Central Node выберите раздел **Параметры**, подраздел **Лицензия**.

В веб-интерфейсе отображается следующая информация о лицензионном ключе KATA/NDR:

- **Серийный номер**.
- **Режим функционирования**.
- **Дата активации**.
- **Дата окончания срока действия**.
- **Осталось дней**.

В веб-интерфейсе отображается следующая информация о лицензионном ключе KEDR:

- **Серийный номер**.
- **Дата активации**.
- **Дата окончания срока действия**.
- **Осталось дней**.

За 30 дней до окончания срока действия лицензии в разделе **Мониторинг** появляется уведомление о необходимости продлить лицензию. Это уведомление отображается на всех серверах с компонентом Central Node (в режиме распределенного решения и мультитенантности – на PCN и всех подключенных SCN) для всех пользователей независимо от их роли.

Просмотр текста Лицензионного соглашения в веб-интерфейсе Central Node

В режиме распределенного решения и мультитенантности вы можете просматривать текст Лицензионного соглашения в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса приложения.

Чтобы просмотреть текст Лицензионного соглашения, выполните следующие действия в веб-интерфейсе сервера с компонентом Central Node:

1. Выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите на кнопку **Лицензионное соглашение** в правом верхнем углу рабочей области.
3. В открывшемся окне просмотрите текст Лицензионного соглашения.
4. По окончании просмотра нажмите на кнопку **Закрыть**.

Просмотр текста Политики конфиденциальности в веб-интерфейсе Central Node

В режиме распределенного решения и мультитенантности вы можете просматривать текст Политики конфиденциальности в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса приложения.

Чтобы просмотреть текст Политики конфиденциальности, выполните следующие действия в веб-интерфейсе сервера с компонентом Central Node:

1. Выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите на кнопку **Политика конфиденциальности** в правом верхнем углу рабочей области.
3. В открывшемся окне просмотрите текст Политики конфиденциальности.
4. По окончании просмотра нажмите на кнопку **Закрыть**.

Просмотр информации о стороннем коде, используемом в приложении

В режиме распределенного решения и мультитенантности вы можете просматривать информацию о стороннем коде, используемом в Kaspersky Anti Targeted Attack Platform, в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса приложения.

Чтобы просмотреть информацию о стороннем коде, выполните следующие действия в веб-интерфейсе сервера с компонентом Central Node:

1. Выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите на кнопку **Сторонний код** в правом верхнем углу рабочей области.
3. В открывшемся окне просмотрите информацию о стороннем коде.
4. По окончании просмотра нажмите на кнопку **Закрыть**.

Просмотр текста Лицензионного соглашения в веб-интерфейсе Sandbox

Чтобы просмотреть текст Лицензионного соглашения в веб-интерфейсе Sandbox:

1. Войдите в веб-интерфейс Sandbox под учетными данными, которые вы задали при установке компонента Sandbox.
2. Нажмите на ссылку с именем вашей учетной записи в нижней части окна веб-интерфейса приложения.
3. В открывшемся списке выберите **О приложении**.
4. В открывшемся окне нажмите на ссылку **Лицензионное соглашение**.
5. Просмотрите текст Лицензионного соглашения.
6. По окончании просмотра нажмите на кнопку ×.

Просмотр текста Лицензионного соглашения компонента Endpoint Agent

Вы можете просмотреть текст Лицензионного соглашения для приложения, которую используете в качестве компонента Endpoint Agent. Подробнее о том, как просмотреть текст Лицензионного соглашения, см. в справке соответствующего приложения.

О Лицензионном соглашении Kaspersky Endpoint Security для Windows

О Лицензионном соглашении Kaspersky Endpoint Security для Linux

О Лицензионном соглашении Kaspersky Endpoint Security для Mac

Режимы работы приложения в соответствии с лицензией

В Kaspersky Anti Targeted Attack Platform предусмотрены различные режимы работы приложения в зависимости от добавленных лицензионных ключей.

Без лицензии

В этом режиме приложение работает с момента установки приложения и запуска веб-интерфейса до тех пор, пока вы не добавите лицензионный ключ.

В режиме Без лицензии действуют следующие ограничения:

- Не обновляются базы приложения.
- Отсутствует подключение к базе знаний Kaspersky Security Network.
- Ограничен прием и обработка данных из сетевого и почтового трафика.
- Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **Пользовательские правила**, **Хранилище**, **Активы**.

Коммерческая работа

Для перевода в режим Коммерческая работа необходимо заменить лицензионный ключ или добавить новый ключ для коммерческой лицензии.

В этом режиме приложение:

- Обновляет базы.
- Подключается к базе знаний Kaspersky Security Network.

Снятие остальных ограничений, описанных для режима Без лицензии, в текущей версии Kaspersky Anti Targeted Attack Platform зависит от типа добавленного лицензионного ключа:

- **Лицензионные ключи KATA + NDR и KEDR**. Полная функциональность приложения.
- **Лицензионный ключ KEDR**. Ограничен прием и обработка данных из сетевого и почтового трафика.
- **Лицензионный ключ KATA + NDR**. Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **Пользовательские правила**, **Хранилище**, **Активы**.
- **Лицензионный ключ KATA**. Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **Пользовательские правила**, **Хранилище**, **Активы**, ограничена функциональность сохранения и выгрузки сетевого трафика в разделе **Обработка SPAN-трафика**.

Архитектура приложения

В состав приложения входят следующие основные компоненты:

- *Sensor*. Выполняет прием и проверку данных, а также может использоваться в качестве прокси-сервера при обмене данными между Endpoint Agent и Central Node.
- *Central Node*. Выполняет прием и проверку данных, исследование поведения объектов, а также публикацию результатов исследования в веб-интерфейс приложения.
- *Sandbox*. Запускает виртуальные образы операционных систем. Запускает файлы в этих операционных системах и отслеживает поведение файлов в каждой операционной системе для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации.
- *Endpoint Agent*. Устанавливается на рабочие станции и серверы, входящие в IT-инфраструктуру организации. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

Компонент Sensor

Компонент может быть развернут на одном сервере с Central Node (встроенный Sensor) или на отдельном сервере.

На каждом сервере Sensor работают следующие модули Kaspersky Anti Targeted Attack Platform:

- *Sensor*. Выполняет прием данных из сетевого и почтового трафика и передает их на обработку на сервер с компонентом Central Node.
- *Intrusion Detection System* (далее также *IDS*). Выполняет проверку интернет-трафика на наличие признаков вторжения в IT-инфраструктуру организации.
- *KSN*. Выполняет для Kaspersky Anti Targeted Attack Platform проверку репутации файлов и URL-адресов в базе знаний Kaspersky Security Network и предоставляет сведения о категориях веб-сайтов (например, вредоносный веб-сайт, фишинговый веб-сайт).

  *Kaspersky Security Network (*далее также *KSN)* – инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

  Если вы не хотите участвовать в KSN, вы можете использовать *Kaspersky Private Security Network* (далее также *KPSN*) – решение, позволяющее пользователям получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров.
- *URL Reputation*. Обнаруживает вредоносные, фишинговые URL-адреса и URL-адреса, которые ранее использовались злоумышленниками для целевых атак и вторжений в IT-инфраструктуру организаций.

Sensor также может использоваться в качестве прокси-сервера для соединений, исходящих от компонента Endpoint Agent.

Компонент Central Node

Компонент может быть развернут на одном сервере или в виде отказоустойчивого кластера, который состоит из серверов 2 ролей – серверов хранения и обрабатывающих серверов.

Отказоустойчивость достигается за счет дублирования данных между серверами хранения и избыточности вычислительных ресурсов: при выходе из строя одного сервера его функции выполняет другой сервер с аналогичной ролью. Kaspersky Anti Targeted Attack Platform при этом продолжает работать.

Допускается выход из строя только одного сервера кластера. При отказе нескольких серверов кластер становится неработоспособным.

На каждом сервере или кластере с компонентом Central Node работают следующие модули, ядра и технологии приложения:

- *Anti-Malware Engine* (далее также *AM* и *AM Engine*). Выполняет проверку файлов и объектов на вирусы и другие программы, представляющие угрозу IT-инфраструктуре организации, с помощью антивирусных баз.
- *Mobile Attack Analyzer* (далее также *MAA*). Выполняет проверку исполняемых файлов формата APK в облачной инфраструктуре на основе технологии машинного обучения. В результате проверки Kaspersky Anti Targeted Attack Platform получает информацию об обнаруженных угрозах или их отсутствии.
- *YARA*. Выполняет проверку файлов и объектов на наличие признаков целевых атак на IT-инфраструктуру организации с помощью баз YARA-правил, создаваемых пользователями Kaspersky Anti Targeted Attack Platform.
- *Targeted Attack Analyzer* (далее также *TAA*, *TA Analyzer*). Выполняет анализ и проверку сетевой активности программного обеспечения, установленного на компьютеры локальной сети организации, на основе правил TAA (IOA). Выполняет поиск признаков сетевой активности, на которую пользователю Kaspersky Anti Targeted Attack Platform рекомендуется обратить внимание, а также признаков целевых атак на IT-инфраструктуру организации.
- *KSN*. Выполняет для Kaspersky Anti Targeted Attack Platform проверку репутации файлов и URL-адресов в базе знаний Kaspersky Security Network и предоставляет сведения о категориях веб-сайтов (например, вредоносный веб-сайт, фишинговый веб-сайт).

Компонент Sandbox

На серверах с компонентом Sandbox запускаются виртуальные машины с образами операционных систем.

Компонент Sandbox запускает объекты в этих операционных системах и анализирует поведение объектов для выявления вредоносной активности, признаков целевых атак на IT-инфраструктуру организации.

Особенности проверки файлов

Существуют следующие особенности проверки файлов в Sandbox:

- Максимальное количество объектов, которое может находиться в очереди на проверку компонентом Sandbox за одни сутки, составляет 20 тысяч объектов. По достижении этого ограничения приложение удаляет 10% объектов, поступивших на проверку раньше остальных, и заменяет их новыми объектами, поступившими на проверку. Удаленные объекты сохраняются в приложении со статусом NOT_SCANNED (непроверенные).
- Общее количество отправляемых из одного архива объектов не превышает 20.
- Проверяются файлы, расположенные до 3 уровня распаковки включительно.

Компонент Endpoint Agent

Программный компонент.

Для функциональности KEDR может быть представлен следующими приложениями:

- Kaspersky Endpoint Security для Windows.
- Kaspersky Endpoint Security для Linux.
- Kaspersky Endpoint Security для Mac.

Для функциональности NDR может быть представлен следующими приложениями:

- Kaspersky Endpoint Security для Windows.
- Kaspersky Endpoint Security для Linux.

Приложения устанавливаются на рабочие станции и серверы в IT-инфраструктуре организации (далее также "компьютеры"). На этих компьютерах приложения постоянно наблюдают за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправляют данные наблюдения на сервер Central Node.

Компьютеры, предназначенные для установки приложений, должны удовлетворять аппаратным и программным требованиям.

Принцип работы приложения

Приложение Kaspersky Anti Targeted Attack Platform включает в себя три функциональных блока:

- Kaspersky Anti Targeted Attack (далее также "KATA"), обнаруживающий угрозы по периметру IT-инфраструктуры предприятия.
- Kaspersky Endpoint Detection and Response (далее также "KEDR"), обеспечивающий защиту компьютеров локальной сети организации.
- Network Detection and Response (далее также "NDR"), обеспечивающий защиту внутренней сети предприятия.

Вы можете использовать как полную функциональность приложения (ключ KATA + NDR и ключ KEDR), так и неполную (только ключ KATA/KATA + NDR или только ключ KEDR).

Принцип работы Kaspersky Anti Targeted Attack

Kaspersky Anti Targeted Attack включает в себя следующие компоненты:

- Sensor.
- Central Node.
- Sandbox.

Компоненты Sensor, Central Node и Sandbox взаимодействуют между собой по следующему принципу:

- Компонент Sensor получает зеркалированный SPAN-, ERSPAN-, RSPAN-трафик, объекты и метаинформацию HTTP-, FTP-, SMTP- и DNS-протоколов, данные HTTP- и FTP-трафика, а также HTTPS-трафика (если администратор настроил подмену SSL-сертификата на прокси-сервере), копии сообщений электронной почты и производит с полученными данными следующие действия:
  - Проверяет интернет-трафик на наличие признаков вторжения в IT-инфраструктуру организации с помощью технологии Intrusion Detection System (далее также "IDS").

    Технология IDS позволяет распознать и обнаружить сетевую активность по 80 протоколам, в частности по 53 протоколам прикладного уровня модели TCP/IP, фиксируя подозрительный трафик и сетевые атаки. В числе поддерживаемых протоколов TCP, UDP, FTP, TFTP, SSH, SMTP, SMB, CIF, SSL, HTTP, HTTP/2, HTTPS, TLS, ICMPv4, ICMPv6, IPv4, IPv6, IRC, LDAP, NFS, DNS, RDP, DCERPC, MS-RPC, WebSocket, Citrix и другие.
  - Проверяет репутацию файлов и URL-адресов по базе знаний Kaspersky Security Network (далее также "KSN") или Kaspersky Private Security Network (далее также "KPSN").
  - Отправляет объекты и файлы на проверку компоненту Central Node.

В качестве компонента Sensor также может использоваться *почтовый сенсор* – сервер или виртуальная машина, на которой установлено приложение "Лаборатории Касперского" Kaspersky Secure Mail Gateway (далее также "KSMG") или Kaspersky Security для Linux Mail Server (далее также "KLMS").

- Компонент Central Node проверяет файлы и объекты с помощью антивирусных баз, баз YARA-правил, создаваемых пользователями Kaspersky Anti Targeted Attack, при необходимости отправляет файлы и объекты на проверку компоненту Sandbox.

- Компонент Sandbox анализирует поведение объектов в виртуальных операционных системах для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации и отправляет данные о результатах проверки на сервер Central Node.

При обнаружении угроз сервер Central Node записывает информацию о них в базу алертов. Вы можете просмотреть таблицу алертов в разделе **Алерты** веб-интерфейса приложения или сформировав отчет об алертах.

Информация об алертах также может публиковаться в SIEM-систему, которая используется в вашей организации, и во внешние системы. Информация об алертах компонента Sandbox может публиковаться в локальную репутационную базу Kaspersky Private Security Network.

Принцип работы Network Detection and Response

Network Detection and Response включает в себя следующие компоненты:

- Sensor.

- Central Node.

- Endpoint Agent, подключенный к фунциональному блоку NDR.

  Компонент может быть представлен приложениями Kaspersky Endpoint Agent для Windows, Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux.

- Sandbox.

  Опциональный компонент.

При использовании этого функционального блока компоненты Sensor, Central Node и Sandbox взаимодействуют между собой так же, как при использовании функционального блока Kaspersky Anti Targeted Attack. Вы можете посмотреть подробную информацию об их взаимодействии выше.

Компоненты Endpoint Agent и Central Node взаимодействуют между собой по следующему принципу:

Одно из приложений, представляющих компонент Endpoint Agent, устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и получает об устройствах, на которые установлен компонент, следующие данные:

- Информация о событиях NDR, записанных в базу событий в результате срабатывания технологии EPP (события защиты рабочих станций и серверов).

- Сведения об устройствах (например, версия операционной системы, сведения о модели или производителе).

- Сведения о соединениях устройств на карте сетевых взаимодействий.
- Сведения о протоколах, по которым осуществляется соединение между устройствами.

Принцип работы Kaspersky Endpoint Detection and Response

Kaspersky Endpoint Detection and Response включает в себя следующие компоненты:

- Central Node.
- Endpoint Agent.

  Компонент может быть представлен приложениями Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac.
- Sandbox.

  Опциональный компонент.

  > В качестве прокси-сервера для соединений, исходящих от компонента Endpoint Agent, может использоваться компонент Sensor.

Компоненты Endpoint Agent и Central Node взаимодействуют между собой по следующему принципу:

Одно из приложений, представляющих компонент Endpoint Agent, устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные наблюдения отправляются на сервер Central Node. На основе этих данных формируются события.

- Kaspersky Endpoint Security для Windows передает на сервер Central Node данные о следующих событиях: **Запущен процесс**, **Завершен процесс**, **Загружен модуль**, **Удаленное соединение**, **Правило запрета**, **Заблокирован документ**, **Изменен файл**, **Журнал событий ОС**, **Изменение в реестре**, **Прослушан порт**, **Загружен драйвер**, **Интерпретированный запуск файла**, **Интерактивный ввод команд в консоли**, **Обнаружение**, **Результат обработки обнаружения**, **AMSI-проверка**, **DNS**, **Внедрение кода**, **Именованный канал**, **WMI**, **LDAP**.
- Kaspersky Endpoint Security для Linux передает на сервер Central Node данные о следующих событиях: **Запущен процесс**, **Завершен процесс**, **Правило запрета**, **Заблокирован документ**, **Изменен файл**, **Журнал событий ОС**, **Обнаружение**, **Результат обработки обнаружения**, **Внедрение кода**, **DNS**.
- Kaspersky Endpoint Security для Mac передает на сервер Central Node данные о следующих событиях: **Запущен процесс**, **Завершен процесс**, **Изменен файл**, **Обнаружение**, **Результат обработки обнаружения**.

  > Endpoint Agent для функциональности NDR подключается отдельно и не отправляет информацию о наблюдениях на сервер Central Node.

События, поступающие на сервер Central Node, отмечаются правилами TAA (IOA). В результате разметки для событий, требующих внимания пользователя, могут формироваться алерты. При наличии компонента Sandbox вы можете также включить автоматическую отправку файлов с хостов с компонентом Endpoint Agent на проверку компоненту Sandbox в соответствии с правилами TAA (IOA) "Лаборатории Касперского".

При интеграции сервера Central Node с Kaspersky Endpoint Security для Windows вы можете осуществлять следующие меры по реагированию на обнаруженные угрозы:

- Работать с файлами и приложениями путем выполнения задач **Завершить процесс**, **Собрать форензику**, **Запустить YARA-проверку**, **Запустить программу**, **Получить файл**, **Удалить файл**, **Поместить файл на карантин**, **Восстановить файл из карантина**, **Управлять службами**, **Получить образ диска**, **Получить дамп памяти** на хостах.
- Настраивать политики запрета запуска файлов и процессов на выбранных хостах.
- Изолировать отдельные хосты от сети.
- Работать с правилами TAA (IOA) для классификации и анализа событий.
- Работать с файлами открытого стандарта описания индикаторов компрометации OpenIOC (IOC-файлы) для поиска признаков целевых атак, зараженных и возможно зараженных объектов на хостах и в базе алертов.
- Выполнять действия по реагированию с помощью интерфейса API.

При интеграции сервера Central Node с Kaspersky Endpoint Security 11.4 для Linux и Kaspersky Endpoint Security для Mac вы можете осуществлять следующие меры по реагированию на обнаруженные угрозы:

- Работать с файлами и приложениями путем выполнения задач **Получить файл**, **Запустить программу**.
- Работать с правилами TAA (IOA) для классификации и анализа событий.
- Выполнять следующие действия по реагированию с помощью интерфейса API: управление задачей запуска приложений.

При интеграции сервера Central Node с Kaspersky Endpoint Security 12 для Linux вы можете осуществлять следующие меры по реагированию на обнаруженные угрозы:

- Работать с файлами и приложениями путем выполнения задач **Получить файл**, **Запустить программу**, **Удалить файл**, **Завершить процесс**.
- Изолировать отдельные хосты от сети.
- Работать с файлами открытого стандарта описания индикаторов компрометации OpenIOC (IOC-файлы) для поиска признаков целевых атак, зараженных и возможно зараженных объектов на хостах и в базе алертов.
- Выполнять следующие действия по реагированию с помощью интерфейса API: управление сетевой изоляцией хостов, управление задачей запуска приложений.

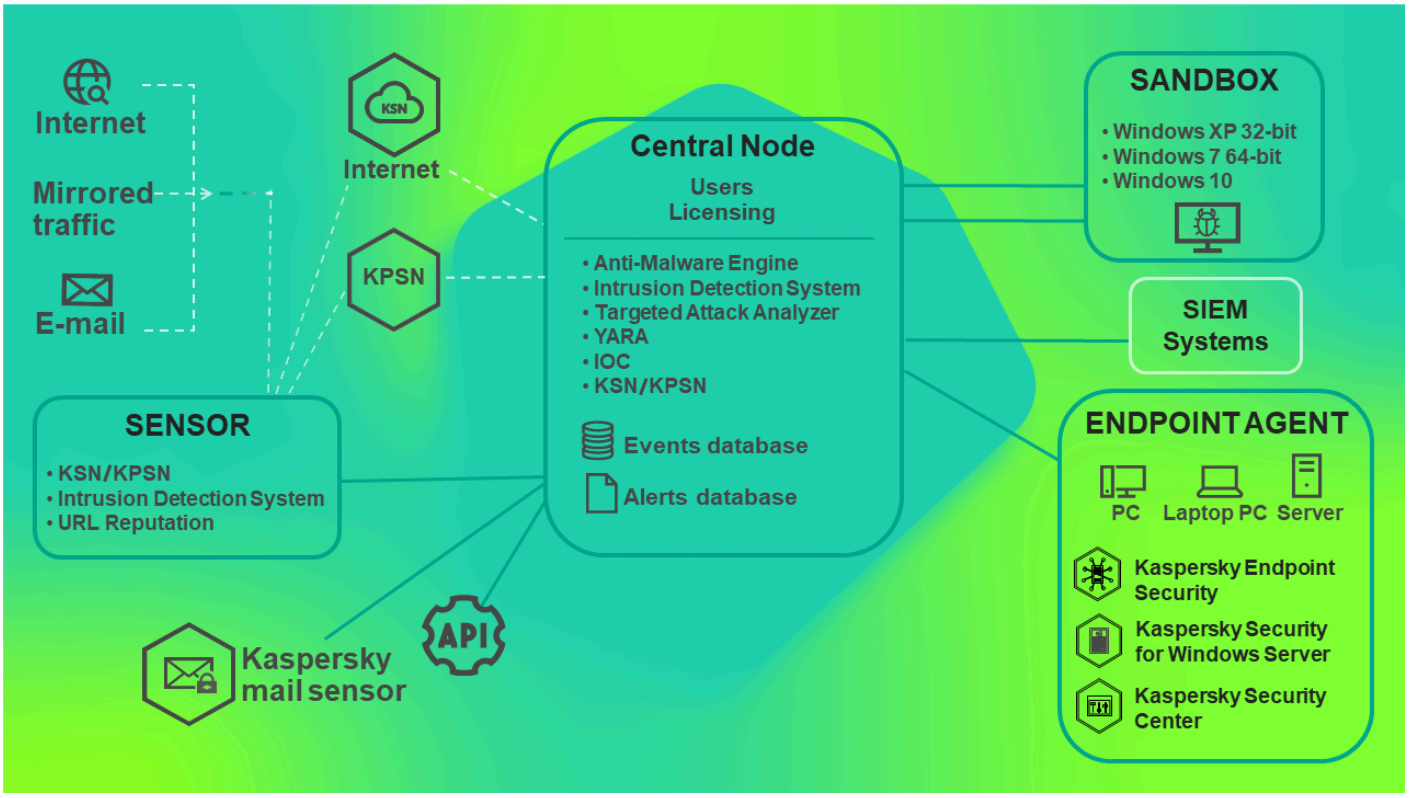
При интеграции сервера Central Node с Kaspersky Endpoint Security 12.2 для Linux вы можете осуществлять следующие меры по реагированию на обнаруженные угрозы:

- Работать с файлами и приложениями путем выполнения задач **Получить файл**, **Запустить программу**, **Удалить файл**, **Завершить процесс**, **Поместить файл на карантин**, **Восстановить файл из карантина**.
- Настраивать политики запрета запуска файлов и процессов на выбранных хостах.
- Изолировать отдельные хосты от сети.

- Работать с файлами открытого стандарта описания индикаторов компрометации OpenIOC (IOC-файлы) для поиска признаков целевых атак, зараженных и возможно зараженных объектов на хостах и в базе алертов.

- Выполнять следующие действия по реагированию с помощью интерфейса API: управление сетевой изоляцией хостов, управление задачей запуска приложений, управление правилами запрета.

Принцип работы Kaspersky Anti Targeted Attack Platform показан на рисунке ниже.

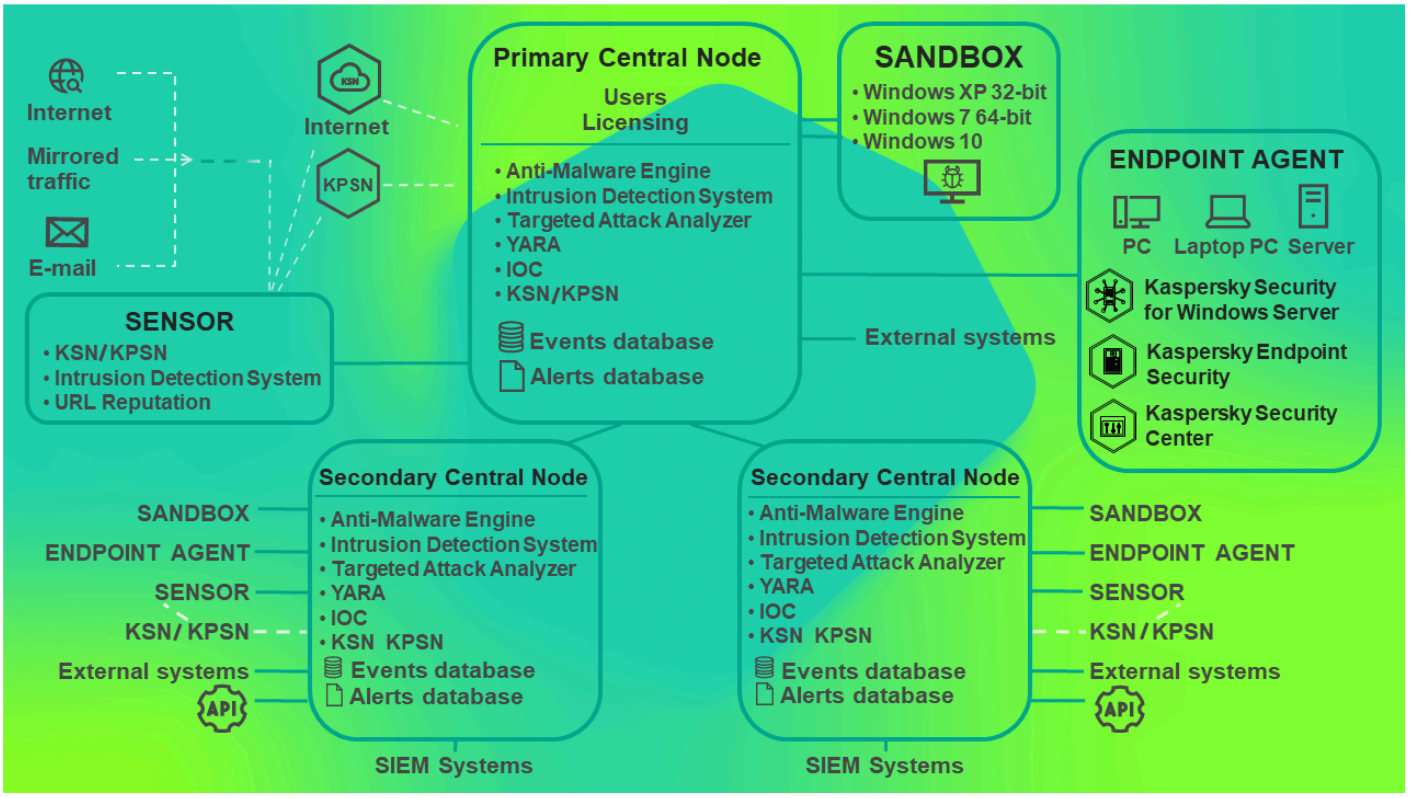


Принцип работы Kaspersky Anti Targeted Attack Platform

Вы можете настраивать параметры каждого компонента Central Node отдельно или управлять несколькими компонентами централизованно в режиме распределенного решения.

Распределенное решение представляет собой двухуровневую иерархию серверов Central Node. В этой структуре выделяется главный сервер управления – Primary Central Node (PCN) и подчиненные серверы – Secondary Central Node (SCN).

Принцип работы Kaspersky Anti Targeted Attack Platform в режиме распределенного решения показан на рисунке ниже.



Принцип работы Kaspersky Anti Targeted Attack Platform в режиме распределенного решения

Распределенное решение и мультитенантность

Вы можете настраивать параметры каждого компонента Central Node отдельно или управлять несколькими компонентами централизованно в режиме распределенного решения.

Распределенное решение представляет собой двухуровневую иерархию серверов с установленными компонентами Central Node. В этой структуре выделяется главный сервер управления – *Primary Central Node (PCN)* и подчиненные серверы – *Secondary Central Node (SCN)*. Для взаимодействия серверов требуется подключить SCN к PCN.

Если вы развернули компонент Central Node в виде кластера, весь кластер выполняет роль PCN или SCN.

PCN и SCN осуществляют проверку файлов и объектов с помощью тех же технологий, что и компонент Central Node, управляемый отдельно.

В распределенном решении вы можете централизованно управлять следующими функциональными областями приложения:

- Пользователи.
- Алерты.
- Поиск угроз.
- Задачи.
- Политики.
- Пользовательские правила.
- Хранилище.
- Endpoint Agents, в том числе сетевая изоляция хостов.
- Отчеты.

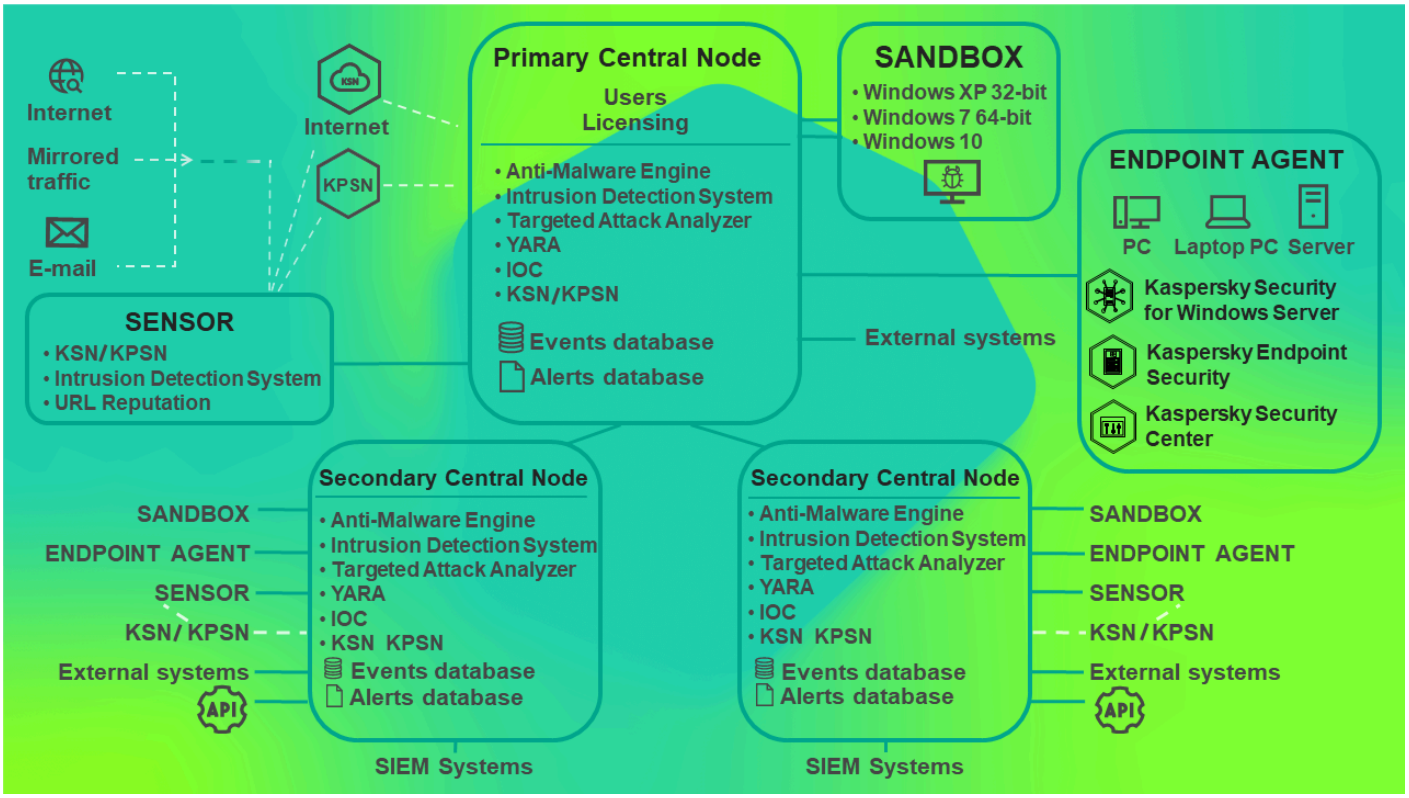
Если вы поддерживаете несколько организаций или филиалов одной организации, вы можете использовать приложение в режиме мультитенантности.

Мультитенантность - это режим работы, при котором приложение используется для защиты инфраструктуры нескольких организаций или филиалов одной организации (далее также "тенантов") одновременно. Вы можете установить Kaspersky Anti Targeted Attack Platform на один или несколько серверов Central Node для каждого тенанта. Каждый тенант может работать с приложением независимо от других тенантов. Поставщик услуг может работать с данными нескольких тенантов.

Компоненты Central Node, которые вы хотите организовать в иерархию, должны быть развернуты на базе одной операционной системы (Ubuntu или Astra Linux). Версии компонентов должны совпадать.

Количество одновременных сеансов работы с приложением под одной учетной записью ограничено одним IP-адресом. При попытке входа в приложение под этим же именем пользователя с другого IP-адреса первый сеанс работы с приложением завершается.

Если вы используете режим распределенного решения и мультитенантности, ограничение действует для каждого сервера PCN и SCN независимо друг от друга.



Принцип работы приложения в режиме распределенного решения

Вы можете использовать режим распределенного решения и мультитенантности в следующих случаях:

- для защиты более 10 000 хостов тенанта;
- для централизованного управления приложением в разных подразделениях тенантов;

- для централизованного управления приложением на серверах нескольких тенантов;
- для обработки сетевого трафика на максимальной скорости 10 Гбит/с при наличии в сети более одного сегмента с пропускной способностью 10 Гбит/с и при необходимости обрабатывать трафик в этих сегментах.

При переключении приложения в режим распределенного решения и мультитенантности на серверах с ролью SCN все ранее добавленные лицензионные ключи удаляются. Каждый подключенный SCN получает ключ от PCN. Если для PCN используется полная функциональность приложения (ключ KATA и KEDR), а для SCN неполная (только ключ KATA или только ключ KEDR), в связи с увеличением объема данных возможно превышение допустимого уровня нагрузки на сервер SCN. Если для PCN используется неполная функциональность приложения (только ключ KATA или только ключ KEDR), а для SCN полная (ключ KATA и KEDR), часть функционала приложения будет недоступна.

Управление лицензионными ключами будет доступно только на PCN.

Вы можете развернуть приложение в режиме распределенного решения и мультитенантности по следующим сценариям:

- Установить компонент Central Node на новых серверах и назначить этим серверам роли PCN и SCN.
- Назначить роли PCN и SCN серверам с ранее установленным компонентом Central Node.

  В этом случае вам требуется обновить компонент Central Node до версии 7.1.1.

  Перед переключением серверов с установленными компонентами Central Node в режим распределенного решения рекомендуется ознакомиться с изменениями, которые произойдут в системе после смены режима работы. Назначение серверу роли PCN является необратимым.

Сценарий перехода в режим распределенного решения и мультитенантности

Переход приложения в режим распределенного решения и мультитенантности содержит следующие этапы:

1. **Назначение DNS-имени серверу Central Node, который будет использоваться в роли PCN**

   Если DNS-имя было назначено ранее, убедитесь, что оно указано верно.

2. **Назначение серверу роли PCN**
3. **Создание на сервере PCN учетной записи администратора приложения**

   Эта учетная запись используется для подключения серверов SCN к PCN. Если для Kaspersky Anti Targeted Attack Platform настроена интеграция с Active Directory, при создании учетной записи требуется выбрать тип аутентификации **Учетная запись KATA**.

4. **Назначение серверам роли SCN и отправка запросов на подключение к PCN**
5. **Обработка запроса на подключение SCN к PCN**

После перехода в режим распределенного решения и мультитенантности приложению может потребоваться время для настройки работы компонентов. В этом случае в веб-интерфейсе SCN не отображается меню приложения, а в веб-интерфейсе PCN в разделе **Мониторинг** отображается ошибка *Данные не передаются на SCN более 5 минут*. Время настройки работы компонентов зависит от количества накопленных данных и в среднем составляет 20-30 минут.

Изменения в параметрах приложения при переходе в режим распределенного решения и мультитенантности

Изменения в параметрах приложения при переключении в режим распределенного решения и мультитенантности приведены в таблице ниже.

Изменения в параметрах приложения при переключении в режим распределенного решения и мультитенантности

Функциональная область	PCN	SCN
Пользователи	Пользователи и назначенные им роли сохраняются. Дополнительно пользователям PCN выдаются права на работу с PCN и всеми подключенными SCN.	Удаляются все пользователи, кроме пользователя, созданного в момент развертывания Central Node. После этого SCN запрашивает у PCN список пользователей и на основе этого списка создает локальных пользователей с такими же параметрами: • имя; • пароль; • роль; • статус. Пользователи, не имеющие прав на доступ к SCN, не отображаются в списке пользователей.
Алерты	В таблице алертов на PCN отображаются записи обо всех алертах, зарегистрированных на подключенных SCN. Данные в карточке алерта не копируются на PCN. При просмотре информации об алерте на PCN данные запрашиваются с SCN.	В информации об уже имеющихся алертах перестает отображаться имя пользователя. Данные о пользователях удаляются из истории операций с алертом.
События в трафике сети	Изменений нет.	Изменений нет.
Мониторинг	На закладке **Алерты** появляется возможность выбрать SCN, информация о которых должна быть отражена на виджете. На закладке **Работоспособность системы** появляется статус соединения PCN с подключенными SCN.	На закладке **Работоспособность системы** появляется статус соединения с PCN.
Задачи	Задачи, созданные на сервере Central Node до назначения ему роли PCN, а также задачи, создаваемые на PCN после перехода в режим распределенного решения, распространяются на все подключенные SCN. В списке задач также отображаются задачи, созданные на SCN. Изменение параметров этих задач на PCN недоступно.	Отображаются задачи, созданные на PCN, а также задачи, созданные на этом SCN. Изменение параметров задач, созданных на PCN, недоступно.
Отчеты	Шаблоны и отчеты, созданные до переключения в режим распределенного решения, сохраняются. В таблице отчетов появляется столбец **Серверы** с информацией о SCN, к которому относится алерт. После переключения в режим распределенного решения отображаются только отчеты, созданные на PCN.	Шаблоны и отчеты, созданные до переключения в режим распределенного решения, сохраняются. Информация о пользователе, создавшем отчет, сохраняется, если на PCN есть пользователь с таким же идентификатором (guid). В остальных случаях информация о пользователе удаляется. После переключения в режим распределенного решения отображаются только отчеты, созданные на SCN.

Функциональная область	PCN	SCN
Политики	Политики, созданные на сервере Central Node до назначения ему роли PCN, а также политики, создаваемые на PCN после перехода в режим распределенного решения, распространяются на все подключенные SCN. В списке политик также отображаются политики, созданные на SCN. Изменение параметров этих политик на PCN недоступно. Предустановки для автоматического создания правил запрета становятся недоступны, новые правила не создаются. Ранее автоматически созданные правила распространяются на все подключенные SCN.	Отображаются политики, созданные на PCN, а также политики, созданные на этом SCN. Изменение параметров политик, созданных на PCN, недоступно. Предустановки для автоматического создания правил запрета становятся недоступны, новые правила не создаются. Ранее автоматически созданные правила действуют только на этом SCN.
Хранилище	Все файлы и метаданные, которые хранились на PCN до перехода в режим распределенного решения, сохраняются. В столбце **Central Node** для них отображается имя PCN. На PCN также сохраняется содержимое Хранилища всех подключенных SCN.	Все файлы и метаданные, которые хранились на SCN до перехода в режим распределенного решения, сохраняются.
Исключение TAA (IOA)	Изменений нет.	Изменений нет.
Статус VIP	Изменений нет.	Изменений нет.
Правила уведомлений	Изменений нет.	Изменений нет.
Интеграция с почтовыми сенсорами	Изменений нет.	Изменений нет.
Поиск угроз	При поиске угроз по базе событий PCN отправляет запрос на все подключенные SCN. В результате обработки поискового запроса отображается список событий PCN и SCN выбранного тенанта.	Изменений нет.
Пользовательские правила - TAA	Правила TAA (IOA), добавленные на сервере Central Node до назначения ему роли PCN, распространяются только на этот сервер PCN. Правила, добавленные после назначения серверу роли PCN распространяются также на SCN.	Отображаются правила TAA (IOA), добавляемые на PCN, а также правила TAA (IOA), добавляемые на этом SCN до и после перехода в режим распределенного решения.
Пользовательские правила - Обнаружение вторжений	Нет изменений.	Нет изменений.
Пользовательские правила - IOC	Поиск индикаторов компрометации по IOC-файлам, добавленным на сервере Central Node до назначения ему роли PCN, выполняются только на этом сервер PCN. Поиск индикаторов компрометации по IOC-файлам, добавленным на сервере Central Node после назначения ему роли PCN, распространяются также на SCN.	Отображаются IOC-файлы, добавляемые на PCN, а также IOC-файлы, добавляемые на этом SCN до и после перехода в режим распределенного решения.
Пользовательские правила - YARA	Правила YARA, добавленные на сервере Central Node до назначения ему роли PCN, распространяются только на этот сервер PCN. Правила, добавленные после назначения серверу роли PCN распространяются также на SCN.	Отображаются правила YARA, добавляемые на PCN, а также правила YARA, добавляемые на этом SCN до и после перехода в режим распределенного решения.
Активы	Нет изменений.	Нет изменений.
Карта сети	Нет изменений.	Нет изменений.
Риски и аномалии	Нет изменений.	Нет изменений.
Резервное копирование приложения	Резервное копирование приложения доступно только на PCN, к которому не подключены SCN. Чтобы сделать резервное копирование приложения на PCN, необходимо отключить все SCN от этого PCN.	Резервное копирование приложения на SCN недоступно. Чтобы сделать резервное копирование приложения на SCN, необходимо отключить этот сервер от PCN, переведя его в режим отдельного сервера.

Назначение серверу роли PCN

Назначение серверу роли PCN необратимо. После изменения роли сервера на PCN вы не сможете изменить роль этого сервера на SCN или отдельный сервер. Если вы захотите изменить роль этого сервера снова, вам потребуется переустановить приложение.

Чтобы назначить серверу роль PCN:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс того сервера, которому вы хотите назначить роль PCN.

2. Выберите раздел **Режим работы**.

3. Нажмите на кнопку **Распределенное решение**.

4. В раскрывающемся списке **Роль сервера** выберите **Primary Central Node**.

5. В поле **Название тенанта** введите название тенанта, к которому относится этот сервер Central Node.

6. Нажмите на кнопку **Назначить роль PCN**.

   Откроется окно подтверждения действия.

   После подтверждения действия вам потребуется снова войти в веб-интерфейс приложения.

7. Нажмите на кнопку **Да**.

Серверу будет назначена роль PCN и присвоено название тенанта.

После того, как вы снова войдете в веб-интерфейс приложения под учетной записью администратора, в окне веб-интерфейса приложения в разделе **Режим работы** отобразится следующая информация:

- **Текущий режим** – Распределенное решение.
- **Роль сервера** – Primary Central Node.
- **Отпечаток сертификата** – отпечаток сертификата сервера, необходимый для проверки подлинности при установке соединения с SCN.
- **Тенанты** – информация о тенантах, к которым относится этот сервер, и все подключенные серверы SCN:
  - **IP** – Primary Central Node для этого сервера и IP-адреса серверов SCN (после их подключения).
  - **Сервер** – имя этого сервера и имена серверов SCN (после их подключения).

    Это имя не связано с именем хоста, на котором установлено приложение. Вы можете его изменить.

- **Отпечаток сертификата** – пустое значение для этого сервера и отпечатки сертификатов серверов SCN (после их подключения).
- **Состояние** – состояние подключения серверов SCN (после их подключения), а также количество серверов, подключенных к тенантам.

- Таблица **Серверы, ожидающие авторизации** с информацией о подключенных SCN.

Назначение серверу роли SCN

Чтобы назначить серверу роль SCN:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс того сервера, которому вы хотите назначить роль SCN.

2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.

3. Нажмите на кнопку **Распределенное решение**.

4. В раскрывающемся списке **Роль сервера** выберите **Secondary Central Node**.

5. В поле **Имя сервера (FQDN)** введите FQDN-имя сервера, которому вы хотите назначить роль SCN.

6. В поле **IP-адрес сервера PCN** укажите IP-адрес сервера с ролью PCN, к которому вы хотите подключить SCN.

7. Нажмите на кнопку **Получить отпечаток сертификата**.

   В рабочей области отобразится отпечаток сертификата сервера с ролью PCN.

8. Свяжитесь с администратором PCN и сравните полученный отпечаток сертификата с отпечатком, указанным на PCN в разделе **Режим работы** в поле **Отпечаток сертификата**.

9. Если отпечатки сертификата на SCN и PCN совпадают, в полях **Имя пользователя** и **Пароль** введите имя пользователя и пароль учетной записи администратора, созданной на PCN для подключения SCN.

10. Нажмите на кнопку **Отправить запрос на подключение**.

    Откроется окно подтверждения.

11. Нажмите на кнопку **Да**.

Серверу будет назначена роль SCN.

Обработка запросов на подключение SCN к PCN

Чтобы обработать запрос на подключение SCN к PCN:

1. Войдите в веб-интерфейс того сервера PCN, на котором вы хотите обработать запросы на подключение от других серверов.
2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.

   В рабочей области отобразится таблица **Серверы, ожидающие авторизации**.
3. Свяжитесь с администратором SCN, отправившим запрос на подключение, и проверьте отпечаток сертификата в таблице **Серверы, ожидающие авторизации**. Он должен совпадать с отпечатком, отображаемым на SCN в разделе **Режим работы** в поле **Отпечаток сертификата из запроса**.
4. Если отпечатки сертификата на PCN и SCN совпадают, выполните одно из следующих действий:
   - Если вы хотите отклонить запрос на подключение от SCN, нажмите на кнопку **Отклонить**.
   - Если вы хотите принять запрос на подключение от SCN, выполните следующие действия:
     a. Нажмите на кнопку **Принять**.
     b. Откроется окно **Принять запрос на подключение**.
     c. В списке **Тенант** выберите тенант, которому вы хотите назначить этот сервер SCN. Список формируется из тенантов, добавленных ранее.
     d. Нажмите на кнопку **Принять**.

Не рекомендуется принимать запросы на подключение при несовпадении отпечатков сертификата. Убедитесь в правильности введенных данных.

На время подключения сервера SCN к PCN все кнопки в окне **Режим работы** блокируются. После того, как подключение завершится, кнопки будут разблокированы.

Если вы отклонили запрос на подключение, SCN продолжит работу в режиме отдельного сервера Central Node.

Просмотр информации о тенантах, серверах PCN и SCN

В веб-интерфейсе сервера PCN вы можете просмотреть информацию об этом сервере, а также о всех серверах SCN, которые к нему подключены.

Чтобы просмотреть информацию о серверах PCN и SCN в режиме мультитенантности:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс сервера PCN.

2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.

В рабочей области отобразится следующая информация о серверах:

- **Текущий режим** – Распределенное решение.
- **Роль сервера** – Primary Central Node.
- **Отпечаток сертификата** – отпечаток сертификата сервера PCN.
- **Тенанты** – информация о тенантах, к которым относятся этот сервер, а также все серверы SCN, подключенные к PCN.
  - **IP** – Primary Central Node для сервера PCN и IP-адреса серверов SCN, подключенных к PCN.
  - **Сервер** – имя этого сервера и имена серверов SCN, подключенных к PCN.

    Это имя не связано с именем хоста, на котором установлено приложение. Вы можете его изменить.
  - **Отпечаток сертификата** – пустое значение для сервера PCN и отпечатки сертификатов серверов SCN, которые ожидают подключения к PCN.
  - **Состояние** – состояние подключения серверов SCN, а также количество серверов, подключенных к тенанту.
- Таблица **Серверы, ожидающие авторизации** со следующей информацией:
  - **IP** – IP-адрес или доменное имя сервера SCN.
  - **Сервер** – имя сервера SCN, которое отображается в веб-интерфейсе приложения.

    Это имя не связано с именем хоста, на котором установлено приложение. Вы можете его изменить.
  - **Отпечаток сертификата** – отпечаток сертификата сервера SCN, передаваемый на PCN вместе с запросом на подключение.
  - **Состояние** – статус подключения SCN к PCN.

Добавление тенанта на сервере PCN

Чтобы добавить тенант в веб-интерфейсе сервера PCN:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс того сервера PCN, для которого вы хотите добавить тенант.

2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.

3. В правой части рабочей области **Тенанты** нажмите на кнопку **Добавить**.

4. В поле **Имя** введите название тенанта, который вы хотите добавить.
5. Нажмите на кнопку **Добавить**.

Тенант будет добавлен и отобразится в списке.

Удаление тенанта на сервере PCN

Чтобы удалить тенант в веб-интерфейсе сервера PCN:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс сервера PCN, для которого вы хотите удалить тенант.
2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.
3. В рабочей области **Тенанты** выберите тенант, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

   Действие необратимо. Все глобальные объекты, а также отчеты и шаблоны отчетов, связанные с этим тенантом, будут потеряны.
5. Нажмите на кнопку **Да**.

Тенант будет удален.

Изменение названия тенанта на сервере PCN

Чтобы изменить название тенанта в веб-интерфейсе сервера PCN:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс сервера PCN, для которого вы хотите изменить название тенанта.
2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.
3. В списке **Тенанты** нажмите на значок справа от названия тенанта, которое вы хотите изменить.

   Откроется окно изменения названия тенанта.
4. В поле **Имя** измените название тенанта.
5. Нажмите на кнопку **Сохранить**.

Название тенанта будет изменено.

Восстановление подключения SCN к PCN

Возможна ситуация, когда SCN теряет соединение с PCN на продолжительное время (более суток), в результате чего истекает срок действия токена, который используется при соединении SCN и PCN. В разделе **Мониторинг** в таком случае появляется сообщение *Истек токен взаимодействия с PCN. Войдите в SCN и восстановите подключение к PCN.*

Чтобы восстановить подключение SCN к PCN:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс того SCN, которому требуется восстановить подключение к PCN.

2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.

3. По ссылке **Войти** откройте окно авторизации на сервере PCN.

4. Введите IP-адрес сервера PCN, к которому был подключен SCN, имя пользователя и пароль учетной записи администратора, созданной на PCN для подключения SCN.

5. Нажмите на кнопку **Войти**.

Через некоторое время подключение SCN к PCN восстановится, сообщение *Истек токен взаимодействия с PCN. Войдите в SCN и восстановите подключение к PCN* в разделе **Мониторинг** исчезнет.

Отключение SCN от PCN

Если вы хотите отключить SCN от PCN, вам нужно учитывать следующие особенности дальнейшей работы с серверами:

- Начиная с версии приложения 7.0 повторное подключение сервера SCN к какому-либо серверу PCN не предусмотрено.
- Если вы хотите повторно подключить сервер в роли SCN, вам нужно переустановить компонент Central Node на этом сервере.
- При отключении SCN от PCN произойдут изменения в параметрах приложения.

Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за сохранность конфиденциальных данных на серверах PCN, SCN и Central Node. Если вы планируете передать сервер SCN от одного тенанта другому, необходимо удалить все данные, оставшиеся на сервере после использования Kaspersky Anti Targeted Attack Platform и переустановить Kaspersky Anti Targeted Attack Platform перед передачей сервера другому тенанту.

Чтобы отключить SCN от PCN:

1. Войдите в веб-интерфейс того сервера PCN, от которого вы хотите отключить SCN, под учетной записью администратора.
2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.
3. В списке серверов выберите SCN, который вы хотите отключить.
4. Нажмите на кнопку **Отключить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

SCN будет отключен от PCN и продолжит работать как отдельный сервер Central Node.

Изменения в параметрах приложения при отключении SCN от PCN

Изменения в параметрах приложения после отключения SCN от PCN представлены в таблице ниже.

Изменения параметров приложения после отключения SCN от PCN

Функциональная область	PCN	SCN
Пользователи	Отключенный SCN не исключается из списка серверов, на которые распространяются права пользователей. Информация об изменении учетной записи пользователя, имеющего права на отключенный SCN, не передается на SCN.	Учетные записи пользователей, полученные с PCN, не удаляются. Появляется возможность создания новых учетных записей пользователей, а также отключения и смены пароля существующих учетных записей.
Алерты	Информация об алертах на отключенном SCN удаляется.	История операций и вся информация об алертах сохраняется.
Задачи	Задачи, созданные на отключенном SCN, удаляются.	Задачи, созданные на PCN, удаляются. Информация о пользователях, создавших задачи на SCN, сохраняется.
Отчеты	Все созданные ранее отчеты об отключенном SCN, а также возможность фильтровать список отчетов по этому серверу, сохраняются.	Шаблоны и отчеты не изменяются.
Политики	Политики, созданные на отключенном SCN, удаляются.	Политики, созданные на PCN, удаляются. Информация о пользователях, создавших политики на SCN, сохраняется.
Хранилище	Из Хранилища удаляются все объекты, относящиеся к отключенному SCN.	Все объекты в Хранилище сохраняются. В информации об объектах, полученных в рамках задач, созданных на PCN, перестает работать ссылка на задачу.
Исключение ТАА (IOA)	Изменений нет.	Изменений нет.
Статус VIP	Изменений нет.	Изменений нет.
Правила уведомлений	Изменений нет.	Изменений нет.
Интеграция с почтовыми сенсорами	Изменений нет.	Изменений нет.
Поиск угроз	В результате обработки поискового запроса события, связанные с отключенным SCN, не отображаются.	Изменений нет.

Функциональная область	PCN	SCN
Пользовательские правила - TAA и IOC	IOC- и правила TAA (IOA) отключенного SCN удаляются.	IOC- и правила TAA (IOA), созданные на PCN, удаляются.
Резервное копирование приложения	Резервное копирование приложения остается недоступным.	Резервное копирование приложения становится доступным.

Руководство по масштабированию

Для достижения и сохранения оптимальной производительности при различных условиях работы приложения требуется учитывать количество устройств в сети, топологию сети и необходимую вам функциональность приложения.

Выбор оптимальной конфигурации приложения состоит из следующих этапов:

1. **Выбор типовой схемы развертывания**
2. **Расчет аппаратных требований с помощью калькулятора масштабирования**

Типовые схемы развертывания и установки компонентов приложения

Схема развертывания и установки компонентов приложения определяется планируемой нагрузкой на серверы приложения.

Вы можете установить один или несколько компонентов Central Node. При установке нескольких компонентов Central Node вы можете использовать их независимо друг от друга или объединить для централизованного управления в режиме распределенного решения.

Выбор схемы развертывания зависит от используемой функциональности приложения. Все приведенные в данном руководстве схемы применимы также для развертывания приложения на виртуальной платформе.

Полная функциональность (KATA, NDR и KEDR)

При использовании функциональности KATA, NDR и KEDR вы можете проверять сетевой и почтовый трафик, а также данные на компьютерах локальной сети организации.

Если в организации используется более 5000 хостов с компонентом Endpoint Agent, не рекомендуется использовать компонент Central Node для обработки трафика.

> Вы можете использовать компонент Sensor в качестве прокси-сервера для соединения компонентов Endpoint Agent, подключенных к функциональному блоку KEDR, и Central Node. Один компонент Sensor поддерживает подключение до 1000 хостов с компонентом Endpoint Agent.

Критерии выбора схемы развертывания при использовании функциональности KATA, NDR и KEDR представлены в таблице ниже. Алгоритм выбора следующий:

1. В каждой строке таблицы выберите ячейку со значением критерия, соответствующим вашей IT-инфраструктуре.

   Если в строке две ячейки с одинаковым значением, необходимо выбрать левую ячейку.

2. Выберите самую правую колонку, в которой есть отмеченные ячейки.

Выбор схемы развертывания при использовании функциональности KATA, NDR и KEDR

Критерий	Схема на два сервера	Схема на три сервера	Схема на четыре и более сервера	Распределенное решение
Сетевой и почтовый трафик не может быть принят на одном устройстве	Нет	Да	Да	Да
Количество хостов с компонентом Endpoint Agent	Нет	От 5000 до 10000	От 5000 до 10000	Более 10000
Пропускная способность канала связи	1 Гбит/с	От 1 до 2 Гбит/с	Более 2 Гбит/с	Более 2 Гбит/с
Количество удаленных инфраструктур, в которых требуется анализировать трафик	Нет	Одна	Две и более	Две и более
Мощности одного компонента Sandbox недостаточно для анализа всех объектов в приемлемые сроки	Нет	Нет	Да	Да

В режиме распределенного решения каждый из компонентов приложения должен отвечать аппаратным требованиям, указанным в калькуляторе масштабирования.

Обработка сетевого, почтового и веб-трафика (KATA и NDR)

Функциональность KATA и NDR рекомендуется использовать, если в организации нет необходимости обрабатывать данные на компьютерах локальной сети организации. В этом случае обрабатывается только сетевой и почтовый трафик.

Критерии выбора схемы развертывания при использовании функциональности KATA представлены в таблице ниже. Алгоритм выбора следующий:

1. В каждой строке таблицы выберите ячейку со значением критерия, соответствующим вашей IT-инфраструктуре.

   Если в строке две ячейки с одинаковым значением, необходимо выбрать левую ячейку.

2. Выберите самую правую колонку, в которой есть отмеченные ячейки.

Выбор схемы развертывания при использовании функциональности KATA

Критерий	Схема на два сервера	Схема на три сервера	Схема на четыре и более серверов
Сетевой и почтовый трафик не может быть принят на одном устройстве	Нет	Да	Да
Пропускная способность канала связи	1 Гбит/с	От 1 до 2 Гбит/с	Более 2 Гбит/с
Количество удаленных инфраструктур, в которых требуется анализировать трафик	Нет	Одна	Две и более
Мощности одного компонента Sandbox недостаточно для анализа всех объектов в приемлемые сроки	Нет	Нет	Да

Обработка данных с компьютеров локальной сети организации (KEDR)

Функциональность KEDR рекомендуется использовать, если в организации нет необходимости обрабатывать трафик. В этом случае обрабатываются только данные на компьютерах локальной сети организации.

В зависимости от наличия в организации стороннего решения Sandbox вы можете использовать одну из следующих схем развертывания:

- схема без компонента Sandbox;
- схема с компонентом Sandbox.

Схема развертывания на два сервера

При использовании функциональности KATA и KEDR вы можете установить компонент Endpoint Agent на компьютерах локальной сети организации. При использовании функциональности KATA компонент Endpoint Agent не устанавливается.

При использовании этой схемы развертывания компоненты Central Node и Sensor устанавливаются на одном сервере или кластере. Этот сервер или кластер принимает трафик, выполняет первичный анализ трафика и более глубокий анализ извлеченных файлов. По результатам проверки компоненты выявляют признаки целевых атак на IT-инфраструктуру организации.

На другом сервере устанавливается компонент Sandbox.

Схема работы приложения при развертывании на два сервера представлена на рисунке ниже.

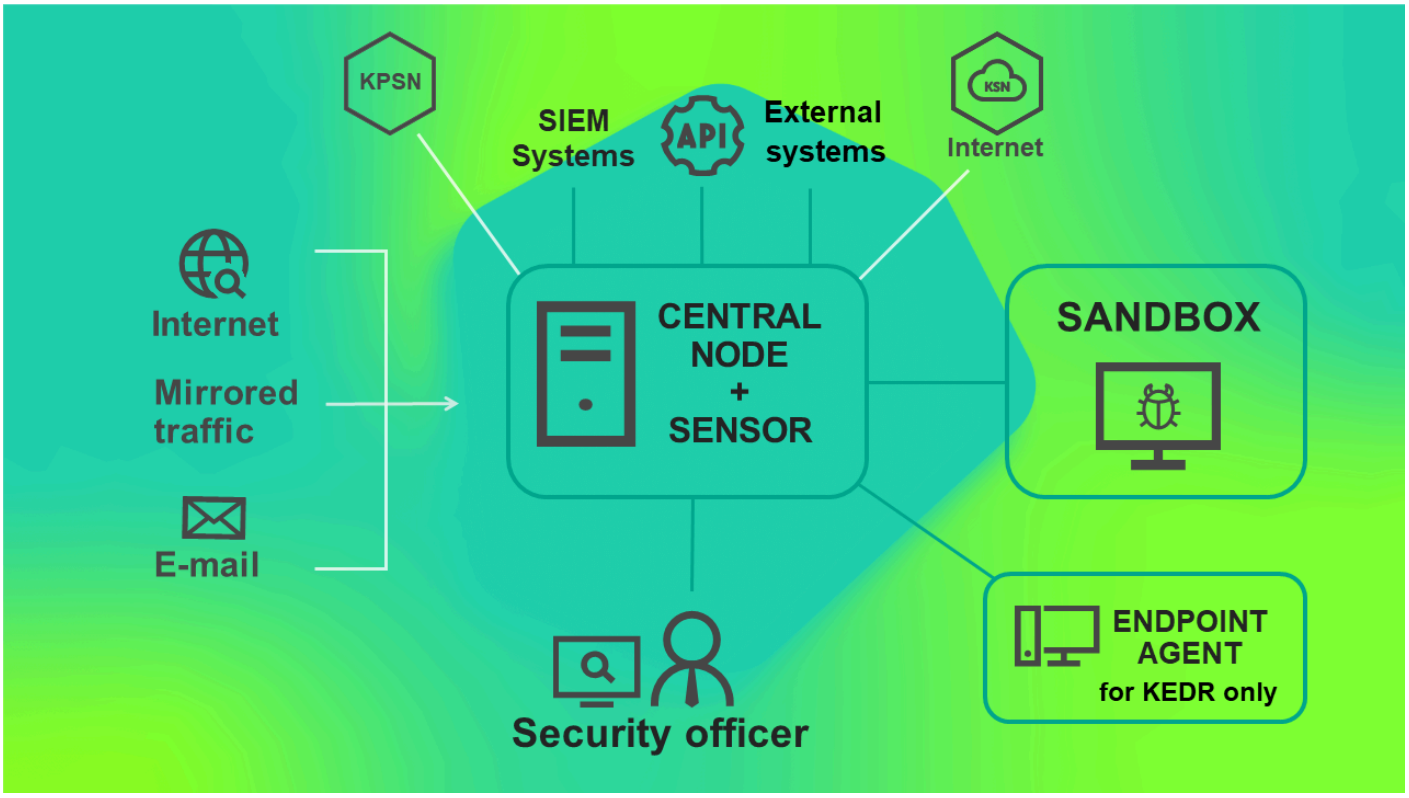


Схема работы приложения при развертывании на два сервера

Схема развертывания на три сервера

При использовании функциональности KATA и KEDR вы можете установить компонент Endpoint Agent на компьютерах локальной сети организации. При использовании функциональности KATA компонент Endpoint Agent не устанавливается.

При использовании этой схемы развертывания компоненты Sensor, Central Node и Sandbox устанавливаются на отдельных серверах. Компонент Central Node также может быть развернут в виде кластера. Sensor принимает трафик, выполняет первичный анализ, извлекает файлы и пересылает их компоненту Central Node для более глубокого анализа.

При такой схеме развертывания компонент Central Node может принимать трафик и выполнять первичный анализ данных в основной инфраструктуре. В этом случае вы можете установить компонент Sensor на сервере удаленной инфраструктуры, трафик которой требуется анализировать. Если пропускная способность канала в основной инфраструктуре составляет более 2 Гбит/с, то Sensor рекомендуется устанавливать в основной инфраструктуре.

Трафик, передаваемый между компонентами Central Node и Sensor, составляет до 20% трафика, получаемого компонентом Sensor.

Схема работы приложения при развертывании на три сервера представлена на рис. ниже.

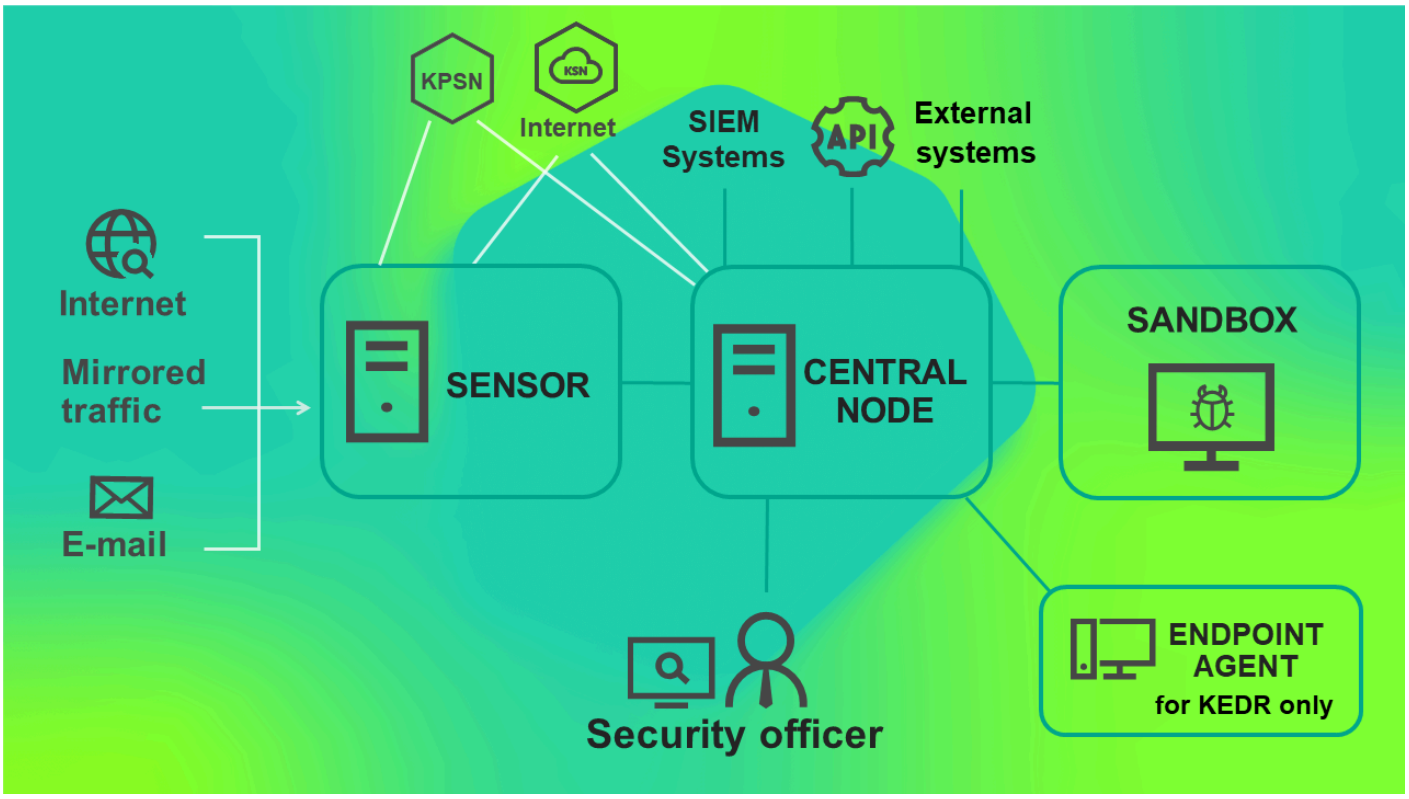


Схема работы приложения при развертывании на три сервера

Схема развертывания на четыре и более сервера

При использовании функциональности KATA и KEDR вы можете установить компонент Endpoint Agent на компьютерах локальной сети организации. При использовании функциональности KATA компонент Endpoint Agent не устанавливается.

При большом объеме трафика вы можете установить несколько компонентов Sensor или несколько компонентов Sandbox на разных серверах. Эта схема рекомендуется для развертывания в крупных организациях.

Вы также можете использовать один компонент Sandbox для подключения к нескольким компонентам Central Node.

Схема работы приложения при развертывании на четыре и более сервера представлена на рисунке ниже.

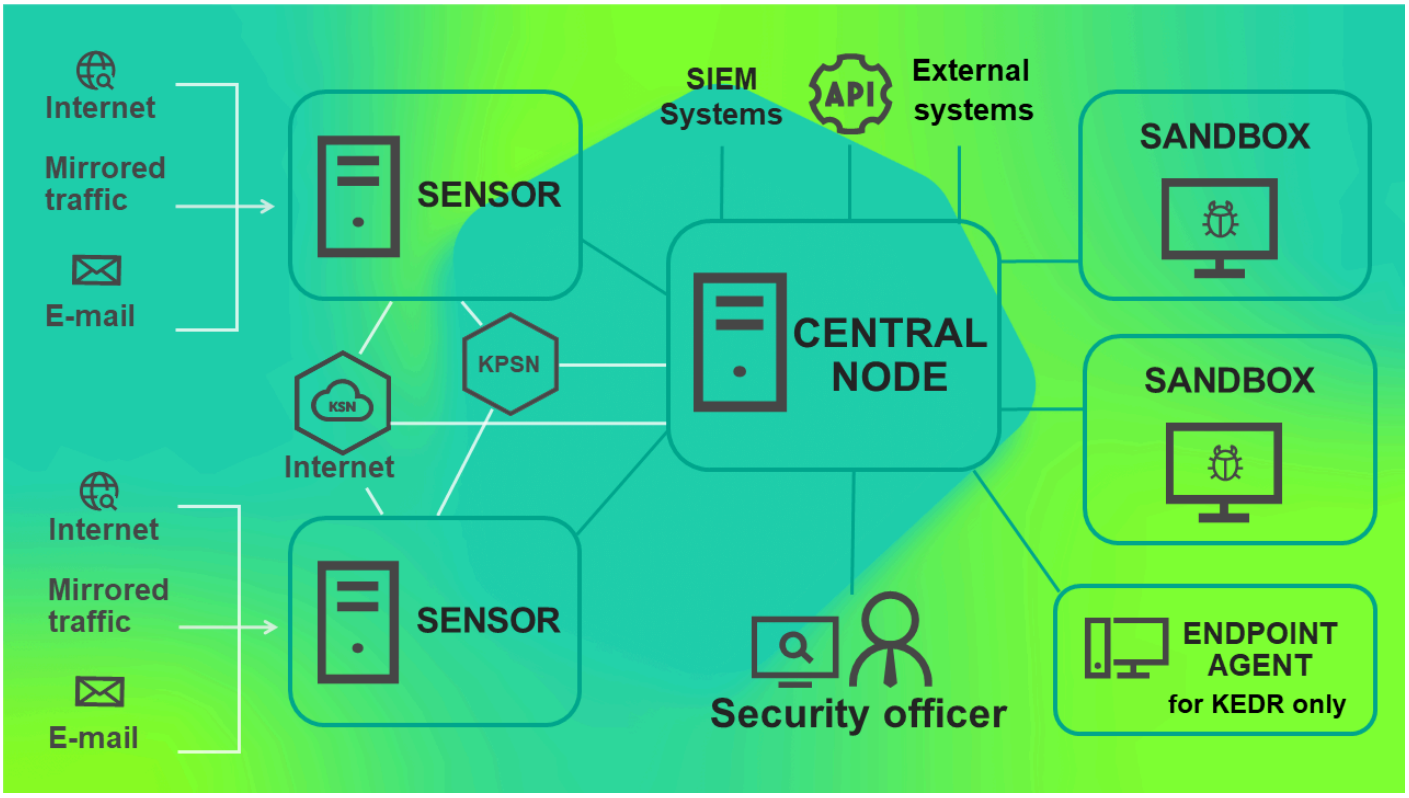


Схема работы приложения при развертывании на четыре и более сервера

Схема развертывания функциональности KEDR с компонентом Sandbox

При такой схеме развертывания вам требуется установить компонент Central Node отдельно от компонента Sensor.

Схема работы приложения при развертывании функциональности KEDR с компонентом Sandbox представлена на рисунке ниже.

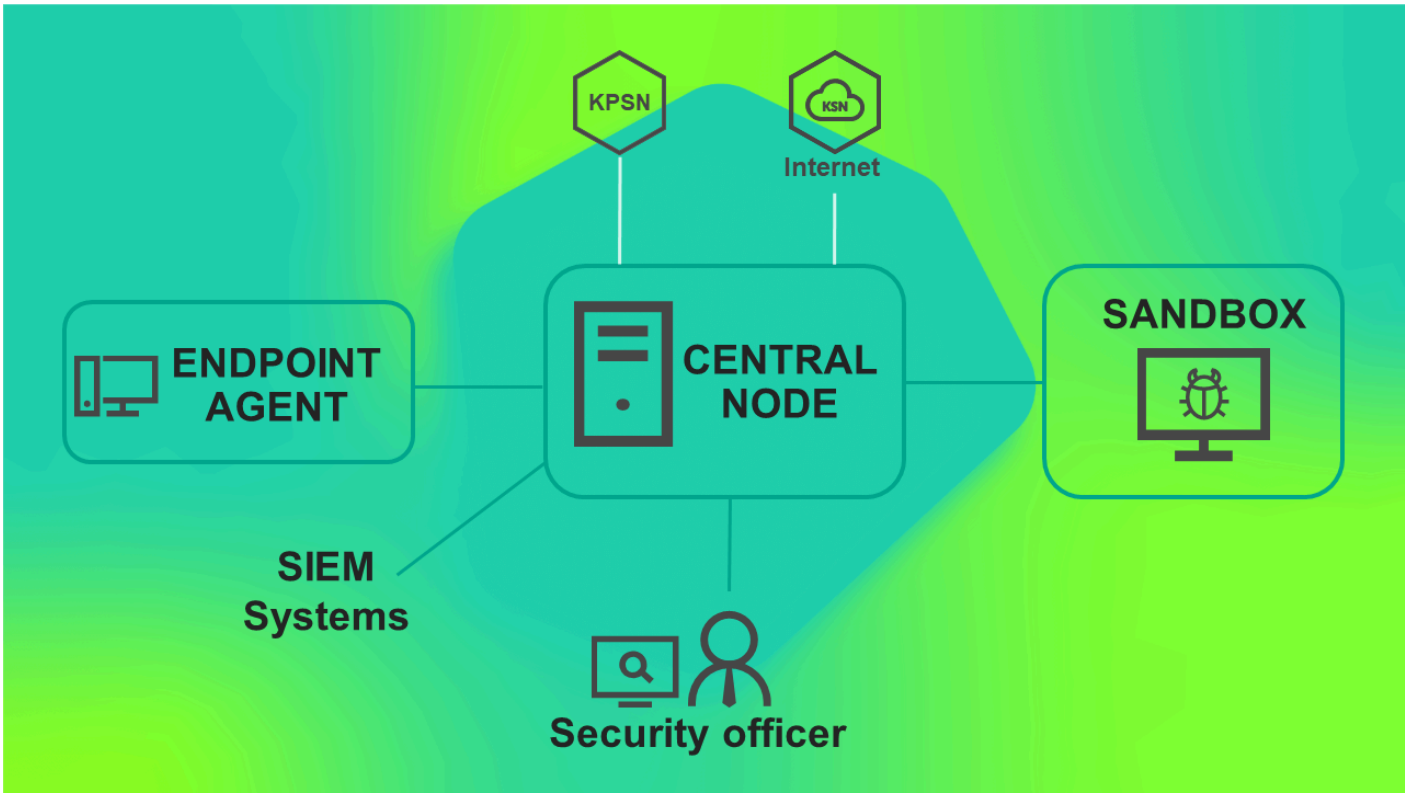


Схема работы приложения при развертывании функциональности KEDR с компонентом Sandbox

Схема развертывания функциональности KEDR без компонента Sandbox

Вы можете не устанавливать компонент Sandbox и использовать компонент Central Node только для управления компонентом Endpoint Agent и анализа данных.

При такой схеме развертывания вам требуется установить компонент Central Node отдельно от компонента Sensor.

Схема работы приложения при развертывании функциональности KEDR без компонента Sandbox представлена на рис. ниже.

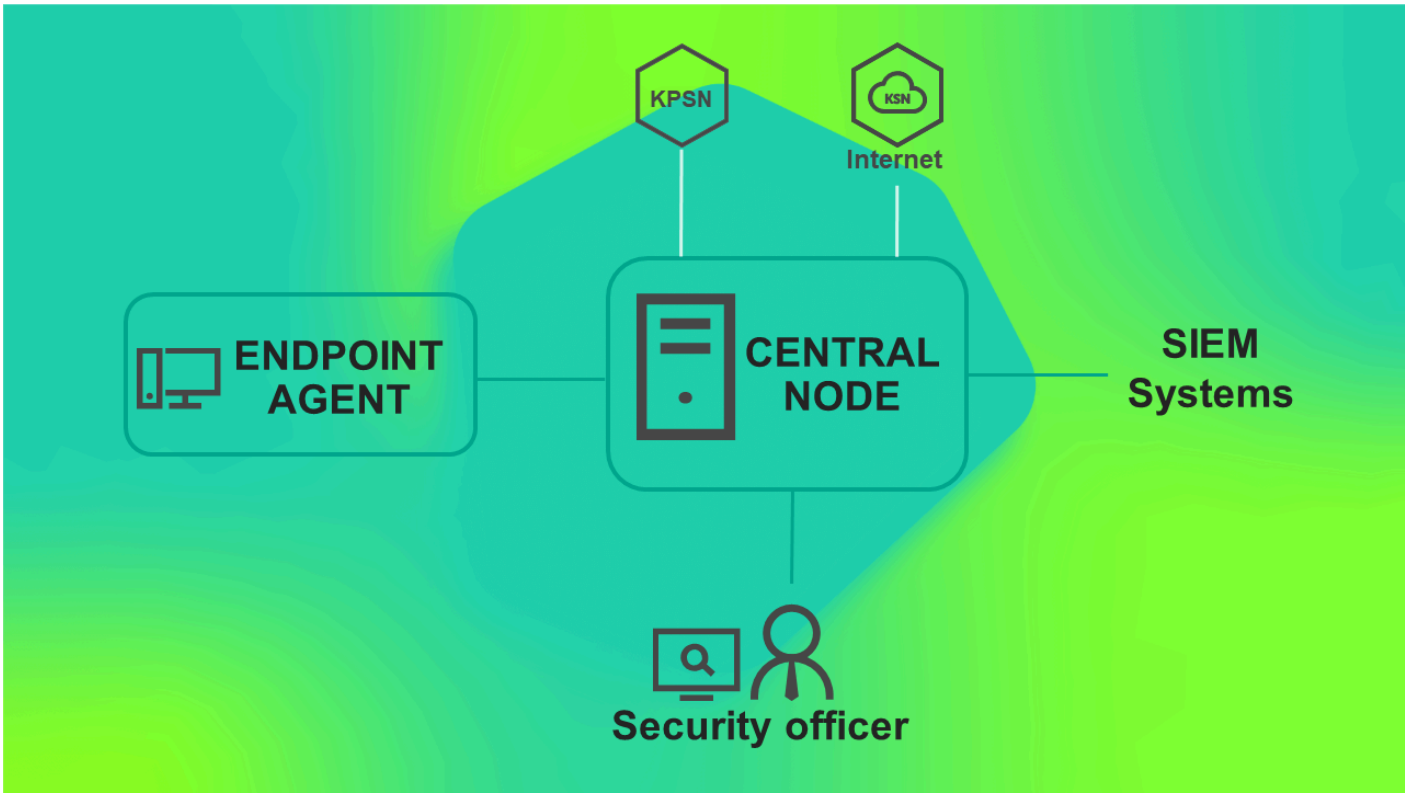


Схема работы приложения при развертывании функциональности KEDR без компонента Sandbox

Калькулятор масштабирования

После того, как вы выбрали схему развертывания, наиболее подходящую для вашей IT-инфраструктуры, вам требуется рассчитать аппаратные требования к серверам для установки компонентов приложения.

Аппаратные требования к серверам для установки компонента Central Node версии 7.1 отличаются от аналогичных аппаратных требований для предыдущей версии компонента. Мы настоятельно рекомендуем убедиться, что конфигурация серверов соответствует требованиям, приведенным в разделах Расчеты для компонента Central Node при использовании функциональности KATA, Расчеты для компонента Central Node при использовании функциональности KEDR, Расчеты для компонента Central Node при использовании функциональности KATA и KEDR, Расчеты для компонента Central Node при использовании функциональности KATA и NDR, Расчеты для компонента Central Node при использовании функциональности KATA, KEDR и NDR.

При необходимости вы можете использовать приложение версии 7.1.7 на оборудовании, предназначенном для приложения версии 5.1.

В этом случае действуют следующие ограничения:

- Вы можете использовать только функции приложения, доступные в версии 5.1. Если вы хотите использовать функционал других версий приложения, аппаратные характеристики серверов Central Node должны соответствовать аппаратным требованиям, приведенным в онлайн-справке для этих версий.

  Список новых функций Kaspersky Anti Targeted Attack Platform 6.0 - 8.0 приведен в разделе *Что нового* онлайн-справки соответствующей версии.

- Приложение должно быть развернуто на базе операционной системы Ubuntu Server.
- Вы можете использовать только лицензионные ключи KATA и/или KEDR.
- Обновление приложения с версии 5.1 до версии 7.1.7 возможно, только если центральный процессор сервера Central Node поддерживает наборы инструкций BMI2, AVX and AVX2. Если перечисленные наборы инструкций не поддерживаются, вы можете установить приложение версии 7.1 из дистрибутива и обновить его до версии 7.1.7.

  Обновление выполняется последовательно с версии 5.1: 5.1 → 6.0, 6.0 → 6.0.2, 6.0.2 → 6.1, 6.1 → 7.0.3, 7.0.3 → 7.1.1, 7.1.1 → 7.1.3, 7.1.3 → 7.1.7.

Расчеты для компонента Sensor

При расчете аппаратных требований к компоненту Sensor требуется учитывать, что максимальный объем обрабатываемого трафика составляет 10 Гбит/с. Для обработки трафика максимального объема можно использовать как один Sensor, установленный на отдельном сервере, так и несколько Sensor, установленных на отдельных серверах, которые подключены к одному Central Node. Суммарный объем передаваемого трафика от всех Sensor, подключенных к одному серверу Central Node, не должен превышать 10 Гбит/с.

> При наличии в сети более одного сегмента с пропускной способностью 10 Гбит/с и при необходимости обрабатывать трафик в этих сегментах, вам необходимо использовать режим распределенного решения.

Вы можете использовать сервер Sensor в качестве прокси-сервера при обмене данными между рабочими станциями с Endpoint Agent и Central Node (при интеграции с функциональным блоком KEDR), чтобы упростить настройку сетевых правил. Например, если рабочие станции с Endpoint Agent находятся в отдельном сегменте сети, то будет достаточно настроить соединение между серверами Central Node и Sensor.

При использовании Sensor в качестве прокси-сервера при обмене данными между компонентами Endpoint Agent и компонентом Central Node учитывайте следующие ограничения:

- Максимальное количество рабочих станций с компонентом Endpoint Agent, подключенных к одному компоненту Central Node, составляет 15 000.
- Максимально допустимые потери пакетов, пересылаемых между серверами Sensor и Central Node, составляют 10% при задержке отправки пакетов до 100 мс.

Требуемая пропускная способность канала связи между серверами Central Node и Sensor зависит от объема обрабатываемого трафика и определяется по следующей формуле:

```
10% от трафика на SPAN-порте при обычной нагрузке или 20% от трафика на SPAN-порте при пиковой нагрузке + почтовый трафик + трафик по протоколу ICAP + требования к каналу связи между Central Node и Endpoint Agent
```

Аппаратные требования к серверу Sensor

Компонент Sensor может быть интегрирован с IT-инфраструктурой организации следующими способами:

- получение зеркалированного трафика от сетевых устройств со SPAN-портов;
- подключение к почтовому серверу по протоколу POP3;
- подключение к почтовому серверу по протоколу SMTP;
- получение трафика от прокси-сервера по протоколу ICAP;
- получение данных от компонента Endpoint Agent.

Аппаратные требования к серверу Sensor приведены в таблицах ниже.

Тестирование компонента Sensor на виртуальных платформах проводилось с нагрузкой до 1000 Мбит/с включительно, однако виртуальные платформы поддерживают больший объем нагрузки. Если вы хотите развернуть компонент Sensor на виртуальной платформе и планируете обрабатывать трафик объемом до 1000 Мбит/с, для расчета аппаратных требований к серверу Sensor вы можете использовать таблицу ниже. Если вы планируете обрабатывать больший объем трафика, обратитесь за расчетами аппаратных требований к вашему аккаунт-менеджеру.

Аппаратные требования к серверу Sensor в зависимости от объема обрабатываемого трафика со SPAN-портов при использовании функциональности KATA и KEDR

Количество компонентов Endpoint Agent (интеграция с функциональным блоком KEDR)	Объем обрабатываемого трафика (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер
10000	100	20	6
15000	500	24	10
15000	1000	32	14
15000	2000	48	20
15000	4000	56	30
15000	7000	128	44
15000	10000	160	60

Аппаратные требования к серверу Sensor в зависимости от объема обрабатываемого трафика со SPAN-портов при использовании функциональности KATA и NDR

Объем обрабатываемого трафика (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Минимальное количество логических ядер при сохранении дампов зеркалированного трафика
100	28	6	8
500	32	12	14
1000	40	16	18
2000	64	24	26
4000	80	36	40
7000	160	52	56
10000	192	72	76

Если Sensor используется в качестве сервера для телеметрии NDR, которую отправляют не более чем 2000 хостов с компонентом Endpoint Agent, дополнительно потребуется 2 логических ядра и 4 ГБ оперативной памяти.

Центральный процессор должен поддерживать набор инструкций BMI2, AVX и AVX2.

Если вы хотите обрабатывать только сообщения электронной почты и не обрабатывать зеркалированный трафик со SPAN-портов, мы рекомендуем использовать Sensor, установленный на одном сервере с Central Node.

Если один сервер Sensor обрабатывает трафик по нескольким протоколам, то для расчета конфигурации сервера необходимо учитывать, что при настроенной интеграции с почтовым сервером или почтовым сенсором необходимо выключить обработку трафика по протоколу SMTP.

Требования к дисковому пространству на сервере Sensor

Рекомендуется использовать дисковый массив RAID 1. Общий объем дискового пространства должен составлять не менее 600 ГБ.

Аппаратные требования к Sensor при сохранении дампов зеркалированного трафика со SPAN-портов

Если вы используете функционал сохранения дампов зеркалированного трафика со SPAN-портов, вам необходимо дополнительно увеличить следующие аппаратные характеристики сервера Sensor:

- Установить отдельное дисковое хранилище в виде пула RAID-массива или DAS с максимальной пропускной способностью, определяемой по формуле:

  `<пропускная способность дискового хранилища> = 3 * <максимальный объем записываемого трафика>`

- Емкость дискового хранилища определяется от желаемого времени хранения и максимального объема сохраняемого трафика с учетом фильтров. По примерным расчетам, для хранения записанного трафика максимальным объемом 10 Гбит/с в течении 7 дней, необходимо дисковое хранилище емкостью 750 ТиБ.

Расчеты для компонента Central Node при использовании функциональности KATA

В этом разделе описываются программные и аппаратные требования к физическим и виртуальным серверам Central Node при использовании функциональности KATA.

Аппаратные требования к физическому серверу Central Node

Аппаратные требования к физическому серверу Central Node зависят от следующих условий:

- объем обрабатываемого трафика;

  Поступление расшифрованного SSL/TLS-трафика в Kaspersky Anti Targeted Attack Platform увеличивает нагрузку по его обработке в 5 раз по сравнению с нерасшифрованным трафиком (стандартным трафиком, поступающим со SPAN-портов). В этом случае объем обрабатываемого трафика для расчета нагрузки на сервер определяется по следующей формуле:

  `<объем расшифрованного трафика> = 5 * <объем нерасшифрованного трафика>`

  Объем трафика, обрабатываемого на ICAP-сервере, рассчитывается согласно таблице, приведенной в разделе Расчеты для Central Node при использовании функциональности ICAP.

- количество обрабатываемых сообщений электронной почты в секунду.

При объеме обрабатываемого трафика более 1 Гбит/с необходимо устанавливать компоненты Central Node и Sensor на отдельных серверах.

Аппаратные требования к физическому серверу Central Node приведены в таблице ниже.

Аппаратные требования к физическому серверу Central Node

Максимальное количество сообщений электронной почты в секунду	Максимальный объем SPAN-трафика на встроенном Sensor (Мбит/с)	Максимальный объем SPAN-трафика на отдельном Sensor (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая подсистема (RAID 1 или RAID 10)			
					ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива (ТБ)	Количество дисков в массиве
2	500	Не обрабатывается	72	24	100	1000	2	4
2	1000	Не обрабатывается	88	32	100	1000	2	4
5	Не обрабатывается	2000	64	32	100	1000	2	2
20	Не обрабатывается	4000	80	56	100	1000	3	2
20	Не обрабатывается	7000	112	92	200	1500	4	2
20	Не обрабатывается	10 000	128	128	200	1500	4	2

Kaspersky Anti Targeted Attack Platform не поддерживает работу с программным RAID-массивом.

Аппаратные требования к виртуальному серверу Central Node

При установке компонента на виртуальной платформе VMware ESXi вам нужно увеличить минимальное количество логических ядер, приведенное в таблицах с аппаратными требованиями к физическому серверу Central Node, на 10%.

Если вы хотите установить Central Node на виртуальных платформах ПК СВ "Брест", "РЕД Виртуализация", KVM или zVirt Node вам нужно увеличить минимальное количество логических ядер на 40%. Если вы хотите устранить уязвимости типа Spectre и Meltdown на уровне операционной системы гипервизора, то вам нужно дополнительно увеличить минимальное количество логических ядер в 1,5 раза.

Остальные требования к аппаратному обеспечению для виртуальных серверов аналогичны требованиям для физических серверов.

Тестирование Central Node на виртуальных платформах проводилось с нагрузкой до 1000 Мбит/с включительно.

Программные требования к виртуальному серверу Central Node

В параметрах виртуального диска должен быть выбран тип диска Thick Provision Eager Zeroed.

Чтобы избежать возможного снижения производительности при развертывании приложения на виртуальной платформе, требуется выполнить следующие действия:

- Установить параметры High Latency Sensitivity.

  Если ваш гипервизор не поддерживает High Latency Sensitivity, вы можете использовать другие механизмы приоритизации виртуальных машин, например, функцию CPU Affinity и резервирование ресурсов.

- Зарезервировать всю оперативную память.

- Зарезервировать всю частоту процессора.

Дополнительные требования к серверам Central Node

Дополнительные аппаратные требования к физическим серверам Central Node приведены в разделах Расчеты для компонента Central Node при наличии интегрированных внешних систем, Расчеты для компонента Central Node при использовании функциональности ICAP, Расчеты для компонента Central Node в режиме распределенного решения и мультитенантности, Расчеты для компонента Central Node, развернутого в виде кластера.

Расчеты для компонента Central Node при использовании функциональности KEDR

В этом разделе описываются программные и аппаратные требования к физическим и виртуальным серверам Central Node при использовании функциональности KEDR.

Аппаратные требования к физическому серверу Central Node

Аппаратные требования к физическому серверу Central Node приведены в таблицах ниже.

Далее в разделе в столбце *Максимальное количество Endpoint Agents* приводятся значения для компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Windows. Эквивалентное количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционных систем Linux, macOS, а также установленных на серверах, рассчитывается по следующим формулам:

- B = <максимальное количество Endpoint Agents>/2, где "B" – количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Linux;
- C = <максимальное количество Endpoint Agents>/3, где "C" – количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы macOS;
- D = <максимальное количество Endpoint Agents>/20, где "D" – количество компонентов Endpoint Agent, установленных на серверах.

Аппаратные требования к физическому серверу Central Node

Максимальное количество Endpoint Agents	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая подсистема (RAID 1 или RAID 10)				Вторая дисковая подсистема RAID 10)	
			ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива (ТБ)	Количество дисков в массиве	ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)
1000	96	24	100	1000	2	4	300	300
2000	128	32	100	1000	2	4	700	700
5000	160	48	100	1200	2	4	1000	900
10 000	224	60	100	1200	2	4	1500	1200
5000	160	52	100	1200	2	4	1000	900
10 000	224	90	100	1500	2	4	1500	**200**
15 000	288	104	100	1500	2	4	1500	1600
15 000	320	140	200	2000	2	4	1500	1600
15 000	336	176	200	2000	2	4	1500	1600

Если вы хотите использовать процессор с частотой 2.1 ГГц, аппаратные характеристики сервера Central Node должны соответствовать требованиям, приведенным в таблице ниже.

Аппаратные требования к физическому серверу Central Node при использовании процессора с частотой 2.1 ГГц

Максимальное количество Endpoint Agents	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 2.1 ГГц	Первая дисковая подсистема (RAID 1 или RAID 10)				Вторая дисковая подсистема (RAID 10 или аппаратный RAID 5 с кешем и батареей)	
			ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива (ТБ)	Количество дисков в массиве	ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)
1000	64	18	100	250	1	4	300	300
3000	96	24	100	500	1	4	700	750

Максимальное количество Endpoint Agents	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 2.1 ГГц	Первая дисковая подсистема (RAID 1 или RAID 10)				Вторая дисковая подсистема (RAID 10 или аппаратный RAID 5 с кешем и батареей)	
			ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива (ТБ)	Количество дисков в массиве	ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)
5000	112	28	100	500	1	4	1000	900
10 000	160	52	100	500	1	4	1500	1200
15 000	224	72	100	750	1	4	1500	1600

При необходимости вы можете снизить нагрузку на Central Node, ограничив объем данных событий (телеметрию), поступающих от Endpoint Agent. В этом случае аппаратные характеристики сервера Central Node должны соответствовать требованиям, приведенным в таблице ниже.

Аппаратные требования к физическому серверу Central Node при ограниченном составе телеметрии

Максимальное количество Endpoint Agents	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая подсистема (RAID 1 или RAID 10)				Вторая дисковая подсистема RAID 10)	
			ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива (ТБ)	Количество дисков в массиве	ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)
1000	64	10	100	250	1	4	300	250
3000	80	14	100	500	1	4	500	500
5000	96	16	100	500	1	4	700	600
10 000	144	24	100	500	1	4	1000	800
15 000	192	32	100	500	1	4	1500	1000

В таблице ниже приводятся аппаратные требования к физическому серверу Central Node при использовании функции проверки цепочек событий.

Аппаратные требования к физическому серверу Central Node при включенной проверке цепочек событий

Максимальное количество Endpoint Agents	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 2.1 ГГц	Первая дисковая подсистема (RAID 1 или RAID 10)				Вторая дисковая подсистема (RAID 10 или аппаратный RAID 5 с кешем и батареей)	
			ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива (ТБ)	Количество дисков в массиве	ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)
1000	64	12	100	250	1	4	300	300
3000	96	16	100	500	1	4	700	750
5000	112	20	100	500	1	4	1000	900
10 000	160	34	100	500	1	4	1500	1200
15 000	224	48	100	750	1	4	1500	1600
20 000*	256	64	150	75	1	4	2000	2000

* Рекомендуется использовать SSD-диски.

Kaspersky Anti Targeted Attack Platform не поддерживает работу с программным RAID-массивом.

Аппаратные требования к виртуальному серверу Central Node

Приведенные ниже значения актуальны при подключении к Central Node до 10 000 компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Windows.

При установке компонента на виртуальной платформе VMware ESXi вам нужно увеличить минимальное количество логических ядер, приведенное в таблицах с аппаратными требованиями к физическому серверу Central Node, на 10%.

Если вы хотите установить Central Node на виртуальных платформах ПК СВ "Брест", "РЕД Виртуализация", KVM, zVirt Node или Nutanix Acropolis Operating System, вам нужно увеличить минимальное количество логических ядер на 30%. Если вы хотите устранить уязвимости типа Spectre и Meltdown на уровне операционной системы гипервизора, то вам нужно дополнительно к этим 30% увеличить минимальное количество логических ядер в 1,5 раза.

Остальные требования к аппаратному обеспечению для виртуальных серверов аналогичны требованиям для физических серверов.

Программные требования к виртуальному серверу Central Node

В параметрах виртуального диска должен быть выбран тип диска Thick Provision Eager Zeroed.

Чтобы избежать возможного снижения производительности при развертывании приложения на виртуальной платформе, требуется выполнить следующие действия:

- Установить параметры High Latency Sensitivity.

  Если ваш гипервизор не поддерживает High Latency Sensitivity, вы можете использовать другие механизмы приоритизации виртуальных машин, например, функцию CPU Affinity и резервирование ресурсов.

- Зарезервировать всю оперативную память.

- Зарезервировать всю частоту процессора.

Требования к объему второй дисковой подсистемы на сервере Central Node

Общий минимальный эффективный объем второй дисковой подсистемы определяется по следующей формуле:

E = 1,5 * (P+T+S)

где

- "E" – общий минимальный эффективный объем второй дисковой подсистемы.
- "P" – объем постоянного хранилища, который определяется по следующей формуле:

  30 МБ * <эффективное количество хостов с компонентом Endpoint Agent> * <срок хранения в днях>.

  Объем постоянного хранилища не должен превышать 20 ТБ.
- "T" – объем временного хранилища, который вычисляется по следующей формуле:

  27 МБ * <эффективное количество хостов с компонентом Endpoint Agent>.

  Если вы включили проверку цепочек событий, то объем временного хранилища вычисляется по следующей формуле:

  40 МБ * <эффективное количество хостов с компонентом Endpoint Agent>.
- "S" – объем для системных файлов, который составляет 150 ГБ.

Эта формула может быть использована для примерной оценки требуемого дискового пространства. Реальный объем хранимых данных зависит от профиля трафика организации и может отличаться от полученного результата вычислений.

Дополнительные требования к оперативной памяти в зависимости от объема постоянного хранилища:

- При объеме хранилища 10-15 ТБ добавьте 16 ГБ к минимальному объему оперативной памяти, приведенному в таблиц*ах* выше.
- При объеме хранилища 15-20 ТБ добавьте 32 ГБ к минимальному объему оперативной памяти, приведенному в таблиц*ах* выше.

Требования к каналам связи

Необходимо обеспечить пропускную способность канала связи между сервером Central Node и каждым сегментом сети в зависимости от количества хостов Endpoint Agent в сегменте. Пропускная способность в зависимости от количества хостов Endpoint Agent приведена в таблице ниже.

Пропускная способность канала связи в зависимости от количества хостов Endpoint Agent

Максимальное количество Endpoint Agents	Требуемая пропускная способность канала связи, зарезервированная для Endpoint Agents (Мбит/с)
10	1
50	2
100	3
1000	20
10 000	200

Дополнительные требования к серверам Central Node

Дополнительные аппаратные требования к физическим серверам Central Node приведены в разделах Расчеты для компонента Central Node при наличии интегрированных внешних систем, Расчеты для компонента Central Node при использовании функциональности ICAP, Расчеты для компонента Central Node в режиме распределенного решения и мультитенантности, Расчеты для компонента Central Node, развернутого в виде кластера.

Расчеты для компонента Central Node при использовании функциональности KATA и KEDR

В этом разделе описываются программные и аппаратные требования к физическим и виртуальным серверам Central Node при использовании функциональности KATA и KEDR.

Аппаратные требования к физическому серверу Central Node

Аппаратные требования к физическому серверу Central Node зависят от следующих условий:

- объем обрабатываемого трафика;

  Поступление расшифрованного SSL/TLS-трафика в Kaspersky Anti Targeted Attack Platform увеличивает нагрузку по его обработке в 5 раз по сравнению с нерасшифрованным трафиком (стандартным трафиком, поступающим со SPAN-портов). В этом случае объем обрабатываемого трафика для расчета нагрузки на сервер определяется по следующей формуле:

  ```
  <объем расшифрованного трафика> = 5 * <объем нерасшифрованного трафика>
  ```

  Объем трафика, обрабатываемого на ICAP-сервере, рассчитывается согласно таблице, приведенной в разделе Расчеты для Central Node при использовании функциональности ICAP.

- количество обрабатываемых сообщений электронной почты в секунду;

- количество хостов с компонентом Endpoint Agent.

  Компонент Endpoint Agent может быть установлен на рабочую станцию, терминальный сервер, файловый сервер или в сетевое хранилище (NAS).

  Совместимость версий приложений, которыми представлен компонент Endpoint Agent, с версиями Kaspersky Anti Targeted Attack Platform см. в следующих разделах справки: Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac.

  Эффективное количество хостов с компонентом Endpoint Agent для расчета нагрузки на сервер определяется по следующей формуле:

  ```
  K = A+2*B+3*C+20*D
  ```

  где

  - "K" – эффективное количество хостов с компонентом Endpoint Agent.

  - "A" – количество рабочих станций и пользователей терминальных серверов под управлением операционной системы Windows с установленным компонентом Endpoint Agent.

- "B" – количество рабочих станций и пользователей терминальных серверов под управлением операционной системы Linux с установленным компонентом Endpoint Agent.
- "C" – количество рабочих станций и пользователей терминальных серверов под управлением операционной системы macOS с установленным компонентом Endpoint Agent.
- "D" – количество серверов.

При объеме обрабатываемого трафика более 1 Гбит/с необходимо устанавливать компоненты Central Node и Sensor на отдельных серверах.

Аппаратные требования к физическому серверу Central Node представлены в таблице ниже.

Далее в разделе в столбце *Максимальное количество Endpoint Agents* приводятся значения для компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Windows. Эквивалентное количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционных систем Linux, macOS, а также установленных на серверах, рассчитывается по следующим формулам:

- B = <максимальное количество Endpoint Agents>/2, где "B" – количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Linux;
- C = <максимальное количество Endpoint Agents>/3, где "C" – количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы macOS;
- D = <максимальное количество Endpoint Agents>/20, где "D" – количество компонентов Endpoint Agent, установленных на серверах.

Аппаратные требования к физическому серверу Central Node

Максимальное количество Endpoint Agents	Максимальное количество сообщений электронной почты в секунду	Максимальный объем SPAN-трафика на встроенном Sensor (Мбит/с)	Максимальный объем SPAN-трафика на отдельном Sensor (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая г (RAID 1 или R		
						ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	ди м
1000	1	200	Не обрабатывается	96	24	100	1000	
2000	2	500	Не обрабатывается	128	32	100	1000	
5000	1	1000	Не обрабатывается	160	48	100	1200	
10 000	2	1000	Не обрабатывается	224	60	100	1200	
5000	5	Не обрабатывается	2000	160	52	100	1200	
10 000	20	Не обрабатывается	4000	224	90	100	1500	
15 000	20	Не обрабатывается	4000	288	104	100	1500	
15 000	20	Не обрабатывается	7000	320	140	200	2000	
15 000	20	Не обрабатывается	10 000	336	176	200	2000	

В таблице ниже приводятся аппаратные требования к физическому серверу Central Node при использовании функции проверки цепочек событий.

Аппаратные требования к физическому серверу Central Node при включенной проверке цепочек событий

Максимальное количество Endpoint Agents	Максимальное количество сообщений электронной почты в секунду	Максимальный объем SPAN-трафика на встроенном Sensor (Мбит/с)	Максимальный объем SPAN-трафика на отдельном Sensor (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая подс (RAID 1 или RAID 1		
						ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объ диско масс (ТБ
1000	1	200	Не обрабатывается	144	24	100	1000	1,9
2000	2	500	Не обрабатывается	160	32	100	1000	2
5000	1	1000	Не обрабатывается	192	48	100	1000	2
10 000	2	1000	Не обрабатывается	240	64	100	1000	2
5000	5	Не обрабатывается	2000	192	60	100	1000	1,9
10 000	20	Не обрабатывается	4000	256	100	100	1000	1,9
15 000	20	Не обрабатывается	4000	304	112	100	1000	1,9
15 000	20	Не обрабатывается	7000	320	148	100	1000	1,9
15 000	20	Не обрабатывается	10 000	336	184	100	1000	1,9

Аппаратные требования к виртуальному серверу Central Node

Приведенные ниже значения актуальны при подключении к Central Node до 10 000 компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Windows.

При установке компонента на виртуальной платформе VMware ESXi вам нужно увеличить минимальное количество логических ядер, приведенное в таблицах с аппаратными требованиями к физическому серверу Central Node, на 10%.

Если вы хотите установить Central Node на виртуальной платформе ПК СВ "Брест", "РЕД Виртуализация", KVM, zVirt Node или Nutanix Acropolis Operating System, вам нужно увеличить минимальное количество логических ядер на 30%. Если вы хотите устранить уязвимости типа Spectre и Meltdown на уровне операционной системы гипервизора, то вам нужно дополнительно к этим 30% увеличить минимальное количество логических ядер в 1,5 раза.

Остальные требования к аппаратному обеспечению для виртуальных серверов аналогичны требованиям для физических серверов.

Программные требования к виртуальному серверу Central Node

В параметрах виртуального диска должен быть выбран тип диска Thick Provision Eager Zeroed.

Чтобы избежать возможного снижения производительности при развертывании приложения на виртуальной платформе, требуется выполнить следующие действия:

- Установить параметры High Latency Sensitivity.

  Если ваш гипервизор не поддерживает High Latency Sensitivity, вы можете использовать другие механизмы приоритизации виртуальных машин, например, функцию CPU Affinity и резервирование ресурсов.

- Зарезервировать всю оперативную память.

- Зарезервировать всю частоту процессора.

Требования к объему второй дисковой подсистемы на сервере Central Node

Общий минимальный эффективный объем второй дисковой подсистемы определяется по следующей формуле:

E = 1,5 * (P+T+S)

где

- "E" – общий минимальный эффективный объем второй дисковой подсистемы.

- "P" – объем постоянного хранилища, который определяется по следующей формуле:

  30 МБ * <эффективное количество хостов с компонентом Endpoint Agent> * <срок хранения в днях>.

  Объем постоянного хранилища не должен превышать 20 ТБ.

- "T" – объем временного хранилища, который вычисляется по следующей формуле:

  27 МБ * <эффективное количество хостов с компонентом Endpoint Agent>.

- Если вы включили проверку цепочек событий, то объем временного хранилища вычисляется по следующей формуле:

  40 МБ * <эффективное количество хостов с компонентом Endpoint Agent>.

- "S" – объем для системных файлов, который составляет 150 ГБ.

Эта формула может быть использована для примерной оценки требуемого дискового пространства. Реальный объем хранимых данных зависит от профиля трафика организации и может отличаться от полученного результата вычислений.

Дополнительные требования к оперативной памяти в зависимости от объема постоянного хранилища:

- При объеме хранилища 10-15 ТБ добавьте 16 ГБ к минимальному объему оперативной памяти, приведенному в таблиц*ах* выше.
- При объеме хранилища 15-20 ТБ добавьте 32 ГБ к минимальному объему оперативной памяти, приведенному в таблиц*ах* выше.

Требования к каналам связи

Необходимо обеспечить пропускную способность канала связи между сервером Central Node и каждым сегментом сети в зависимости от количества хостов Endpoint Agent в сегменте. Пропускная способность в зависимости от количества хостов Endpoint Agent приведена в таблице ниже.

Пропускная способность канала связи в зависимости от количества хостов Endpoint Agent

Максимальное количество Endpoint Agents	Требуемая пропускная способность канала связи, зарезервированная для Endpoint Agents (Мбит/с)
10	1
50	2
100	3
1000	20
10 000	200

Дополнительные требования к серверам Central Node

Дополнительные аппаратные требования к физическим серверам Central Node приведены в разделах Расчеты для компонента Central Node при наличии интегрированных внешних систем, Расчеты для компонента Central Node при использовании функциональности ICAP, Расчеты для компонента Central Node в режиме распределенного решения и мультитенантности, Расчеты для компонента Central Node, развернутого в виде кластера.

Расчеты для компонента Central Node при использовании функциональности KATA и NDR

В этом разделе описываются программные и аппаратные требования к физическим и виртуальным серверам Central Node при использовании функциональности KATA и NDR.

Аппаратные требования к физическому серверу Central Node

Аппаратные требования к физическому серверу Central Node зависят от следующих условий:

- объем обрабатываемого трафика;

Поступление расшифрованного SSL/TLS-трафика в Kaspersky Anti Targeted Attack Platform увеличивает нагрузку по его обработке в 5 раз по сравнению с нерасшифрованным трафиком (стандартным трафиком, поступающим со SPAN-портов). В этом случае объем обрабатываемого трафика для расчета нагрузки на сервер определяется по следующей формуле:

```
<объем расшифрованного трафика> = 5 * <объем нерасшифрованного трафика>
```

Объем трафика, обрабатываемого на ICAP-сервере, рассчитывается согласно таблице, приведенной в разделе Расчеты для Central Node при использовании функциональности ICAP.

- количество обрабатываемых сообщений электронной почты в секунду.

При объеме обрабатываемого трафика более 1 Гбит/с необходимо устанавливать компоненты Central Node и Sensor на отдельных серверах.

Аппаратные требования к физическому серверу Central Node приведены в таблице ниже.

Аппаратные требования к физическому серверу Central Node

Максимальное количество сообщений электронной почты в секунду	Максимальный объем SPAN-трафика на встроенном Sensor (Мбит/с)	Максимальный объем SPAN-трафика на отдельном Sensor (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая подсистема (RAID 1 или RAID 10)			
					ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива (ТБ)	Количество дисков в массиве
2	500	Не обрабатывается	96	38	100	1000	2	4
2	1000	Не обрабатывается	112	48	200	2000	2	4
5	Не обрабатывается	2000	96	44	200	2000	3	4
20	Не обрабатывается	4000	112	72	200	2000	3	4
20	Не обрабатывается	7000	144	104	300	2500	4	4
20	Не обрабатывается	10 000	160	140	300	2500	4	4

Kaspersky Anti Targeted Attack Platform не поддерживает работу с программным RAID-массивом.

При подключении до 1000 компонентов Endpoint Agent NDR аппаратные требования к серверу Central Node аналогичны приведенным в таблице выше. При подключении более 1000 компонентов Endpoint Agent NDR вам потребуется дополнительно 4 ГБ оперативной памяти и 3 логических ядра.

При установке компонента на виртуальной платформе VMware ESXi вам нужно увеличить минимальное количество логических ядер, приведенное в таблицах с аппаратными требованиями к физическому серверу Central Node, на 10%.

Остальные требования к аппаратному обеспечению для виртуальных серверов аналогичны требованиям для физических серверов.

Программные требования к виртуальному серверу Central Node

В параметрах виртуального диска должен быть выбран тип диска Thick Provision Eager Zeroed.

Чтобы избежать возможного снижения производительности при развертывании приложения на виртуальной платформе, требуется выполнить следующие действия:

- Установить параметры High Latency Sensitivity.

  Если ваш гипервизор не поддерживает High Latency Sensitivity, вы можете использовать другие механизмы приоритизации виртуальных машин, например, функцию CPU Affinity и резервирование ресурсов.

- Зарезервировать всю оперативную память.

- Зарезервировать всю частоту процессора.

Дополнительные требования к серверам Central Node

Дополнительные аппаратные требования к физическим серверам Central Node приведены в разделах Расчеты для компонента Central Node при наличии интегрированных внешних систем, Расчеты для компонента Central Node при использовании функциональности ICAP, Расчеты для компонента Central Node в режиме распределенного решения и мультитенантности, Расчеты для компонента Central Node, развернутого в виде кластера.

Расчеты для компонента Central Node при использовании функциональности KATA, KEDR и NDR

В этом разделе описываются программные и аппаратные требования к физическим и виртуальным серверам Central Node при использовании функциональности KATA, KEDR и NDR.

Аппаратные требования к физическому серверу Central Node

Аппаратные требования к физическому серверу Central Node зависят от следующих условий:

- объем обрабатываемого трафика;

  Поступление расшифрованного SSL/TLS-трафика в Kaspersky Anti Targeted Attack Platform увеличивает нагрузку по его обработке в 5 раз по сравнению с нерасшифрованным трафиком (стандартным трафиком, поступающим со SPAN-портов). В этом случае объем обрабатываемого трафика для расчета нагрузки на сервер определяется по следующей формуле:

  ```
  <объем расшифрованного трафика> = 5 * <объем нерасшифрованного трафика>
  ```

  Объем трафика, обрабатываемого на ICAP-сервере, рассчитывается согласно таблице, приведенной в разделе Расчеты для Central Node при использовании функциональности ICAP.

- количество обрабатываемых сообщений электронной почты в секунду;

- количество хостов с компонентом Endpoint Agent.

  Компонент Endpoint Agent может быть установлен на рабочую станцию, терминальный сервер, файловый сервер или в сетевое хранилище (NAS).

Совместимость версий приложений, которыми представлен компонент Endpoint Agent, с версиями Kaspersky Anti Targeted Attack Platform см. в следующих разделах справки: Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac.

Эффективное количество хостов с компонентом Endpoint Agent для расчета нагрузки на сервер определяется по следующей формуле:

```
K = A+2*B+3*C+20*D
```

где

- "K" – эффективное количество хостов с компонентом Endpoint Agent.
- "A" – количество рабочих станций и пользователей терминальных серверов под управлением операционной системы Windows с установленным компонентом Endpoint Agent.
- "B" – количество рабочих станций и пользователей терминальных серверов под управлением операционной системы Linux с установленным компонентом Endpoint Agent.
- "C" – количество рабочих станций и пользователей терминальных серверов под управлением операционной системы macOS с установленным компонентом Endpoint Agent.
- "D" – количество серверов.

При объеме обрабатываемого трафика более 1 Гбит/с необходимо устанавливать компоненты Central Node и Sensor на отдельных серверах.

Аппаратные требования к физическим серверам Central Node приведены в таблицах ниже.

Далее в разделе в столбце *Максимальное количество Endpoint Agents* приводятся значения для компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Windows. Эквивалентное количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционных систем Linux, macOS, а также установленных на серверах, рассчитывается по следующим формулам:

- B = <максимальное количество Endpoint Agents>/2, где "B" – количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Linux;
- C = <максимальное количество Endpoint Agents>/3, где "C" – количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы macOS;
- D = <максимальное количество Endpoint Agents>/20, где "D" – количество компонентов Endpoint Agent, установленных на серверах.

Аппаратные требования к физическому серверу Central Node при подключении до 1000 компонентов Endpoint Agent NDR

Максимальное количество Endpoint Agents	Максимальное количество сообщений электронной почты в секунду	Максимальный объем SPAN-трафика на встроенном Sensor (Мбит/с)	Максимальный объем SPAN-трафика на отдельном Sensor (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая г (RAID 1 или R		
						ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	ди м
1000	1	200	Не обрабатывается	160	36	100	1000	
2000	2	500	Не обрабатывается	160	48	100	1000	

Максимальное количество Endpoint Agents	Максимальное количество сообщений электронной почты в секунду	Максимальный объем SPAN-трафика на встроенном Sensor (Мбит/с)	Максимальный объем SPAN-трафика на отдельном Sensor (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая г (RAID 1 или RA		
						ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	ди м
5000	1	1000	Не обрабатывается	224	72	100	1000	
10 000	2	1000	Не обрабатывается	256	80	100	1000	
5000	5	Не обрабатывается	2000	192	72	100	1000	
10 000	20	Не обрабатывается	4000	256	104	100	1000	
15 000	20	Не обрабатывается	4000	320	120	100	1000	
15 000	20	Не обрабатывается	7000	352	160	100	1000	
15 000	20	Не обрабатывается	10 000	384	192	100	1000	

Аппаратные требования к физическому серверу Central Node при подключении до 2000 компонентов Endpoint Agent NDR

Максимальное количество Endpoint Agents	Максимальное количество сообщений электронной почты в секунду	Максимальный объем SPAN-трафика на встроенном Sensor (Мбит/с)	Максимальный объем SPAN-трафика на отдельном Sensor (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая г (RAID 1 или RA		
						ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	ди м
1000	1	200	Не обрабатывается	160	40	100	1000	
2000	2	500	Не обрабатывается	160	52	100	1000	
5000	1	1000	Не обрабатывается	224	72	100	1000	
10 000	2	1000	Не обрабатывается	288	88	100	1000	
5000	5	Не обрабатывается	2000	192	72	100	1000	
10 000	20	Не обрабатывается	4000	256	112	100	1000	
15 000	20	Не обрабатывается	4000	320	128	100	1000	
15 000	20	Не обрабатывается	7000	352	160	100	1000	
15 000	20	Не обрабатывается	10 000	384	192	100	1000	

Kaspersky Anti Targeted Attack Platform не поддерживает работу с программным RAID-массивом.

Аппаратные требования к виртуальному серверу Central Node

Приведенные ниже значения актуальны при подключении к Central Node до 10 000 компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Windows.

При установке компонента на виртуальной платформе VMware ESXi вам нужно увеличить минимальное количество логических ядер, приведенное в таблицах с аппаратными требованиями к физическому серверу Central Node, на 10%.

Остальные требования к аппаратному обеспечению для виртуальных серверов аналогичны требованиям для физических серверов.

Программные требования к виртуальному серверу Central Node

В параметрах виртуального диска должен быть выбран тип диска Thick Provision Eager Zeroed.

Чтобы избежать возможного снижения производительности при развертывании приложения на виртуальной платформе, требуется выполнить следующие действия:

- Установить параметры High Latency Sensitivity.

  Если ваш гипервизор не поддерживает High Latency Sensitivity, вы можете использовать другие механизмы приоритизации виртуальных машин, например, функцию CPU Affinity и резервирование ресурсов.

- Зарезервировать всю оперативную память.

- Зарезервировать всю частоту процессора.

Требования к объему второй дисковой подсистемы на сервере Central Node

Общий минимальный эффективный объем второй дисковой подсистемы определяется по следующей формуле:

E = 1,5 * (P+T+S+N)

где

- "E" – общий минимальный эффективный объем второй дисковой подсистемы.

- "P" – объем постоянного хранилища, который определяется по следующей формуле:

  30 МБ * <эффективное количество хостов с компонентом Endpoint Agent> * <срок хранения в днях>.

  Объем постоянного хранилища не должен превышать 20 ТБ.

- "T" – объем временного хранилища, который вычисляется по следующей формуле:

  27 МБ * <эффективное количество хостов с компонентом Endpoint Agent>.

- "S" – объем для системных файлов, который составляет 150 ГБ.

- "N" – объем хранилища NDR, который вычисляется по следующей формуле:

  (<количество компонентов Endpoint Agent, подключенных к функциональному блоку NDR> * 0.02 ГБ + <объем трафика со SPAN-портов (Гб/с)> * 10 ГБ) * <срок, за который требуется хранить данные NDR, в днях, = 7>.

Дополнительные требования к оперативной памяти в зависимости от объема постоянного хранилища:

- При объеме хранилища 10-15 ТБ добавьте 16 ГБ к минимальному объему оперативной памяти, приведенному в таблицах выше.

- При объеме хранилища 15-20 ТБ добавьте 32 ГБ к минимальному объему оперативной памяти, приведенному в таблицах выше.

Эта формула может быть использована для примерной оценки требуемого дискового пространства. Реальный объем хранимых данных зависит от профиля трафика организации и может отличаться от полученного результата вычислений.

Требования к каналам связи

Необходимо обеспечить пропускную способность канала связи между сервером Central Node и каждым сегментом сети в зависимости от количества хостов Endpoint Agent в сегменте. Пропускная способность в зависимости от количества хостов Endpoint Agent приведена в таблице ниже.

Пропускная способность канала связи в зависимости от количества хостов Endpoint Agent

Максимальное количество Endpoint Agents	Требуемая пропускная способность канала связи, зарезервированная для Endpoint Agents (Мбит/с)
10	1
50	2
100	3
1000	20
10 000	200

Дополнительные требования к серверам Central Node

Дополнительные аппаратные требования к физическим серверам Central Node приведены в разделах Расчеты для компонента Central Node при наличии интегрированных внешних систем, Расчеты для компонента Central Node при использовании функциональности ICAP, Расчеты для компонента Central Node в режиме распределенного решения и мультитенантности, Расчеты для компонента Central Node, развернутого в виде кластера.

Расчеты для компонента Central Node при наличии интегрированных внешних систем

Если вы настроили интеграцию для проверки объектов внешней системы с помощью REST API, вам необходимо увеличить аппаратные характеристики физического сервера Central Node, приведенные в разделах Расчеты для Central Node при использовании функциональности KATA, KEDR, KATA и KEDR, KATA и NDR, KATA, KEDR и NDR. Дополнительные аппаратные требования приведены в таблице ниже.

Дополнительные аппаратные требования к физическому серверу Central Node при наличии интегрированных внешних систем

Максимальное количество обрабатываемых объектов в секунду	Количество дополнительных логических ядер	Количество дополнительных серверов Sandbox
8	2	1
16	4	2
24	7	3

Если вы настроили интеграцию для отправки событий во внешнюю систему с помощью REST API, вам необходимо увеличить аппаратные характеристики сервера Central Node на 1 логическое ядро и 6 ГБ оперативной памяти.

Расчеты для компонента Central Node при интеграции с Kaspersky Secure Mail Gateway

В таблице ниже приводятся аппаратные требования к физическому серверу Central Node при использовании функциональности KATA и интеграции с Kaspersky Secure Mail Gateway версии 2.1.1.

Аппаратные требования к физическому серверу Central Node при использовании функциональности KATA и интеграции с Kaspersky Secure Mail Gateway 2.1.1

Максимальное количество сообщений электронной почты в секунду	Максимальный объем трафика со SPAN-портов (Мбит/с)	Диск			
		Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Частота логических ядер	WOPS (запись, операций в секунду)
1	10 000	36	4	1.15	200
2	10 000	36	4	1.15	200
5	10 000	36	6	1.15	200
10	10 000	36	10	1.15	200
20	10 000	36	12	1.5	200
30	10 000	36	16	2.7	200
50	10 000	36	20	2.7	200
100	10 000	36	40	2.7	200

Расчеты для компонента Central Node при использовании функциональности ICAP

Величина **AV_rps** в таблице ниже означает количество отправляемых на антивирусную проверку файлов в секунду.

В среднем на 1 Мбит/с трафика создается два задания на антивирусную проверку в секунду. Общее количество запросов ICAP не должно превышать 5000 в секунду.

Конфигурации физических серверов Central Node

Lite: до 65 AV_rps, 75 Мбит/с	
Минимальное количество логических ядер	16
Минимальный объем оперативной памяти	64 ГБ
Первая дисковая подсистема (RAID 10)	4 диска по 1200 ГБ
Medium: до 250 AV_rps, 0,3 Гбит/с	
Минимальное количество логических ядер	32
Минимальный объем оперативной памяти	80 ГБ
Первая дисковая подсистема (RAID 10)	4 диска по 1200 ГБ
High: до 750 AV_rps, 1 Гбит/с	
Минимальное количество логических ядер	72
Минимальный объем оперативной памяти	96 ГБ
Первая дисковая подсистема (RAID 10)	4 диска по 1200 ГБ

Расчеты для компонента Central Node в режиме распределенного решения и мультитенантности

Вы можете подключить к одному PCN до 150 SCN.

Если вы хотите подключить к одному PCN до 10 SCN, минимальный объем оперативной памяти и минимальное количество логических ядер на сервере PCN должны быть на 20% выше, чем на сервере с Central Node вне распределенного решения. Нагрузка на SCN может быть любая в пределах, приведенных в аппаратных требованиях к серверу с Central Node.

При подключении к одному PCN от 11 до 150 SCN должны выполняться следующие условия:

- К одному серверу SCN подключено не более 5000 компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Windows.

Для компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционных систем Linux, macOS, а также установленных на серверах, максимальное количество подключений к одному SCN рассчитывается по следующим формулам:

- B = 5000/2, где "B" – количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Linux;
- C = 5000/3, где "C" – количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы macOS;
- D = 5000/20, где "D" – количество компонентов Endpoint Agent, установленных на серверах.

- Аппаратная конфигурация сервера PCN отвечает следующим требованиям:
  - <Минимальное количество логических ядер, приведенное в аппаратных требованиях к серверу Central Node> + 10.
  - <Минимальный объем оперативной памяти, приведенный в аппаратных требованиях к серверу Central Node> + 32.
  - <Значение ROPS, приведенное в аппаратных требованиях к серверу Central Node> + 1500.
  - <Значение WOPS, приведенное в аппаратных требованиях к серверу Central Node> + 3000.

Если вы хотите использовать PCN только для управления SCN и не планируете подключать к нему внешние источники данных (например, Endpoint Agent или внешние системы), физический сервер PCN может иметь следующую конфигурацию:

- Процессор:
  - Частота: 2,5 ГГц.
  - Количество потоков: 20.
  - Количество ядер: 10.
- Оперативная память: 80 ГБ.
- 2 SSD-диска (Write Intensive (WI)).

Расчеты для компонента Central Node приведены в следующих разделах:

- *Расчеты для компонента Central Node при использовании функциональности KATA*.
- *Расчеты для компонента Central Node при использовании функциональности KEDR*.
- *Расчеты для компонента Central Node при использовании функциональности KATA и KEDR*.
- *Расчеты для компонента Central Node при использовании функциональности KATA и NDR*.
- *Расчеты для компонента Central Node при использовании функциональности KATA, KEDR и NDR*.

Минимальные требования к каналу связи между серверами PCN и SCN

Минимальные требования к каналу связи между серверами PCN и SCN в режиме распределенного решения приведены в таблице ниже.

Минимальные требования к каналу связи между серверами PCN и SCN

Максимальное количество хостов Endpoint Agent	Максимальное количество сообщений электронной почты в секунду	Максимальный объем трафика со SPAN-портов (Мбит/с)	Требуемая пропускная способность канала связи (Мбит/с)
5000	5	2000	20
10 000	20	4000	30

Расчеты для компонента Central Node, развернутого в виде кластера

Кластер должен включать минимум 4 сервера: 2 сервера хранения и 2 обрабатывающих сервера. При подключении до 15 000 компонентов Endpoint Agent вам нужно минимум 2 обрабатывающих сервера. При подключении от 15 000 до 30 000 компонентов Endpoint Agent вам требуется не менее 3 обрабатывающих серверов. Количество серверов хранения определяется требуемым объемом дискового пространства для хранения данных.

Каждый сервер кластера должен иметь два сетевых адаптера для настройки кластерной и внешней подсети. Кластерная подсеть должна функционировать со скоростью 10 Гбит/с.

Для кластерной подсети также должны выполняться следующие требования:

- В кластерную подсеть должны входить только серверы кластера и сетевые коммутаторы.
- Кластерная подсеть должна быть изолированной.
- Серверы кластера должны находиться в одном L1- или L2-сегменте. Для этого вы можете подключить все серверы кластера к одному коммутатору или использовать программное туннелирование. Например, L2TPv3 или Overlay Transport Virtualization (OTV).
- Значение сетевой задержки (англ. network latency) должно удовлетворять требованию single digit latency, то есть в миллисекундах значение должно быть менее 10.

Аппаратные требования к физическим серверам кластера при использовании функциональности KEDR приведены в таблице ниже.

Аппаратные требования к обрабатывающим серверам при использовании функциональности KEDR

Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Тип массива RAID	Количество дисков в массиве RAID	Объем одного жесткого диска (ГБ)
256	48	RAID 1	2	1200

Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Первая дисковая подсистема			Вторая дисковая подсистема	
		Тип массива RAID	Количество дисков в массиве RAID	Объем одного жесткого диска (ГБ)	Количество дисков	Объем одного жесткого диска (ГБ)
128	16	RAID 1	2	1200	не менее 6	не менее 1200

Рекомендуется использовать для двух дисковых подсистем диски одинакового объема. Для второй дисковой подсистемы используются диски, не объединенные в RAID-массив.

Требования к скорости дисковых подсистем аналогичны требованиям, приведенным в разделе *Аппаратные требования к серверу Central Node при использовании функциональности KEDR*.

Расчеты для малых конфигураций решения

В этом разделе описываются аппаратные и программные требования к серверам Central Node, к которым подключено от 50 до 750 компонентов Endpoint Agent.

Для развертывания приложения на виртуальной платформе KVM вам необходимо установить гипервизор KVM на базе операционной системы Debian GNU/Linux 12 с использованием эмулятора QEMU version 8.0.2.

Программные требования к виртуальной платформе VMware ESXi приведены в разделе *Аппаратные и программные требования*.

При развертывании Central Node на виртуальных платформах вам нужно учитывать следующие ограничения:

- KVM:
  - Возможна установка только приложения с установочными файлами операционной системы Ubuntu.
  - Возможна установка только неотказоустойчивой версии приложения.
  - Возможно использование только встроенного компонента Sensor.
  - Возможно подключение только компонента Sandbox, развернутого вне платформы виртуализации KVM на физическом сервере или на другой поддерживаемой платформе виртуализации.
  - Для каждого сервера Central Node, развернутого в виртуальной инфраструктуре, необходимо использовать отдельный сетевой интерфейс для получения зеркалированного SPAN-трафика.
  - Невозможно использование API для получения внешними системами информации об алертах и событиях приложения.
  - Не гарантируется поддержка KVM-виртуализаций, используемых в облачных решениях.
  - В настройках виртуальной машины необходимо установить значение **host** для параметра **type** в настройках CPU и значение **VMware vmxnet3** для параметра **model** в настройках сетевой карты.

- VMware ESXi:
  - Возможна установка только неотказоустойчивой версии приложения.
  - Возможно использование только встроенного компонента Sensor.
  - Для каждого сервера Central Node, развернутого в виртуальной инфраструктуре, необходимо использовать отдельный сетевой интерфейс для получения зеркалированного SPAN-трафика.

Аппаратные требования к серверу Central Node в зависимости от используемой функциональности представлены в таблице ниже.

Далее в разделе в столбце *Максимальное количество Endpoint Agents* приводятся значения для компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Windows. Эквивалентное количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционных систем Linux, macOS, а также установленных на серверах, рассчитывается по следующим формулам:

- B = <максимальное количество Endpoint Agents>/2, где "B" – количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Linux;
- C = <максимальное количество Endpoint Agents>/3, где "C" – количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы macOS;
- D = <максимальное количество Endpoint Agents>/20, где "D" – количество компонентов Endpoint Agent, установленных на серверах.

Аппаратные требования к серверу Central Node при использовании функциональности KEDR

Максимальное количество хостов с компонентом Endpoint Agent	Максимальное количество сообщений электронной почты в минуту	Максимальный объем трафика со SPAN-портов на сервере с компонентом Central Node (Мбит/с)	Минимальное количество логических ядер с частотой 3 ГГц	Минимальный объем оперативной памяти (ГБ)
50	0	0	4	31
100	0	0	4	31
150	0	0	6	31*/32
250	0	0	6	31/32
500	0	0	8	31/34
750	0	0	10	31/38

* Значение до косой черты означает объем оперативной памяти, необходимый для установки компонента Central Node. После установки объем оперативной памяти необходимо увеличить до значения, указанного после косой черты.

Аппаратные требования к серверу Central Node при использовании функциональности KATA и KEDR

Максимальное количество хостов с компонентом Endpoint Agent	Максимальное количество сообщений электронной почты в минуту	Максимальный объем трафика со SPAN-портов на сервере с компонентом Central Node (Мбит/с)	Минимальное количество логических ядер с частотой 3 ГГц	Минимальный объем оперативной памяти (ГБ)
100	1	20	6	31*/32
250	5	50	6	31/32
500	30	100	12	31/40
750	30	100	12	31/46

* Значение до косой черты означает объем оперативной памяти, необходимый для установки компонента Central Node. После установки объем оперативной памяти необходимо увеличить до значения, указанного после косой черты.

Расчет объема базы событий и Хранилища для настройки параметров масштабирования приложения

Если вы установили Central Node на сервере (не в виде отказоустойчивого кластера), при настройке параметров масштабирования вам необходимо рассчитать объем на диске для параметров **База событий, ГБ** и **Хранилище, ГБ** по следующей формуле:

```
A = F - R, ГБ.
```

где

- "A" – объем, используемый для базы событий и Хранилища.
- "F" – объем жесткого диска, на котором установлен компонент Central Node.
- "R" – зарезервированное количество свободного пространства (ГБ) на второй дисковой подсистеме, соответствующее количеству подключенных хостов с компонентом Endpoint Agent, приведенное в таблице ниже.

Далее в разделе в столбце *Максимальное количество Endpoint Agents* приводятся значения для компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Windows. Эквивалентное количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционных систем Linux, macOS, а также установленных на серверах, рассчитывается по следующим формулам:

- B = <максимальное количество Endpoint Agents>/2, где "B" – количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы Linux;
- C = <максимальное количество Endpoint Agents>/3, где "C" – количество компонентов Endpoint Agent, установленных на рабочих станциях и терминальных серверах под управлением операционной системы macOS;
- D = <максимальное количество Endpoint Agents>/20, где "D" – количество компонентов Endpoint Agent, установленных на серверах.

Если количество подключенных к Central Node компонентов Endpoint Agent находится в диапазоне между значениями, используйте в расчетах большее число.

Зарезервированное количество свободного пространства в зависимости от количества компонентов Endpoint Agent

Количество хостов с компонентом Endpoint Agent	Зарезервированное количество свободного пространства (ГБ)
1000	1000
3000	1200
5000	1400
10 000	1900
15 000	2400

Расчеты для компонента Sandbox

Аппаратные требования к серверу с компонентом Sandbox зависят от типа и объема обрабатываемого трафика и от допустимого времени проверки объекта.

По умолчанию допустимое время проверки объекта составляет 1 час. Для уменьшения этого времени требуется более мощный сервер или большее количество серверов с компонентом Sandbox.

Рекомендуется рассчитывать конфигурацию компонента Sandbox следующим образом:

1. Установите компоненты Central Node и Sensor на одном сервере и компонент Sandbox на другом сервере для пилотирования приложения.

   Для получения достаточных статистических данных необходимо, чтобы приложение обрабатывало трафик организации в течение недели.

2. Запустите скрипт для записи данных, выполнив команды:

   ```
   sudo kata-run.sh kata-collect --output-dir path-to-folder
   ```

   ```
   --output-dir <путь к директории>
   ```

   Когда скрипт завершит работу, в указанную директорию будет помещен архив *collect.tar.gz*.

3. Передайте этот архив для анализа сотрудникам "Лаборатории Касперского".

   При одновременном запуске нескольких виртуальных машин скорость обработки объектов из очереди увеличивается.

Работа компонента Sandbox не поддерживается на процессорах AMD.

Аппаратные требования к серверу с компонентом Sandbox

Расчет количества серверов с компонентом Sandbox при использовании преднастроенных образов операционных систем приведен в таблице ниже.

Аппаратные требования к компоненту Sandbox при использовании преднастроенных образов операционных систем

Максимальное количество сообщений электронной почты в секунду	Максимальный объем трафика со SPAN-портов (Мбит/с)	Максимальное количество компьютеров с компонентом Endpoint Agent	Количество физических серверов с компонентом Sandbox	
			При использовании всех образов	При использовании только двух образов с ОС Linux
1	200	1000	1	1
2	500	3000	1	1
1	1000	5000	1	1
5	2000	5000	1	1

Максимальное количество сообщений электронной почты в секунду	Максимальный объем трафика со SPAN-портов (Мбит/с)	Максимальное количество компьютеров с компонентом Endpoint Agent	Количество физических серверов с компонентом Sandbox	
			При использовании всех образов	При использовании только двух образов с ОС Linux
20	4000	10 000	2	1
20	7000	15 000	4	2
20	10 000	15 000	5	2

Если вы хотите установить компонент Sandbox на виртуальную машину VMware ESXI, для достижения производительности, аналогичной физическому серверу, вам понадобится в 5 раз больше серверов. При установке компонента Sandbox на виртуальной платформе ПК СВ "Брест", "РЕД Виртуализация" или zVirt Node потребуется в 13 раз больше серверов. Расчетное количество серверов дано с учетом необходимости настроить время проверки объектов.

Если вы используете пользовательские образы для серверов с компонентом Sandbox, могут потребоваться дополнительные мощности. Расчет количества физических серверов с компонентом Sandbox, необходимых при использовании пользовательских образов операционных систем, выполняется по следующей формуле:

```
<количество файлов, которое будет поступать на обработку согласно пользовательским правилам Sandbox, в час> * <количество пользовательских образов операционных систем> / 1000
```

Расчет количества виртуальных машин VMware ESXi с компонентом Sandbox, необходимых при использовании пользовательских образов операционных систем, выполняется по следующей формуле:

```
<количество файлов, которое будет поступать на обработку согласно пользовательским правилам Sandbox, в час> * <количество пользовательских образов операционных систем> / 200
```

При установке компонента Sandbox на виртуальные платформы ПК СВ "Брест" или zVirt Node расчет количества виртуальных машин, необходимых при использовании пользовательских образов операционных систем, выполняется по следующей формуле:

```
<количество физических серверов с компонентом Sandbox> * 5 * 2.6
```

При установке компонента Sandbox на виртуальную платформу "РЕД Виртуализация" расчет количества виртуальных машин, необходимых при использовании пользовательских образов операционных систем, выполняется по следующей формуле:

```
<количество физических серверов с компонентом Sandbox> * 5 * 2.5
```

Количество физических серверов с компонентом Sandbox см. в таблице *Аппаратные требования к компоненту Sandbox при использовании преднастроенных образов операционных систем* выше.

Оценка количества серверов Sandbox приведена для серверов следующей конфигурации:

- При установке компонента Sandbox на физический сервер:
  - 2 процессора Intel® Xeon® 8 Core™ (HT) с частотой 2,6 ГГц или выше.
  - 80 ГБ оперативной памяти.
  - 2 HDD объемом 300 ГБ каждый, объединенные в массив RAID 1.

При установке компонента Sandbox на физический сервер с приведенной выше конфигурацией вам нужно установить ограничение для количества одновременно запускаемых виртуальных машин – 48.

- При установке компонента Sandbox на виртуальную машину:
  - Процессор Intel Xeon 15 Core (HT) с частотой 2,1 ГГц или выше.

    При установке компонента Sandbox на виртуальные платформы ПК СВ "Брест", zVirt Node и "РЕД Виртуализация" рекомендуется использовать процессоры Intel поколения Ice Lake и выше.
  - 32 ГБ оперативной памяти.
  - HDD объемом 300 ГБ.

    На виртуальной машине:

    1. Разрешена вложенная виртуализация.
    2. Установлены параметры High Latency Sensitivity (только при установке на виртуальную машину VMware ESXi).
    3. Зарезервирована вся оперативная память.
    4. Зарезервирована вся частота процессора.

При установке компонента Sandbox на виртуальную машину с приведенной выше конфигурацией вам нужно установить ограничение для количества одновременно запускаемых виртуальных машин – 12.

Если вы планируете использовать пользовательские образы операционных систем, рекомендуется увеличить объем дискового пространства до 600 ГБ и больше.

Установка и первоначальная настройка приложения

В этом разделе содержатся инструкции по установке и первоначальной настройке Kaspersky Anti Targeted Attack Platform.

Для компонентов действует ряд ограничений. Мы рекомендуем ознакомиться с ними перед установкой приложения.

Подготовка к установке компонентов приложения

В этом разделе представлена информация о том, как подготовить IT-инфраструктуру вашей организации к установке компонентов Kaspersky Anti Targeted Attack Platform.

Подготовка IT-инфраструктуры к установке компонентов приложения

В этом разделе приводится описание портов, которые необходимо настроить перед установкой приложения. Для корректной работы компонентов приложения после установки вам нужно настроить правила сетевого экрана.

Перед установкой приложения подготовьте IT-инфраструктуру вашей организации к установке компонентов Kaspersky Anti Targeted Attack Platform:

1. Убедитесь, что серверы, а также компьютер, предназначенный для работы с веб-интерфейсом приложения, и компьютеры, на которых устанавливается компонент Endpoint Agent, удовлетворяют аппаратным и программным требованиям.

2. Для обеспечения безопасности сети от анализируемых объектов запретите доступ в локальную сеть сервера Sandbox управляющему сетевому интерфейсу и интерфейсу для доступа обрабатываемых объектов.

3. Произведите подготовку IT-инфраструктуры организации, согласно таблице ниже:

Порты взаимодействия компонентов Kaspersky Anti Targeted Attack Platform

Источник	Направление	Порт или протокол	Описание
Central Node	Входящее	TCP 22	Подключение к серверу по протоколу SSH
		TCP 443	Получение данных Endpoint Agent (KEDR).
		TCP 8085	Получение данных Endpoint Agent (NDR)
		TCP 8443	Доступ к веб-интерфейсу приложения
		TCP 7423, 8443, 9081, 13520	Связь с сервером Sensor
		UDP 53	
	Исходящее	TCP 80 TCP 443 TCP 1443	Связь с серверами службы KSN и серверами обновлений "Лаборатории Касперского"
		TCP 443	Передача объектов на проверку в Sandbox
		TCP 601	Отправка сообщений в SIEM-систему
		TCP 9443	Связь с сервером Sensor
		UDP 53	
	Входящее и исходящее	ESP	Для взаимодействия Central Node и Sensor по защищенному каналу связи на базе протокола IPSec
Sensor	Входящее	TCP 22	Подключение к серверу по протоколу SSH
		TCP 1344	Получение трафика от прокси-сервера
		TCP 25	Получение SMTP-трафика от почтового сервера
		TCP 443	При использовании Sensor в качестве прокси-сервера для обмена данными между рабочими станциями с Endpoint Agent и Central Node
		TCP 8085	Получение данных Endpoint Agent (NDR)
		TCP 9444	Доступ к веб-интерфейсу компонента. По умолчанию порт закрыт.
		TCP 9443	Связь с сервером Central Node
		UDP 53	
	Исходящее	TCP 80 TCP 443	Связь с серверами службы KSN и серверами обновлений "Лаборатории Касперского"
		TCP 995	Интеграция с почтовым сервером для защищенных соединений
		TCP 110	Интеграция с почтовым сервером для незащищенных соединений
		TCP 7423, 8443, 9081, 13520	Связь с сервером Central Node
		UDP 53	
	Входящее и исходящее	ESP	Для взаимодействия Central Node и Sensor по защищенному каналу связи на базе протокола IPSec

Источник	Направление	Порт или протокол	Описание
Sandbox	Входящее (управляющий интерфейс)	TCP 22	Подключение к серверу по протоколу SSH
		TCP 443	Взаимодействие с Central Node
		TCP 8443	Доступ к веб-интерфейсу приложения
	Исходящее (управляющий интерфейс)	TCP 80 TCP 443	Связь с серверами обновлений "Лаборатории Касперского"
	Исходящее и ответное входящее (интерфейс для доступа обрабатываемых объектов)	Любой	Доступ в сеть Интернет для анализа сетевого поведения исследуемых объектов. Запретите доступ в локальную сеть организации для обеспечения безопасности сети от анализируемых объектов.
SCN (при использовании режима распределенного решения)	Исходящее	TCP 8443, 8444	Для взаимодействия SCN и PCN по защищенному каналу связи на базе протокола IPSec
	Входящее и исходящее	TCP 443, 53, 11000:11006, UDP 53 ESP	
PCN (при использовании режима распределенного решения)	Входящее	TCP 8443, 8444	
	Входящее и исходящее	TCP 443, 53, 11000:11006, UDP 53 ESP	

При установке дополнительного сетевого интерфейса, принимающего только зеркалированный трафик, в виртуальной среде VMware ESXi используйте сетевой адаптер E1000 или отключите опцию LRO (large receive offload) на сетевом адаптере VMXNET3.

Корректная работа соединения между Central Node, Sensor, PCN и SCN возможна только при размещении серверов с установленными компонентами в одной подсети. Использование Network Address Translation (NAT) не поддерживается. Ограничение не распространяется на компоненты Endpoint Agent: они могут располагаться в отдельной от Central Node подсети.

На рисунках ниже показана схема сетевого взаимодействия между компонентами приложения и системами, необходимыми для работы приложения. Стрелки на схеме указывают направление соединения: каждая стрелка проведена от объекта, который инициирует соединение, к объекту, который отвечает на вызов.

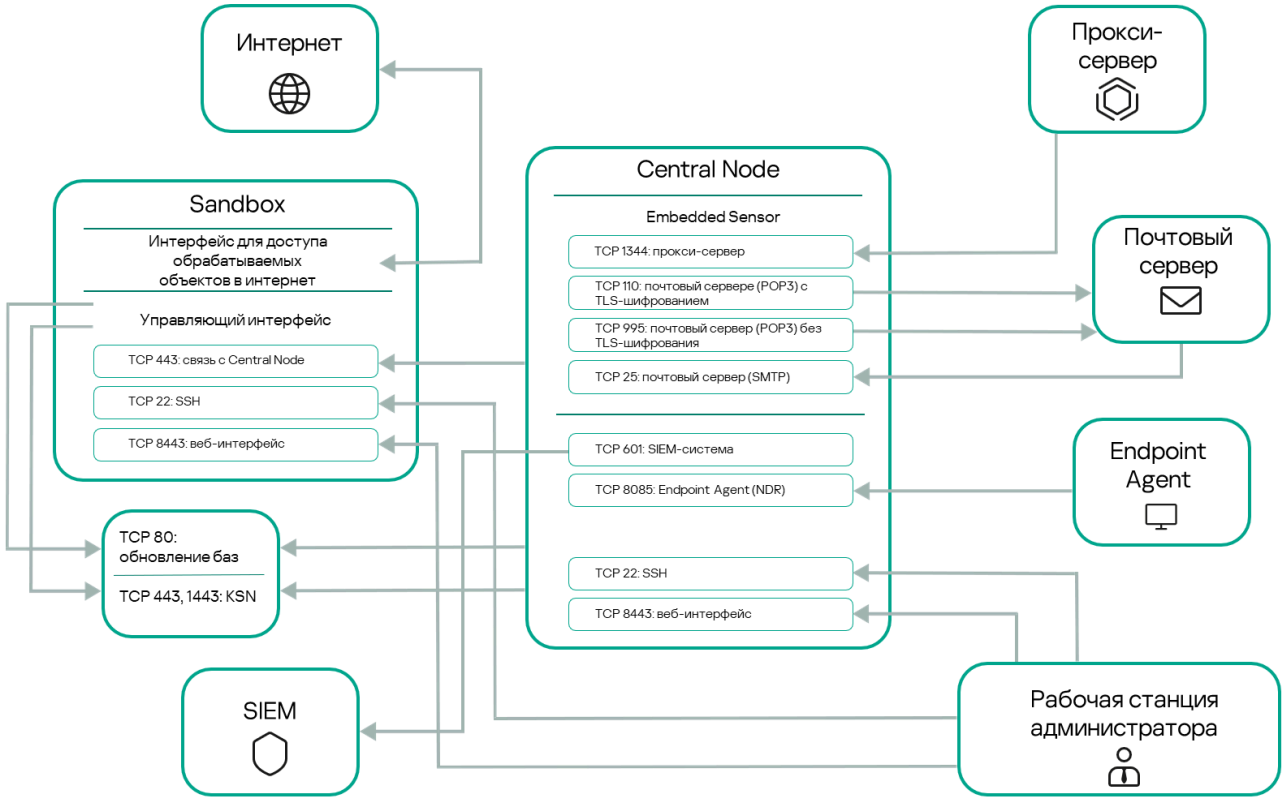


Схема сетевого взаимодействия между компонентами приложения и системами, которые необходимы для работы приложения. Central Node развернут со встроенным Sensor

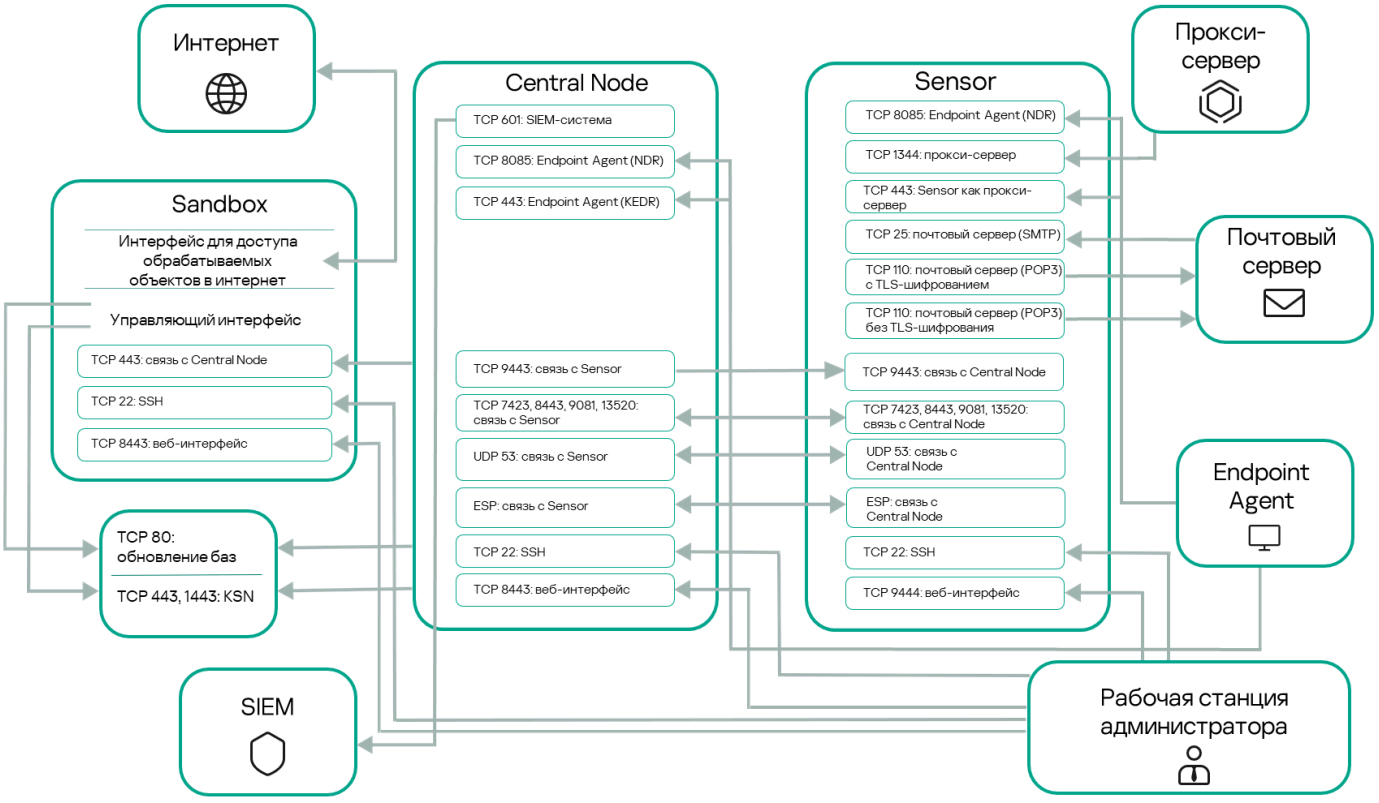


Схема сетевого взаимодействия между компонентами приложения и системами, которые необходимы для работы приложения. Sensor развернут на отдельном от Central Node сервере

Подготовка IT-инфраструктуры к интеграции с почтовым сервером для приема сообщений по протоколу POP3

Если в качестве почтового сервера вы используете почтовый сервер Microsoft Exchange и отправитель настроил запрос уведомления о прочтении сообщения электронной почты, то необходимо отключить отправку уведомлений о прочтении. В противном случае уведомления о прочтении будут отправляться с того адреса электронной почты, который вы настроили в качестве адреса электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform. Также необходимо отключить автоматическую обработку приглашений на встречи для предотвращения заполнения почтового ящика для приема сообщений Kaspersky Anti Targeted Attack Platform.

Чтобы отключить отправку уведомлений о прочтении с адреса электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform:

1. На сервере Microsoft Exchange проверьте, включена ли отправка уведомлений. Для этого выполните команду:

   ```
   Get-MailboxMessageConfiguration -Identity <адрес электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform> | fl
   ```

2. Если отправка уведомлений включена, выполните команду:

   ```
   Set-MailboxMessageConfiguration -Identity <адрес электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform> -ReadReceiptResponse NeverSend
   ```

   Отправка уведомлений о прочтении с адреса электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform будет отключена.

Чтобы отключить автоматическую обработку приглашений на встречи:

1. На сервере Microsoft Exchange проверьте, включена ли отправка уведомлений. Для этого выполните команду:

   ```
   Get-CalendarProcessing -Identity <адрес электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform> | fl
   ```

2. Если автоматическая обработка приглашений на встречи включена, выполните команду:

   ```
   Set-CalendarProcessing -Identity <адрес электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform> -AutomateProcessing:None
   ```

   Автоматическая обработка приглашений на встречи будет отключена.

Подготовка IT-инфраструктуры к интеграции с почтовым сервером для отправки сообщений по протоколу SMTP

Чтобы подготовить IT-инфраструктуру вашей организации к интеграции Kaspersky Anti Targeted Attack Platform с почтовым сервером по протоколу SMTP:

1. На внешнем почтовом сервере настройте правила пересылки копий тех сообщений, которые вы хотите отправлять на проверку Kaspersky Anti Targeted Attack Platform на адреса, указанные в Kaspersky Anti Targeted Attack Platform.

2. Укажите маршрут для пересылки сообщений электронной почты на Sensor.

   Рекомендуется указать статический маршрут – IP-адрес сервера Sensor.

3. На сетевом экране вашей организации разрешите входящие соединения сервера Sensor на порт 25 от почтовых серверов, пересылающих копии сообщений электронной почты.

Вы также можете увеличить безопасность интеграции Kaspersky Anti Targeted Attack Platform с почтовым сервером по протоколу SMTP.

Чтобы увеличить безопасность интеграции Kaspersky Anti Targeted Attack Platform с почтовым сервером по протоколу SMTP:

1. Настройте аутентификацию сервера Kaspersky Anti Targeted Attack Platform на стороне почтовых серверов, передающих сообщения электронной почты для Kaspersky Anti Targeted Attack Platform.

2. Настройте обязательное шифрование трафика на почтовых серверах, передающих сообщения электронной почты для Kaspersky Anti Targeted Attack Platform.

3. Настройте аутентификацию почтовых серверов, передающих сообщения электронной почты для Kaspersky Anti Targeted Attack Platform, на стороне Kaspersky Anti Targeted Attack Platform.

Подготовка виртуальной машины к установке компонента Sandbox

Чтобы подготовить виртуальную машину к установке компонента Sandbox:

1. Запустите гипервизор VMware ESXi.

2. Откройте консоль для управления виртуальными машинами.

3. В контекстном меню виртуальной машины, на которой вы хотите установить компонент Sandbox, выберите пункт **Edit Settings**.

   Откроется окно свойств виртуальной машины.

4. На закладке **Virtual Hardware** раскройте блок параметров **CPU** и установите флажок **Expose hardware-assisted virtualization to guest OS**.

5. На закладке **VM Options** в раскрывающемся списке **Latency Sensitivity** выберите **High**.

6. Нажмите на кнопку **OK**.

Виртуальная машина будет готова к установке компонента Sandbox.

Подготовка установочного образа диска с компонентами Central Node, Sensor и Sandbox

Перед установкой приложения вам необходимо подготовить установочный iso-образ диска с компонентами Central Node, Sensor и Sandbox на базе операционной системы Astra Linux.

Минимальные аппаратные требования к устройству, на котором будет происходить создание iso-образа:

- Процессор: 4 ядра, частота от 2500 МГц.
- Оперативная память: 8 ГБ.
- Объем свободного места на диске: 100 ГБ.

Требования к программному обеспечению:

- Операционная система на базе актуального ядра Linux.
- Docker версии 20 и выше.
- Наличие iso-образа операционной системы Astra Linux Special Edition версии 1.8.1.16 **без** Debian Installer (в названии образа отсутствует -di). Далее в этом разделе образ упоминается под именем `astra-installation.iso`.

> Kaspersky Anti Targeted Attack Platform не поддерживает работу с другими версиями операционной системы Astra Linux.

Вы можете создать iso-образ компонентов Central Node и Sensor следующих версий:

- 7.1.1.531 (сертифицированная версия).
- 7.1.2.532 (несертифицированная версия).
- 7.1.3.533 (несертифицированная версия).
- 7.1.7.537.1 (несертифицированная версия).

Используйте номер требуемой вам версии вместо переменной <номер версии компонента> при выполнении команд из инструкции, приведенной ниже. Для создания iso-образа одной версии требуется последовательно выполнить все шаги инструкции.

Чтобы смонтировать iso-образ на базе операционной системы Astra Linux компонентов Central Node и Sensor или Sandbox:

1. Загрузите из комплекта поставки следующие файлы:

   a. Дистрибутив Central Node и Sensor с именем kata-cn-distribution-<номер версии компонента>-x86_64_en-ru-zh.tar.gz.

   b. Дистрибутив Sandbox с именем kata-sb-distribution-7.1.0.530-x86_64_en-ru-zh.tar.gz.

   c. Файл для создания iso-образа с именем iso-builder-7.1.7.537-x86_64_en-ru-zh.tar.

2. Создайте файл iso_builder.sh **со следующим содержимым**.

```
#!/bin/bash
usage="Builds the KATA install ISO.
Usage:
$(basename "$0") [-h] source_iso distribution iso_builder_image build target_iso_name
where:
    -h, --help        - show this text and exit
    source_iso        - absolute path to the source OS ISO file
    distribution      - absolute path to the KATA distribution archive
    iso_builder_image - absolute path to the iso_builder docker image
    build             - absolute path to a temporary build directory
    target_iso_name   - absolute path to the resulting ISO file
"
if [ "$#" -eq 0 ] || [ "$1" == "-h" ] || [ "$1" == "--help" ]
then
    echo "$usage"; exit 10;
fi
if [ "$#" -lt 5 ]
then
    echo "Error: not enough arguments. Please, refer the help text."; exit 11;
fi
docker load -i $3
docker run -v $1:$1 -v $2:$2 -v $4:/build kaspersky/kata/deployment/iso_builder:6.0 --
source-iso-uri file://$1 --kata-distribution-uri file://$2 --target-iso-name $5
```

3. Выполните команду:

```
mkdir /var/kata_builder
```

4. Поместите в созданный каталог по пути /var/kata_builder файлы, указанные в шаге 1, и образ `astra-installation.iso`.

5. Выполните команду:

   - Если вы подготавливаете образ диска с Central Node и Sensor:

     ```
     sudo ./iso_builder.sh /var/kata_builder/astra-installation.iso
     /var/kata_builder/kata-cn-distribution-<номер версии компонента>-x86_64_en-ru-
     zh.tar.gz /var/kata_builder/iso-builder-7.1.7.537-x86_64_en-ru-zh.tar
     /var/kata_builder buildCNSensorAstra.iso
     ```

- Если вы подготавливаете образ диска с Sandbox:

  ```
  sudo ./iso_builder.sh /var/kata_builder/astra-installation.iso
  /var/kata_builder/kata-sb-distribution-7.1.0.530-x86_64_en-ru-zh.tar.gz
  /var/kata_builder/iso-builder-7.1.7.537-x86_64_en-ru-zh.tar /var/kata_builder
  buildSandboxAstra.iso
  ```

После выполнения команд установочный образ диска с компонентами Central Node и Sensor с именем buildCNSensorAstra.iso и buildSandboxAstra.iso будут размещены по пути /var/kata_builder.

Если вы используете другие директории для хранения файлов, вы можете выполнить команду:

```
sudo ./iso_builder.sh <путь к дистрибутиву Astra Linux Special Edition 1.8.1.16> <путь к дистрибутиву компонента> <путь к файлу iso-builder-7.1.7.537-x86_64_en-ru-zh.tar> <путь, где будет размещен смонтированный iso-образ без указания присваиваемого имени iso-образа> <имя, присваиваемое iso-образу>
```

Порядок установки и настройки компонентов приложения

Установка и настройка приложения состоит из следующих этапов:

1. **Установка Central Node со встроенным Sensor**

   Вы можете установить компонент Central Node со встроенным компонентом Sensor в одной из следующих конфигураций:

   - Кластер.
   - Сервер.

   При наличии нескольких компонентов Central Node вы можете использовать приложение в режиме распределенного решения.

2. **Установка Sensor на отдельном от Central Node сервере**

   При наличии нескольких компонентов Sensor вы можете установить и настроить компонент Sensor на необходимом количестве серверов.

3. **Установка образа диска с компонентом Sandbox**

4. **Настройка компонентов Central Node и Sensor**

5. **Настройка компонента Sandbox через веб-интерфейс Sandbox**

6. **Установка образов дисков операционных систем Microsoft Windows и приложений для работы компонента Sandbox**

7. **Установка компонента Endpoint Agent на компьютеры, входящие в IT-инфраструктуру организации**

   В качестве компонента Endpoint Agent вы можете использовать следующие приложения: Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac.

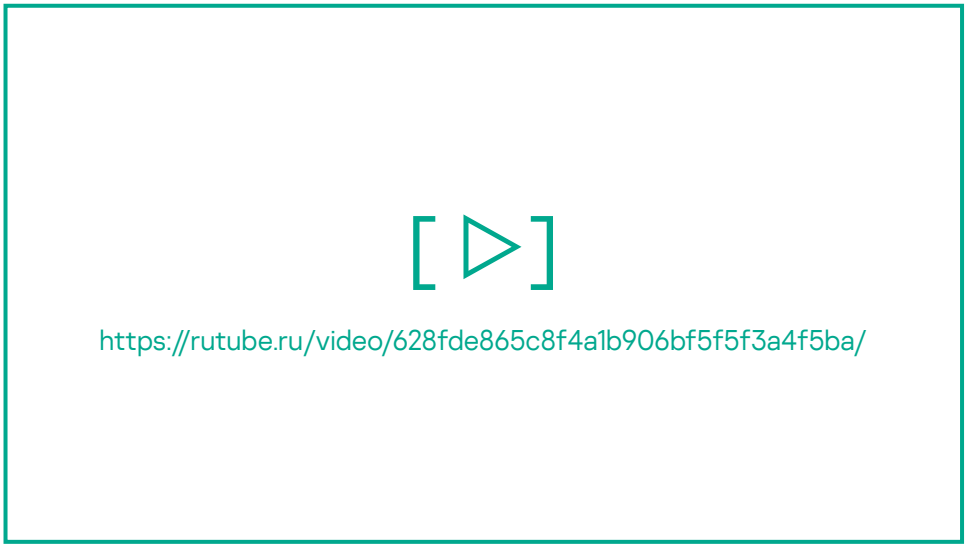
   Совместимость версий приложений, которыми представлен компонент Endpoint Agent, с версиями Kaspersky Anti Targeted Attack Platform см. в следующих разделах справки: Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac.

Подробнее об установке Kaspersky Endpoint Security см. в справке соответствующего приложения:

- Установка Kaspersky Endpoint Security для Windows
- Установка Kaspersky Endpoint Security для Linux
- Установка Kaspersky Endpoint Security для Mac

Если на хостах установлены более ранние версии приложений, вы можете обновить их.

Посмотрите обучающее видео о развертывании EDR на операционной системе Microsoft Windows. Для воспроизведения видео вы можете запустить его на странице справки (см. ниже) или перейти по ссылке https://rutube.ru/video/628fde865c8f4a1b906bf5f5f3a4f5ba/?playlist=891497.



Развертывание EDR на операционной системе Microsoft Windows

Установка компонента Sandbox

Этот раздел представляет собой пошаговую инструкцию по установке компонента Sandbox.

Чтобы приступить к установке компонента Sandbox, выполните следующие действия:

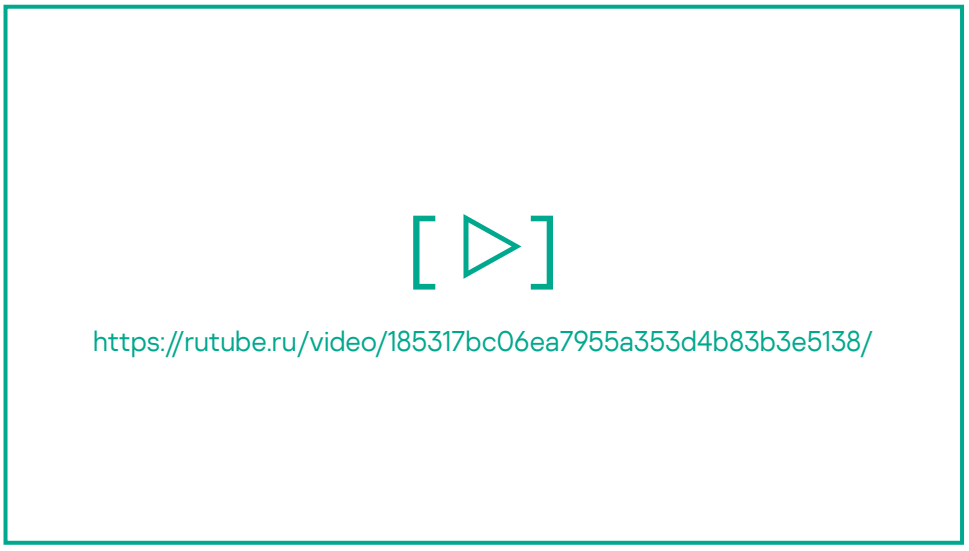
1. Запустите образ диска с компонентом Sandbox.

   Запустится мастер установки.

2. Выберите **Continue** и нажмите на клавишу **ENTER**.

После установки компонента вам нужно настроить его соединение с Central Node.

Посмотрите обучающее видео о развертывании компонента Sandbox. Для воспроизведения видео вы можете запустить его на странице справки (см. ниже) или перейти по ссылке https://rutube.ru/video/185317bc06ea7955a353d4b83b3e5138/?playlist=891497.



Развертывание компонента Sandbox

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

Для продолжения установки вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности АО "Лаборатория Касперского" (далее также "Лицензионное соглашение" и "Политика конфиденциальности") и принять их условия. Если условия Лицензионного соглашения и Политики конфиденциальности не приняты, установка не выполняется.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности АО "Лаборатория Касперского" при установке компонента Sandbox на базе операционной системы Ubuntu Server:

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке и нажмите на клавишу **Enter**.

   Для перемещения вверх и вниз вы можете использовать клавиши **↑**, **↓**, **PageUp** и **PageDown**.

   Откроется окно с текстом Лицензионного соглашения.

2. Ознакомьтесь с Лицензионным соглашением.

3. Если вы принимаете условия Лицензионного соглашения, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Политики конфиденциальности.

4. Ознакомьтесь с Политикой конфиденциальности.

5. Если вы принимаете условия Политики конфиденциальности, выберите **Я принимаю** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности АО "Лаборатория Касперского" при установке компонента Sandbox на базе операционной системы Astra Linux:

1. Выберите язык для просмотра Лицензионного соглашения на использование операционных систем Astra Linux, Лицензионного соглашения и Политики конфиденциальности в списке и нажмите на клавишу **Enter**.

   Для перемещения вверх и вниз вы можете использовать клавиши ↑, ↓, **PageUp** и **PageDown**.

   Откроется окно с текстом Лицензионного соглашения на использование операционных систем Astra Linux.

2. Ознакомьтесь с Лицензионным соглашением на использование операционных систем Astra Linux.

3. Если вы принимаете условия Лицензионного соглашения на использование операционных систем Astra Linux, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Лицензионного соглашения АО "Лаборатория Касперского".

4. Ознакомьтесь с Лицензионным соглашением.

5. Если вы принимаете условия Лицензионного соглашения, выберите кнопку **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Политики конфиденциальности.

6. Ознакомьтесь с Политикой конфиденциальности.

7. Если вы принимаете условия Политики конфиденциальности, выберите кнопку **Я принимаю** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор диска для установки компонента Sandbox

Выберите физический диск для установки компонента Sandbox.

На выбранном диске будут удалены все данные.

Если объем диска менее 150 ГБ, установка завершается ошибкой.

Чтобы выбрать диск для установки компонента:

1. Выберите один из предложенных дисков для установки компонента и нажмите на клавишу **Enter**.

   Отобразится окно подтверждения удаления всех данных с диска и последующей установки компонента на этот диск.

2. Выберите **Install** и нажмите на клавишу **Enter,** чтобы подтвердить удаление всех данных на диске и установку компонента на этот диск.

   Во время установки произойдет перезагрузка устройства.

Мастер установки перейдет к следующему шагу.

Шаг 3. Настройка минимальной длины пароля администратора Sandbox

Чтобы задать минимальную длину пароля администратора компонента Sandbox:

1. В поле **Minimal password length** введите количество символов пароля (не менее 8).

   Рекомендуется использовать пароли длиной 12 и более символов.

2. Выберите **OK** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Создание учетной записи администратора Sandbox

Создайте учетную запись администратора для работы в веб-интерфейсе Sandbox, в меню администратора и в консоли управления сервером с компонентом Sandbox.

Чтобы создать учетную запись администратора Sandbox:

1. В поле **New username** введите имя учетной записи администратора. По умолчанию используется учетная запись admin.

2. В поле **New password** введите пароль учетной записи администратора.

   Пароль должен удовлетворять следующим требованиям:

   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);
     - символ нижнего регистра (a-z);
     - цифру;
     - специальный символ.
   - не должен полностью или в значительной части совпадать с именем пользователя.
   - не должен содержать три и более одинаковых символов подряд.

3. В поле **Confirm password** введите пароль повторно.

4. Выберите **OK** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Настройка управляющего сетевого интерфейса

Для работы компонента Sandbox необходимо подключить минимум две сетевые карты и настроить следующие сетевые интерфейсы:

- Управляющий сетевой интерфейс. Этот интерфейс предназначен для доступа к серверу Sandbox по протоколу SSH, а также через этот интерфейс сервер Sandbox будет принимать объекты от Central Node.
- Сетевой интерфейс для доступа обрабатываемых объектов в интернет. Через этот интерфейс объекты, которые обрабатывает Sandbox, смогут предпринимать попытки действий в интернете, а Sandbox сможет анализировать их поведение. Если вы запретите доступ в интернет, Sandbox не сможет анализировать поведение объектов в интернете, и будет анализировать поведение объектов без доступа в интернет.

  > Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть изолирован от локальной сети вашей организации.

Выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего и настройте его параметры.

Чтобы выбрать управляющий сетевой интерфейс и настроить его параметры:

1. В списке сетевых интерфейсов выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.
2. Нажмите на клавишу **Enter**.
3. В поле **Address** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.
4. В поле **Netmask** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. Выберите **OK** и нажмите на клавишу **Enter**.
6. Выберите **Continue** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Назначение имени хоста и добавление адресов DNS-серверов

Назначьте имя хоста сервера для использования DNS-серверами и добавьте адреса DNS-серверов.

Чтобы назначить имя хоста сервера и добавить адреса DNS-серверов:

1. В окне **DNS settings** выберите пункт **Host name**.
2. В поле **Hostname** введите полное доменное имя сервера.

   Указывайте имя сервера в формате FQDN (например, host.domain.com или host.domain.subdomain.com).

3. Выберите **Ok** и нажмите на клавишу **Enter**.

4. В окне **DNS settings** выберите пункт **DNS servers**.

5. Выберите **New** и нажмите на клавишу **Enter**.

   Откроется окно ввода адреса DNS-сервера.

6. В поле **DNS server** введите IP-адрес основного DNS-сервера в формате IPv4.

7. Выберите **Ok** и нажмите на клавишу **Enter**.

   Окно ввода адреса DNS-сервера закроется.

8. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, повторите шаги 5-7 этой инструкции для каждого сервера, который вы хотите добавить.

9. Когда вы добавите все DNS-серверы, выберите **Go back** и нажмите на клавишу **Enter**.

10. В окне **DNS servers** выберите **Continue** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 7. Настройка статического сетевого маршрута

Чтобы настроить статический сетевой маршрут:

1. В окне **IPv4 Routes** выберите **New** и нажмите на клавишу **Enter**.

   Откроется окно **IPv4 Static Route**.

2. В поле **Address/Mask** введите IP-адрес и маску подсети, для которой вы хотите настроить сетевой маршрут.

   Если вы хотите использовать сетевой маршрут по умолчанию, введите 0.0.0.0/0.

3. В поле **Gateway** введите IP-адрес шлюза.

4. Выберите **Ok** и нажмите на клавишу **Enter**.

5. Если вы хотите добавить другие сетевые маршруты, повторите шаги 1-5 этой инструкции для каждого сетевого маршрута, который вы хотите добавить.

6. Когда вы закончите добавлять сетевые маршруты, нажмите на кнопку **Continue**.

Настройка займет некоторое время. После этого установка завершится.

Развертывание компонента Central Node со встроенным Sensor в виде кластера

Кластер должен включать минимум 4 сервера: 2 сервера хранения и 2 обрабатывающих сервера. Чтобы определить подходящее для вашей организации количество серверов, вы можете воспользоваться Руководством по масштабированию.

Развертывание компонентов Central Node со встроенным Sensor в виде кластера включает следующие этапы:

1. **Развертывание первого сервера хранения**

   Первым требуется развернуть сервер хранения. После того, как он будет развернут, вы можете добавить в кластер дополнительные серверы хранения и обрабатывающие серверы.

2. **Развертывание обрабатывающих серверов** и **дополнительных серверов хранения**

   Вы можете разворачивать серверы в произвольном порядке.

3. **Настройка параметров масштабирования приложения**

   На завершающем этапе развертывания кластера вам нужно настроить параметры масштабирования приложения: указать планируемый объем SPAN-трафика, почтового трафика, количество хостов с компонентом Endpoint Agent, а также размер Хранилища и базы событий.

   Рекомендуется сразу после установки приложения настроить (включить или оставить выключенной) обязательную смену пароля после первой успешной аутентификации.

Если вы развернули кластер на физических серверах и хотите добавить к этим серверам дополнительные жесткие диски или заменить часть существующих дисков, и затем переустановить кластер, вам нужно очистить диски, ранее выделенные под OSD (Object Storage Daemon), на серверах хранения перед установкой компонентов. В противном случае корректная работа приложения не гарантируется. Если вы хотите полностью отключить диски и не планируете больше подключать их к серверу, очистка дисков не требуется.

Развертывание сервера хранения данных

Для развертывания сервера хранения данных вам нужно запустить образ диска с компонентами Central Node и Sensor.

Если при выполнении шагов мастера установки возникла ошибка, обратитесь в Службу технической поддержки.

Объем системного диска и количество и объем дисков для Ceph-хранилища, необходимые для корректной работы компонента, определяются в соответствии с руководством по масштабированию. Минимальный объем системного диска, необходимый только для установки компонента, – 150 ГБ. Минимальное количество дисков для Ceph-хранилища, необходимое только для установки компонента, – 3. Минимальный объем каждого диска должен быть не менее 30 ГБ.

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

Для продолжения установки вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности АО "Лаборатория Касперского" (далее также "Лицензионное соглашение" и "Политика конфиденциальности") и принять их условия. Если условия Лицензионного соглашения и Политики конфиденциальности не приняты, установка не выполняется.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонентов на базе операционной системы Ubuntu:

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке и нажмите на клавишу **Enter**.

   Откроется окно с текстом Лицензионного соглашения.

2. Ознакомьтесь с Лицензионным соглашением.

   Для перемещения вверх и вниз вы можете использовать клавиши ↑, ↓, **PageUp** и **PageDown**.

3. Если вы согласны с Лицензионным соглашением, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Политики конфиденциальности.

4. Ознакомьтесь с Политикой конфиденциальности.

5. Если вы принимаете условия Политики конфиденциальности, выберите **Я принимаю** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонентов на базе операционной системы Astra Linux:

1. Выберите язык для просмотра Лицензионного соглашения на использование операционных систем Astra Linux, Лицензионного соглашения и Политики конфиденциальности в списке и нажмите на клавишу **Enter**.

   Для перемещения вверх и вниз вы можете использовать клавиши ↑, ↓, **PageUp** и **PageDown**.

   Откроется окно с текстом Лицензионного соглашения на использование операционных систем Astra Linux.

2. Ознакомьтесь с Лицензионным соглашением на использование операционных систем Astra Linux.

3. Если вы принимаете условия Лицензионного соглашения на использование операционных систем Astra Linux, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Лицензионного соглашения АО "Лаборатория Касперского".

4. Ознакомьтесь с Лицензионным соглашением.

5. Если вы принимаете условия Лицензионного соглашения, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Политики конфиденциальности.

6. Ознакомьтесь с Политикой конфиденциальности.

7. Если вы принимаете условия Политики конфиденциальности, выберите кнопку **Я принимаю** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор роли сервера

Чтобы выбрать роль сервера:

1. Выберите вариант **storage**.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор режима развертывания

Чтобы выбрать режим развертывания:

1. Выберите один из следующих вариантов:

   - **First node installation**.

     Это значение нужно выбрать при развертывании первого сервера кластера.

   - **Add extra node to the cluster**.

     Это значение нужно выбрать при развертывании сервера, который будет добавлен в существующий кластер.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Выбор диска для установки компонента

На этом шаге вам нужно выбрать диск для установки компонента (системный диск). Объем системного диска, необходимый для корректной работы компонента, определяется в соответствии с руководством по масштабированию. Минимальный объем системного диска, необходимый для установки компонента, – 150 ГБ.

Если объем диска менее 150 ГБ, установка завершается ошибкой.

Чтобы выбрать диск для установки компонента:

1. Выберите один из предложенных дисков для установки компонента и нажмите на клавишу **Enter**.

   Отобразится окно подтверждения.

2. Выберите **Yes** и нажмите на клавишу **Enter.**

Мастер установки перейдет к следующему шагу.

Шаг 5. Выбор маски сети для адресации серверов

Рекомендуется использовать значение по умолчанию.

Маска сети не должна совпадать с используемыми в инфраструктуре организации масками сети.

Чтобы указать маску сети для адресации серверов:

- Если вы хотите использовать предустановленное значение для маски сети, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.18.0.0/16.

- Если вы хотите указать другую маску сети, в поле **Subnet** введите значение, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 6. Выбор маски сети для адресации компонентов приложения

Рекомендуется использовать значение по умолчанию.

Сеть для адресации компонентов приложения не должна пересекаться с сетью для адресации серверов кластера.

Чтобы указать маску сети для адресации основных компонентов приложения:

- Если вы хотите использовать предустановленное значение для маски сети, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.19.0.0/16.

- Если вы хотите указать другую маску сети, в поле **Bridge/overlay subnets** введите значение, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 7. Выбор кластерного сетевого интерфейса

Кластерный сетевой интерфейс используется для взаимодействия между серверами кластера.

Чтобы выбрать кластерный сетевой интерфейс:

1. Выберите строку с сетевым интерфейсом, который используется для внутренней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Выбор внешнего сетевого интерфейса

Внешний сетевой интерфейс используется для доступа к серверу по протоколу SSH, работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и других внешних подключений.

Чтобы выбрать внешний сетевой интерфейс:

1. Выберите строку с сетевым интерфейсом, который используется для внешней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Выбор способа получения IP-адресов для сетевых интерфейсов

Чтобы выбрать способ получения IP-адреса для сетевых интерфейсов:

1. Выберите строку **Configuration type:** и нажмите на клавишу **Enter**.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

2. В открывшемся окне выберите один из следующих вариантов:

   - **dhcp**.
   - **static**.

3. Если вы выбрали **static**, выполните следующие действия:

   a. Выберите строку с параметром и нажмите на клавишу **Enter**.

   b. В открывшемся окне введите требуемые данные.

   Вам нужно указать значение для каждого параметра.

4. Выберите строку **Ok**.

5. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 10. Создание учетной записи администратора и аутентификация сервера в кластере

На этом шаге вам нужно выполнить одно из следующих действий:

- Создать учетную запись администратора, если вы разворачиваете первый сервер кластера.
- Аутентифицировать сервер в кластере, если вы разворачиваете дополнительные серверы хранения.

Создание учетной записи администратора

Создание учетной записи администратора требуется только при развертывании первого сервера кластера. Если вы разворачиваете дополнительный сервер хранения, вместо окна для создания учетной записи администратора приложение предлагает аутентифицировать сервер в кластере.

При развертывании первого сервера кластера вам нужно создать учетную запись администратора. Эта учетная запись используется для работы в веб-интерфейсе приложения, меню администратора приложения и для работы с приложением в режиме Technical Support Mode.

По умолчанию в качестве имени пользователя для учетной записи администратора используется *admin*. Вам требуется задать пароль для этой учетной записи.

Чтобы задать пароль для учетной записи администратора:

1. В открывшемся окне в поле **min length** введите минимальную длину пароля. Вам нужно ввести значение не меньше 8.

2. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

   Откроется окно создания пароля.

3. В открывшемся окне в поле **password** введите пароль учетной записи администратора.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

4. В поле **confirm** введите пароль повторно.

5. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Аутентификация сервера в кластере

Аутентификация сервера в кластере требуется только при развертывании дополнительных серверов хранения. Если вы разворачиваете первый сервер кластера, вместо аутентификации сервера приложение предлагает создать учетную запись администратора.

Для аутентификации сервера в кластере вам нужно ввести пароль для учетной записи admin, заданный при развертывании первого сервера кластера.

Чтобы аутентифицировать сервер в кластере:

1. В поле **password** введите пароль учетной записи администратора.
2. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

   Для выбора кнопки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

Сервер кластера будет аутентифицирован. Мастер установки перейдет к следующему шагу.

Шаг 11. Добавление адресов DNS-серверов

Этот шаг доступен, если вы развертываете первый сервер кластера.

Настройте параметры DNS для работы серверов с компонентами приложения.

Убедитесь, что вы указали корректные IP-адреса DNS серверов. Если указанные IP-адреса некорректны, настройка синхронизации времени с NTP-серверами завершится ошибкой и установка приложения прервется.

Чтобы добавить адреса DNS-серверов:

1. Выберите поле **Add** и нажмите на клавишу **Enter**.
2. Введите IP-адрес DNS-сервера в формате IPv4.
3. Выберите **Ok** и нажмите на клавишу **Enter**.
4. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, повторите шаги 1-3 этой инструкции.

   Когда вы добавите все DNS-серверы, выберите **Continue** нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 12. Настройка синхронизации времени с NTP-сервером

Этот шаг доступен, если вы развертываете первый сервер кластера.

Настройте синхронизацию времени сервера с NTP-сервером.

1. Выберите поле **Add** и нажмите на клавишу **Enter**.
2. Введите IP-адрес или имя NTP-сервера.
3. Выберите **Ok** и нажмите на клавишу **Enter**.
4. Если вы хотите добавить IP-адрес или имя дополнительного NTP-сервера, повторите шаги 1-3 этой инструкции.
5. Когда вы добавите все NTP-серверы, выберите **Continue** нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Чтобы кластер был работоспособным, время на серверах кластера должно быть синхронизировано. Убедитесь, что добавляемый NTP-сервер работает корректно и может обеспечить синхронизацию времени между серверами кластера.

Шаг 13. Выбор дисков для Ceph-хранилища

Выберите диски для Ceph-хранилища. Количество и объем дисков, необходимые для Ceph-хранилища, определяются в соответствии с руководством по масштабированию. Минимальное количество дисков, необходимое только для установки компонента, – 3. Минимальный объем каждого диска в этом случае должен быть не менее 30 ГБ.

Чтобы выбрать диски для Ceph-хранилища:

1. Выберите строку с требуемым диском.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.
2. Нажмите на клавишу **Enter**.
3. Повторите шаги 1–2 для выбора следующих дисков, если вы хотите выбрать несколько дисков.
4. Выберите поле **Apply and finish** и нажмите на клавишу **Enter**.

   Отобразится окно подтверждения.
5. Выберите **Yes** и нажмите на клавишу **Enter**.

Настройка займет некоторое время. После этого установка завершится. Вы можете перейти к настройке конфигурации серверов кластера.

Развертывание обрабатывающего сервера

Для развертывания обрабатывающего сервера вам нужно запустить образ диска с компонентами Central Node и Sensor.

Если при выполнении шагов мастера установки возникла ошибка, обратитесь в Службу технической поддержки.

Объем системного диска, необходимый для корректной работы компонента, определяется в соответствии с руководством по масштабированию. Минимальный объем системного диска, необходимый только для установки компонента, – 150 ГБ.

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

Для продолжения установки вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности АО "Лаборатория Касперского" (далее также "Лицензионное соглашение" и "Политика конфиденциальности") и принять их условия. Если условия Лицензионного соглашения и Политики конфиденциальности не приняты, установка не выполняется.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонентов на базе операционной системы Ubuntu:

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке и нажмите на клавишу **Enter**.

   Откроется окно с текстом Лицензионного соглашения.

2. Ознакомьтесь с Лицензионным соглашением.

   Для перемещения вверх и вниз вы можете использовать клавиши ↑, ↓, **PageUp** и **PageDown**.

3. Если вы согласны с Лицензионным соглашением, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Политики конфиденциальности.

4. Ознакомьтесь с Политикой конфиденциальности.

5. Если вы принимаете условия Политики конфиденциальности, выберите **Я принимаю** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонентов на базе операционной системы Astra Linux:

1. Выберите язык для просмотра Лицензионного соглашения на использование операционных систем Astra Linux, Лицензионного соглашения и Политики конфиденциальности в списке и нажмите на клавишу **Enter**.

   Для перемещения вверх и вниз вы можете использовать клавиши ↑, ↓, **PageUp** и **PageDown**.

   Откроется окно с текстом Лицензионного соглашения на использование операционных систем Astra Linux.

2. Ознакомьтесь с Лицензионным соглашением на использование операционных систем Astra Linux.

3. Если вы принимаете условия Лицензионного соглашения на использование операционных систем Astra Linux, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Лицензионного соглашения АО "Лаборатория Касперского".

4. Ознакомьтесь с Лицензионным соглашением.

5. Если вы принимаете условия Лицензионного соглашения, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Политики конфиденциальности.

6. Ознакомьтесь с Политикой конфиденциальности.

7. Если вы принимаете условия Политики конфиденциальности, выберите кнопку **Я принимаю** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор роли сервера

Чтобы выбрать роль сервера:

1. Выберите **processing**.

   Эта роль включает также установку и настройку компонента Sensor.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонента

На этом шаге вам нужно выбрать диск для установки компонента (системный диск). Объем системного диска, необходимый для корректной работы компонента, определяется в соответствии с руководством по масштабированию. Минимальный объем системного диска, необходимый для установки компонента, – 150 ГБ.

Если объем диска менее 150 ГБ, установка завершается ошибкой.

Чтобы выбрать диск для установки компонента:

1. Выберите один из предложенных дисков для установки компонента и нажмите на клавишу **Enter**.

   Отобразится окно подтверждения.

2. Выберите **Yes** и нажмите на клавишу **Enter.**

Мастер установки перейдет к следующему шагу.

Шаг 4. Выбор маски сети для адресации серверов кластера

Рекомендуется использовать значение по умолчанию.

Маска сети не должна совпадать с используемыми в инфраструктуре организации масками сети.

Чтобы указать маску сети для адресации серверов кластера:

- Если вы хотите использовать предустановленное значение для маски сети, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.18.0.0/16.

- Если вы хотите указать другую маску сети, в поле **Subnet** введите значение, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 5. Выбор маски сети для адресации компонентов приложения

Рекомендуется использовать значение по умолчанию.

Сеть для адресации компонентов приложения не должна пересекаться с сетью для адресации серверов кластера.

Чтобы указать маску сети для адресации основных компонентов приложения:

- Если вы хотите использовать предустановленное значение для маски сети, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.19.0.0/16.

- Если вы хотите указать другую маску сети, в поле **Bridge/overlay subnets** введите значение, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 6. Выбор кластерного сетевого интерфейса

Кластерный сетевой интерфейс используется для взаимодействия между серверами кластера.

Чтобы выбрать кластерный сетевой интерфейс:

1. Выберите строку с сетевым интерфейсом, который используется для внутренней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 7. Выбор внешнего сетевого интерфейса

Внешний сетевой интерфейс используется для доступа к серверу по протоколу SSH, работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и других внешних подключений.

Чтобы выбрать внешний сетевой интерфейс:

1. Выберите строку с сетевым интерфейсом, который используется для внешней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Выбор способа получения IP-адресов для сетевых интерфейсов

Чтобы выбрать способ получения IP-адреса для сетевых интерфейсов:

1. Выберите строку **Configuration type:** и нажмите на клавишу **Enter**.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

2. В открывшемся окне выберите один из следующих вариантов:

   - **dhcp**.
   - **static**.

3. Если вы выбрали **static**, выполните следующие действия:

   a. Выберите строку с параметром и нажмите на клавишу **Enter**.

   b. В открывшемся окне введите требуемые данные.

   > Вам нужно указать значение для каждого параметра.

4. Выберите строку **Ok**.

5. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Аутентификация сервера в кластере

Для аутентификации сервера в кластере вам нужно ввести пароль для учетной записи admin, заданный при развертывании первого сервера кластера.

Чтобы аутентифицировать сервер в кластере:

1. В поле **password** введите пароль учетной записи администратора.
2. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

   Для выбора кнопки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

Сервер кластера будет аутентифицирован. Мастер установки перейдет к следующему шагу.

Шаг 10. Выбор языка локализации функциональности NDR и настройка получения зеркалированного трафика со SPAN-портов

Если вы разворачиваете первый обрабатывающий сервер кластера, на этом шаге вам нужно выполнить шаги мастера установки в следующем порядке:

1. Выбрать язык локализации функциональности NDR.
2. Настроить получение зеркалированного трафика со SPAN-портов.

Если вы разворачиваете дополнительный обрабатывающий сервер, шаг выбора языка локализации NDR отсутствует. После аутентификации сервера в кластере мастер установки перейдет к шагу настройки получения зеркалированного трафика со SPAN-портов.

Выбор языка локализации функционала NDR

На выбранном языке будут отображаться области приложения, связанные с функциональностью NDR.

Чтобы выбрать язык локализации функционала NDR,

выберите его в списке и нажмите на клавишу Enter.

Язык локализации функциональности NDR будет выбран. Мастер установки перейдет к шагу настройки получения зеркалированного трафика со SPAN-портов.

Настройка получения зеркалированного трафика со SPAN-портов

Для корректной работы приложения необходимо, чтобы на одном из обрабатывающих серверов кластера было включено получение зеркалированного трафика со SPAN-портов. Если в действительности обработка зеркалированного трафика со SPAN-портов вам не требуется, укажите 0 для SPAN-трафика при настройке масштабирования.

Обработка зеркалированного трафика должна быть включена только на одном обрабатывающем сервере кластера.

Чтобы включить получение зеркалированного трафика со SPAN-портов,

в открывшемся окне выберите **Yes** и нажмите на клавишу **Enter**.

Настройка займет некоторое время. После этого установка завершится. Для корректной работы приложения вам требуется настроить конфигурацию сервера.

Чтобы отказаться от получения зеркалированного трафика со SPAN-портов,

в открывшемся окне выберите **No** и нажмите на клавишу **Enter**.

Настройка займет некоторое время. После этого установка завершится. Для корректной работы приложения вам требуется настроить конфигурацию сервера.

Очистка жестких дисков на серверах хранения

Если вы развернули кластер на серверах и хотите добавить к этим серверам дополнительные жесткие диски или заменить часть существующих дисков, и затем переустановить кластер, вам нужно очистить диски, ранее выделенные под OSD (Object Storage Daemon), на серверах хранения перед установкой кластера. В противном случае корректная работа приложения не гарантируется.

Чтобы очистить диски, выделенные под OSD, на функционирующем сервере хранения:

1. Войдите в консоль управления сервера, на котором необходимо очистить диски, по протоколу SSH или через терминал.
2. Остановите службу запуска OSD с помощью команды `sudo systemctl stop kata-osd-starter.service`.
3. Остановите контейнеры OSD с помощью команды `sudo docker ps --filter name=osd -q | xargs docker stop`.
4. Получите список дисков с OSD с помощью команды `sudo ceph-volume --cluster ceph lvm list | grep devices`.
5. Удалите сигнатуры файловых систем и таблиц разделов с этих дисков с помощью команды `sudo wipefs -af /dev/<название диска>`.

   Команду необходимо выполнить для каждого диска, полученного на шаге 4. Например: `sudo wipefs -af /dev/sda`.

6. Очистите эти диски с помощью команды `sudo ceph-volume lvm zap --destroy /dev/<название диска>`.

   Команду необходимо выполнить для каждого диска, полученного на шаге 4. Например: `sudo ceph-volume lvm zap --destroy /dev/sda`.

Демон OSD будет удален с дисков.

Если сервер не функционирует, вам нужно удалить информацию о группах томов с каждого диска, выделенного под OSD.

Чтобы удалить информацию о группах томов с каждого диска, выделенного под OSD, на нефункционирующем сервере:

1. Запустите сервер с альтернативной операционной системой.

2. Получите идентификаторы групп для каждого диска, выделенного под OSD, с помощью команды `sudo pvs`.

   В результате выполнения команды отобразится таблица, где `PV` – физические тома, `VG` – принадлежность к логической группе, `Fmt` – формат тома, `Size` – размер физического тома.

3. Удалите соответствующие группы томов с помощью команды `sudo vgremove <идентификатор группы томов>`.

Информация о группах томов на дисках, выделенных под OSD, будет удалена.

Установка компонента Central Node со встроенным Sensor на сервере

Установка компонента Central Node со встроенным Sensor на сервер включает следующие этапы:

1. **Установка компонента Central Node со встроенным Sensor**

   Для установки компонента на физическом сервере вам нужно запустить образ диска с компонентами Central Node и Sensor.

   Для установки компонента на виртуальном сервере вам нужно подключить образ диска с компонентами Central Node и Sensor к выбранной виртуальной машине и запустить ее. Установка запускается сразу после включения виртуальной машины. Вы можете управлять процессом установки с помощью консоли виртуальной машины.

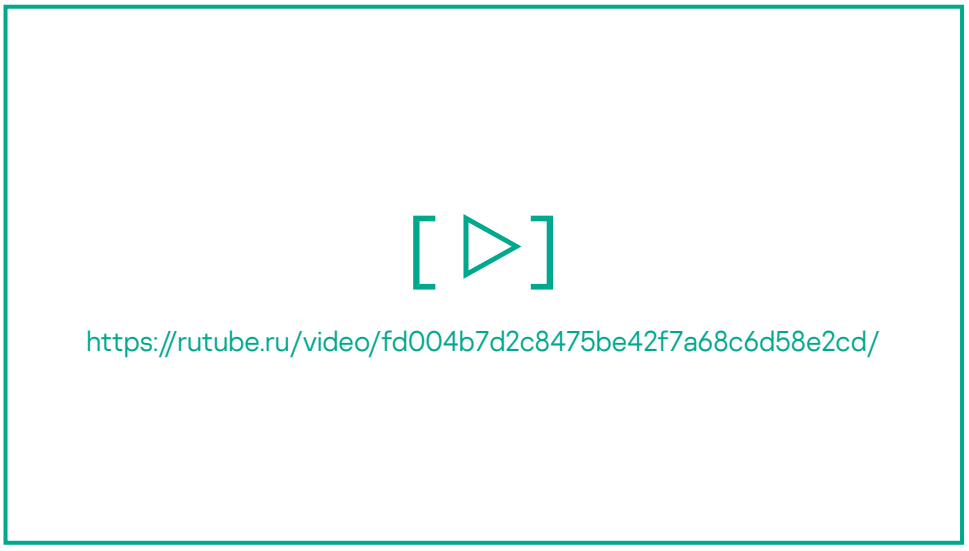
2. **Настройка параметров масштабирования приложения**

   На завершающем этапе развертывания кластера вам нужно настроить параметры масштабирования приложения: указать планируемый объем SPAN-трафика, почтового трафика, количество хостов с компонентом Endpoint Agent, а также размер Хранилища и базы событий.

   Рекомендуется сразу после установки приложения настроить (включить или оставить выключенной) обязательную смену пароля после первой успешной аутентификации.

Если при выполнении шагов мастера установки возникла ошибка, обратитесь в Службу технической поддержки.

Посмотрите обучающее видео о развертывании компонента Central Node. Для воспроизведения видео вы можете запустить его на странице справки (см. ниже) или перейти по ссылке https://rutube.ru/video/fd004b7d2c8475be42f7a68c6d58e2cd/?playlist=891497.



Развертывание компонента Central Node

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

Для продолжения установки вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности АО "Лаборатория Касперского" (далее также "Лицензионное соглашение" и "Политика конфиденциальности") и принять их условия. Если условия Лицензионного соглашения и Политики конфиденциальности не приняты, установка не выполняется.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонентов на базе операционной системы Ubuntu:

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке и нажмите на клавишу **Enter**.

   Откроется окно с текстом Лицензионного соглашения.

2. Ознакомьтесь с Лицензионным соглашением.

   Для перемещения вверх и вниз вы можете использовать клавиши **↑**, **↓**, **PageUp** и **PageDown**.

3. Если вы согласны с Лицензионным соглашением, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Политики конфиденциальности.

4. Ознакомьтесь с Политикой конфиденциальности.

5. Если вы принимаете условия Политики конфиденциальности, выберите **Я принимаю** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонентов на базе операционной системы Astra Linux:

1. Выберите язык для просмотра Лицензионного соглашения на использование операционных систем Astra Linux, Лицензионного соглашения и Политики конфиденциальности в списке и нажмите на клавишу **Enter**.

   Для перемещения вверх и вниз вы можете использовать клавиши ↑, ↓, **PageUp** и **PageDown**.

   Откроется окно с текстом Лицензионного соглашения на использование операционных систем Astra Linux.

2. Ознакомьтесь с Лицензионным соглашением на использование операционных систем Astra Linux.

3. Если вы принимаете условия Лицензионного соглашения на использование операционных систем Astra Linux, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Лицензионного соглашения АО "Лаборатория Касперского".

4. Ознакомьтесь с Лицензионным соглашением.

5. Если вы принимаете условия Лицензионного соглашения, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Политики конфиденциальности.

6. Ознакомьтесь с Политикой конфиденциальности.

7. Если вы принимаете условия Политики конфиденциальности, выберите кнопку **Я принимаю** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор роли сервера

Чтобы выбрать роль сервера:

1. Выберите **single**.

   Эта роль предполагает установку компонентов Central Node и Sensor на одном сервере.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонента

На этом шаге вам нужно выбрать диск для установки компонента (системный диск). Объем системного диска, необходимый для корректной работы компонента, определяется в соответствии с руководством по масштабированию. Минимальный объем системного диска, необходимый для установки компонента, – 150 ГБ.

Если объем диска менее 150 ГБ, установка завершается ошибкой.

Не поддерживается возможность использовать систему хранения данных SAN в качестве диска для установки компонента.

Чтобы выбрать диск для установки компонента:

1. Выберите один из предложенных дисков для установки компонента и нажмите на клавишу **Enter**.

   Отобразится окно подтверждения.

2. Выберите **Yes** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Выделение диска для базы данных компонента Targeted Attack Analyzer

На этом шаге вы можете выделить физический диск для базы данных компонента Targeted Attack Analyzer или отказаться от выделения физического диска. Для оптимальной работы компонента Targeted Attack Analyzer рекомендуется выделить на сервере физический диск объемом не менее 1 ТБ для базы данных компонента.

Выделение физического диска для базы данных компонента Targeted Attack Analyzer возможно только на этом шаге. Возможность выделить диск после установки приложения не предусмотрена.

Чтобы выделить диск для базы данных компонента Targeted Attack Analyzer:

1. Выберите один из предложенных дисков для базы данных компонента Targeted Attack Analyzer.

   Если вам не требуется база данных компонента Targeted Attack Analyzer, выберите строку **Do not allocate a separate disk for TAA.**

2. В окне подтверждения выберите **Yes** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Если вы хотите использовать систему хранения данных SAN, на этом шаге установки выберите SAN, отображаемую как локальный диск, в качестве диска для хранения данных.

Инструкцию по подключению SAN предоставляет ее поставщик.

Шаг 5. Выбор маски сети для адресации серверов

Рекомендуется использовать значение по умолчанию.

Маска сети не должна совпадать с используемыми в инфраструктуре организации масками сети.

Чтобы указать маску сети для адресации серверов:

- Если вы хотите использовать предустановленное значение для маски сети, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.18.0.0/16.

- Если вы хотите указать другую маску сети, в поле **Subnet** введите значение, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 6. Выбор маски сети для адресации компонентов приложения

Рекомендуется использовать значение по умолчанию.

Сеть для адресации компонентов приложения не должна пересекаться с сетью для адресации серверов.

Чтобы указать маску сети для адресации основных компонентов приложения:

- Если вы хотите использовать предустановленное значение для маски сети, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.19.0.0/16.

- Если вы хотите указать другую маску сети, в поле **Bridge/overlay subnets** введите значение, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 7. Выбор внешнего сетевого интерфейса

Внешний сетевой интерфейс используется для доступа к серверу по протоколу SSH, работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и других внешних подключений.

Чтобы выбрать внешний сетевой интерфейс:

1. Выберите строку с сетевым интерфейсом, который используется для внешней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Выбор способа получения IP-адресов для сетевых интерфейсов

Чтобы выбрать способ получения IP-адреса для сетевых интерфейсов:

1. Выберите строку **Configuration type:** и нажмите на клавишу **Enter**.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

2. В открывшемся окне выберите один из следующих вариантов:

   - **dhcp**.
   - **static**.

3. Если вы выбрали **static**, выполните следующие действия:

   a. Выберите строку с параметром и нажмите на клавишу **Enter**.

   b. В открывшемся окне введите требуемые данные.

   > Вам нужно указать значение для каждого параметра.

4. Выберите строку **Ok**.

5. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Создание учетной записи администратора

Учетная запись администратора используется для работы в веб-интерфейсе приложения, меню администратора приложения и для работы с приложением в режиме Technical Support Mode.

По умолчанию в качестве имени пользователя для учетной записи администратора используется *admin*. Вам требуется задать пароль для этой учетной записи.

Чтобы задать пароль для учетной записи администратора:

1. В открывшемся окне в поле **min length** введите минимальную длину пароля. Вам нужно ввести значение не меньше 8.
2. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

   Откроется окно создания пароля.
3. В открывшемся окне в поле **password** введите пароль учетной записи администратора.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.
4. В поле **confirm** введите пароль повторно.
5. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 10. Выбор языка локализации функционала NDR

На выбранном языке будут отображаться области приложения, связанные с функциональностью NDR.

Чтобы выбрать язык локализации функционала NDR,

выберите его в списке и нажмите на клавишу Enter.

Шаг 11. Добавление адресов DNS-серверов

Настройте параметры DNS для работы серверов с компонентами приложения.

Убедитесь, что вы указали корректные IP-адреса DNS серверов. Если указанные IP-адреса некорректны, настройка синхронизации времени с NTP-серверами завершится ошибкой и установка приложения прервется.

Чтобы добавить адреса DNS-серверов:

1. Выберите поле **Add** и нажмите на клавишу **Enter**.
2. Введите IP-адрес DNS-сервера в формате IPv4.

3. Выберите **Ok** и нажмите на клавишу **Enter**.
4. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, повторите шаги 1-3 этой инструкции.
5. Когда вы добавите все DNS-серверы, выберите **Continue** нажмите на клавишу **Enter**.

   Мастер установки перейдет к следующему шагу.

Шаг 12. Настройка синхронизации времени с NTP-сервером

Настройте синхронизацию времени сервера с NTP-сервером.

1. Выберите поле **Add** и нажмите на клавишу **Enter**.
2. Введите IP-адрес или имя NTP-сервера.
3. Выберите **Ok** и нажмите на клавишу **Enter**.
4. Если вы хотите добавить IP-адрес или имя дополнительного NTP-сервера, повторите шаги 1-3 этой инструкции.
5. Когда вы добавите все NTP-серверы, выберите **Continue** нажмите на клавишу **Enter**.

   Установка завершится. Для корректной работы приложения вам требуется настроить конфигурацию сервера.

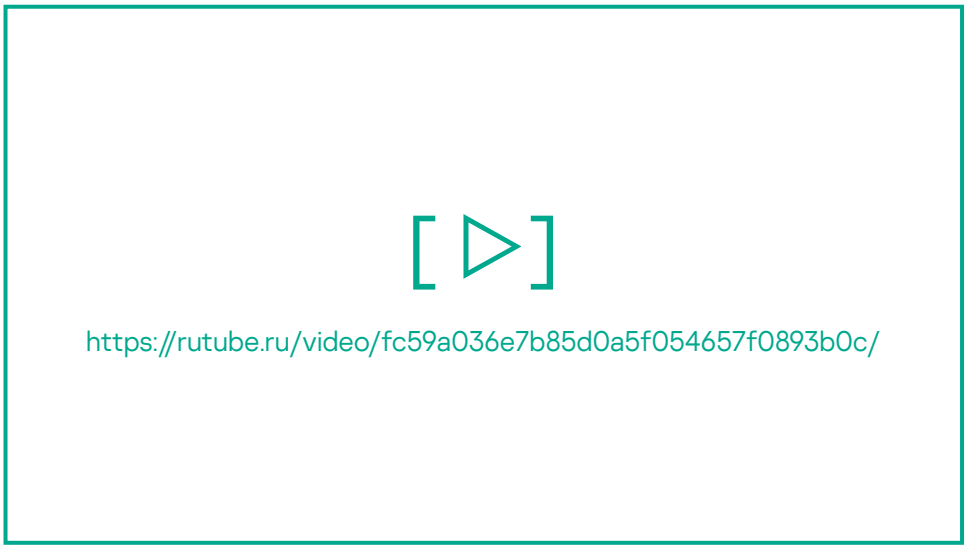
Установка компонента Sensor на отдельном сервере

Для установки компонента Sensor на физическом сервере вам нужно запустить образ диска с компонентами Central Node и Sensor.

Для установки компонента Sensor на виртуальном сервере вам нужно подключить образ диска с компонентами Central Node и Sensor к выбранной виртуальной машине и запустить ее. Установка запускается сразу после включения виртуальной машины. Вы можете управлять процессом установки с помощью консоли виртуальной машины.

После установки компонента вам нужно подключить его к Central Node.

Посмотрите обучающее видео о развертывании компонента Sensor. Для воспроизведения видео вы можете запустить его на странице справки (см. ниже) или перейти по ссылке https://rutube.ru/video/fc59a036e7b85d0a5f054657f0893b0c/?playlist=891497.



Развертывание компонента Sensor

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

Для продолжения установки вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности АО "Лаборатория Касперского" (далее также "Лицензионное соглашение" и "Политика конфиденциальности") и принять их условия. Если условия Лицензионного соглашения и Политики конфиденциальности не приняты, установка не выполняется.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонентов на базе операционной системы Ubuntu:

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке и нажмите на клавишу **Enter**.

   Откроется окно с текстом Лицензионного соглашения.

2. Ознакомьтесь с Лицензионным соглашением.

   Для перемещения вверх и вниз вы можете использовать клавиши **↑**, **↓**, **PageUp** и **PageDown**.

3. Если вы согласны с Лицензионным соглашением, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Политики конфиденциальности.

4. Ознакомьтесь с Политикой конфиденциальности.

5. Если вы принимаете условия Политики конфиденциальности, выберите **Я принимаю** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонентов на базе операционной системы Astra Linux:

1. Выберите язык для просмотра Лицензионного соглашения на использование операционных систем Astra Linux, Лицензионного соглашения и Политики конфиденциальности в списке и нажмите на клавишу **Enter**.

   Для перемещения вверх и вниз вы можете использовать клавиши ↑, ↓, **PageUp** и **PageDown**.

   Откроется окно с текстом Лицензионного соглашения на использование операционных систем Astra Linux.

2. Ознакомьтесь с Лицензионным соглашением на использование операционных систем Astra Linux.

3. Если вы принимаете условия Лицензионного соглашения на использование операционных систем Astra Linux, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Лицензионного соглашения АО "Лаборатория Касперского".

4. Ознакомьтесь с Лицензионным соглашением.

5. Если вы принимаете условия Лицензионного соглашения, выберите **Я принимаю** и нажмите на клавишу **Enter**.

   Откроется окно с текстом Политики конфиденциальности.

6. Ознакомьтесь с Политикой конфиденциальности.

7. Если вы принимаете условия Политики конфиденциальности, выберите кнопку **Я принимаю** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор роли сервера

Чтобы выбрать роль сервера:

1. Выберите **sensor**.

   Эта роль предполагает установку компонента Sensor на отдельном сервере.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонента

На этом шаге вам нужно выбрать диск для установки компонента (системный диск). Объем системного диска, необходимый для корректной работы компонента, определяется в соответствии с руководством по масштабированию. Минимальный объем системного диска, необходимый для установки компонента, – 150 ГБ.

Если объем диска менее 150 ГБ, установка завершается ошибкой.

Чтобы выбрать диск для установки компонента:

1. Выберите один из предложенных дисков для установки компонента и нажмите на клавишу **Enter**.

   Отобразится окно подтверждения.

2. Выберите **Yes** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Выбор маски сети для адресации серверов

Рекомендуется использовать значение по умолчанию.

Маска сети не должна совпадать с используемыми в инфраструктуре организации масками сети.

Чтобы указать маску сети для адресации серверов:

- Если вы хотите использовать предустановленное значение для маски сети, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.18.0.0/16.

- Если вы хотите указать другую маску сети, в поле **Subnet** введите значение, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 5. Выбор маски сети для адресации компонентов приложения

Рекомендуется использовать значение по умолчанию.

Сеть для адресации компонентов приложения не должна пересекаться с сетью для адресации серверов.

Чтобы указать маску сети для адресации основных компонентов приложения:

- Если вы хотите использовать предустановленное значение для маски сети, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.19.0.0/16.

- Если вы хотите указать другую маску сети, в поле **Bridge/overlay subnets** введите значение, выберите кнопку **Ok** и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 6. Выбор внешнего сетевого интерфейса

Внешний сетевой интерфейс используется для доступа к серверу по протоколу SSH, работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и других внешних подключений.

Чтобы выбрать внешний сетевой интерфейс:

1. Выберите строку с сетевым интерфейсом, который используется для внешней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 7. Выбор способа получения IP-адресов для сетевых интерфейсов

Чтобы выбрать способ получения IP-адреса для сетевых интерфейсов:

1. Выберите строку **Configuration type:** и нажмите на клавишу **Enter**.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

2. В открывшемся окне выберите один из следующих вариантов:

   - **dhcp**.
   - **static**.

3. Если вы выбрали **static**, выполните следующие действия:

   a. Выберите строку с параметром и нажмите на клавишу **Enter**.

   b. В открывшемся окне введите требуемые данные.

   > Вам нужно указать значение для каждого параметра.

4. Выберите строку **Ok**.

5. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Создание учетной записи администратора

Учетная запись администратора используется для работы в веб-интерфейсе приложения, меню администратора приложения и для работы с приложением в режиме Technical Support Mode.

По умолчанию в качестве имени пользователя для учетной записи администратора используется *admin*. Вам требуется задать пароль для этой учетной записи.

Чтобы задать пароль для учетной записи администратора:

1. В открывшемся окне в поле **min length** введите минимальную длину пароля. Вам нужно ввести значение не меньше 8.
2. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

   Откроется окно создания пароля.
3. В открывшемся окне в поле **password** введите пароль учетной записи администратора.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.
4. В поле **confirm** введите пароль повторно.
5. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Добавление адресов DNS-серверов

Настройте параметры DNS для работы серверов с компонентами приложения.

Убедитесь, что вы указали корректные IP-адреса DNS серверов. Если указанные IP-адреса некорректны, настройка синхронизации времени с NTP-серверами завершится ошибкой и установка приложения прервется.

Чтобы добавить адреса DNS-серверов:

1. Выберите поле **Add** и нажмите на клавишу **Enter**.
2. Введите IP-адрес DNS-сервера в формате IPv4.
3. Выберите **Ok** и нажмите на клавишу **Enter**.
4. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, повторите шаги 1-3 этой инструкции.
5. Когда вы добавите все DNS-серверы, выберите **Continue** нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 10. Настройка синхронизации времени с NTP-сервером

Настройте синхронизацию времени сервера с NTP-сервером.

1. Выберите поле **Add** и нажмите на клавишу **Enter**.
2. Введите IP-адрес или имя NTP-сервера.
3. Выберите **Ok** и нажмите на клавишу **Enter**.
4. Если вы хотите добавить IP-адрес или имя дополнительного NTP-сервера, повторите шаги 1-3 этой инструкции.
5. Когда вы добавите все NTP-серверы, выберите **Continue** нажмите на клавишу **Enter**.

Установка завершится.

Оптимизация настроек сетевых интерфейсов для компонента Sensor

Следуйте инструкции, если в процессе работы приложения наблюдаются потери сетевых пакетов или проблемы с производительностью при обработке сетевого трафика.

Чтобы уменьшить потери сетевых пакетов и неполного извлечения файлов из трафика:

1. Укажите максимальное количество RSS-очередей:
   - Если скорость передачи данных в вашей сети составляет менее 1 Гбит/с, установите значение 1.
   - Если скорость передачи данных в вашей сети составляет более 1 Гбит/с, установите значение 16.

   Если ваш сетевой интерфейс не позволяет установить значение 16 для параметра максимальное количество RSS-очередей, установите максимально возможное значение параметра.
2. Настройте симметричное RSS-хеширование для сетевого интерфейса. Подробнее о настройке RSS-хеширования см. в документации производителя сетевой карты.
3. Создайте файл interrupts.sh со следующим **содержимым**.

```
#!/usr/bin/env bash

set -e
```

```
dev=$1
min_cpu=$2
max_cpu=$3
step=$4

irs=($(cat /proc/interrupts | grep "$dev" | awk '{split($1,a,":"); print a[1]}'))

cpu=$min_cpu
for ir in ${irs[@]}; do
        echo $cpu > /proc/irq/$ir/smp_affinity_list
        cpu=$(((cpu + step) % max_cpu))
        cat "/proc/irq/$ir/smp_affinity_list"
done
```

4. Выполните команду:

   `sudo bash interrupts.sh <dev> <min_cpu> <max_cpu> <step>`, где

   - `<dev>` – сетевой интерфейс, прерывания которого нужно распределить по ядрам.
   - `<min_cpu>` – ядро, с которого нужно начать распределять прерывания от сетевой карты;
   - `<max_cpu>` – ядро, на котором нужно закончить распределять прерывания от сетевой карты;
   - `<step>` – шаг, с которым будет назначаться ядро для прерывания.

     Пример:

     ```
     sudo bash interrupts.sh ens192 2 11 1
     ```

5. Если вы используете сетевые карты семейства NVIDIA Mellanox (mlx4), настройте количество RSS-очередей и RSS-хеширование, выполнив команды:

   ```
   ethtool -L $dev rx 16
   ethtool -X $dev equal 16
   ethtool -X $dev hfunc xor
   ```

6. Если вы используете сетевые карты семейства Intel (i40e), настройте количество RSS-очередей и RSS-хеширование, выполнив команды:

   ```
   rmmod i40e && modprobe i40e
   ifconfig $dev down
   ethtool -L $dev combined 16
   ethtool -K $dev rxhash on
   ethtool -K $dev ntuple on
   ifconfig $dev up
   ethtool -X $dev hkey
   6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:
   5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A equal 16
   ethtool -A $dev rx off
   ethtool -C $dev adaptive-rx off adaptive-tx off rx-usecs 125
   ethtool -G $dev rx 1024
   ethtool -N $dev rx-flow-hash tcp4 sdfn
   ethtool -N $dev rx-flow-hash tcp6 sdfn
   ```

```
ethtool -N $dev rx-flow-hash udp4 sdfn
ethtool -N $dev rx-flow-hash udp6 sdfn
```

Сетевые интерфейсы будут настроены.

После перезагрузки приложения вам необходимо заново настроить сетевые интерфейсы следуя инструкции.

Подключение и настройка внешнего хранилища для компонента Sensor

Kaspersky Anti Targeted Attack Platform сохраняет трафик, полученный от сетевых интерфейсов, в виде файлов дампа сетевого трафика. Если вы хотите обеспечить долговременное хранение файлов дампа сетевого трафика, вы можете подключить и настроить внешнее хранилище. Файлы дампа сетевого трафика, хранящиеся во внешнем хранилище, можно использовать для выгрузки сетевого трафика в файлы формата PCAP. В качестве внешнего хранилища рекомендуется использовать SSD-диски.

Этапы настройки внешнего хранилища отличаются для компонента Sensor, установленного на одном сервере с Central Node (Embedded Sensor), и на отдельном сервере. Ниже приведены инструкции по настройке внешнего хранилища для указанных конфигураций Sensor.

Если вы подключаете диск повторно и хотите сохранить записанные на него данные, вам нужно пропустить шаги 4 и 9 приведенной ниже инструкции.

Подключение и настройка внешнего хранилища для файлов дампа сетевого трафика на Sensor, установленным вместе с Central Node (Embedded Sensor)

Чтобы подключить и настроить внешнее хранилище для файлов дампа сетевого трафика на Sensor, установленным вместе с Central Node (Embedded Sensor):

1. Подключите диск, который будет использоваться в качестве внешнего хранилища, объемом не менее 100 ГБ.
2. Перейдите в режим Technical Support Mode.
3. Выполните команды:

   ```
   sudo -i
   fdisk -l
   ```

   Убедитесь, что диск, подключенный для использования в качестве внешнего хранилища, отобразился в консоли.
4. Выполните команду:

   ```
   mke2fs -t ext4 -L DATA -m 0 /dev/<имя подключенного диска>
   ```

Пропустите этот шаг, если вы хотите сохранить дампы трафика, записанные на диск ранее.

5. Откройте файл `fstab` в текстовом редакторе:

   ```
   nano /etc/fstab
   ```

6. Добавьте в конец файла запись:

   ```
   /dev/<имя подключенного диска> /data/volumes/dumps/ ext4 defaults 0 0
   ```

7. Закройте текстовый редактор.

8. Перезапустите службу daemon-reload:

   ```
   systemctl daemon-reload
   ```

9. Смонтируйте диск:

   ```
   mount -a
   ```

10. Убедитесь, что диск смонтирован:

    ```
    df -h | grep /data/volumes/dumps
    ```

11. Выполните команду:

    rm -r /data/volumes/dumps/*

Пропустите этот шаг, если вы хотите сохранить дампы трафика, записанные на диск ранее.

12. Выполните команды:

    ```
    chown kluser:klusers /data/volumes/dumps/
    ls -lah /data/volumes/dumps/
    lsblk
    ```

    Убедитесь, что напротив имени подключенного диска в столбце **MOUNTPOINTS** отображается значение **/data/volumes/dumps**.

13. Выполните команды:

    ```
    docker service update kata_product_main_1_preprocessor_span --force
    docker ps | grep preprocessor_span
    ```

    Дождитесь, когда в консоли появится статус **Up <количество секунд > seconds**.

14. Выполните команды:

    ```
    docker exec -it $(docker ps | grep preprocessor_span | awk '{print $1}') bash
    lsblk
    ```

    Убедитесь, что напротив имени подключенного диска в столбце **MOUNTPOINTS** отображается значение **/mnt/kaspersky/nta/dumps**. Это означает, что папка /data/volumes/dumps/ на сервере была смонтирована в Docker-контейнер как /mnt/kaspersky/nta/dumps.

15. Войдите в веб-интерфейс приложения под учетной записью администратора.

16. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

17. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.

    Откроется окно с информацией о компоненте.

18. Нажмите на кнопку **Изменить**.

19. Перейдите на вкладку **Внешнее хранилище** и включите режим использования внешнего хранилища с помощью переключателя **Подключить внешнее хранилище для файлов дампа трафика**.

20. Задайте ограничение занимаемого объема для хранения файлов дампа трафика в блоке параметров **Максимальный объем**.

    Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

21. При необходимости в блоке **Фильтрация с использованием BPF** включите фильтрацию и введите выражение для фильтрации с использованием технологии BPF (Berkeley Packet Filter). Для написания выражения фильтрации BPF используется формат libpcap. Подробнее об описании синтаксиса см. в Руководстве pcap-filter.

22. При необходимости в блоке **Ограничение времени хранения** включите ограничение на минимальное время хранения файлов и укажите нужное количество дней для хранения.

23. Нажмите на кнопку **Сохранить**.

Внешнее хранилище для файлов дампа сетевого трафика на сервере с установленными Sensor и Central Node будет подключено и настроено.

Подключение и настройка внешнего хранилища для файлов дампа сетевого трафика на отдельном сервере с установленным компонентом Sensor

Чтобы подключить и настроить внешнее хранилище для файлов дампа сетевого трафика на отдельном сервере с установленным компонентом Sensor:

1. Подключите диск, который будет использоваться в качестве внешнего хранилища, объемом не менее 100 ГБ.

2. Перейдите в режим Technical Support Mode.

3. Выполните команды:

   ```
   sudo -i
   ```

   ```
   fdisk -l
   ```

   Убедитесь, что диск, подключенный для использования в качестве внешнего хранилища, отобразился в консоли.

4. Выполните команду:

   ```
   mke2fs -t ext4 -L DATA -m 0 /dev/<имя подключенного диска>
   ```

   Пропустите этот шаг, если вы хотите сохранить дампы трафика, записанные на диск ранее.

5. Откройте файл `fstab` в текстовом редакторе:

   ```
   nano /etc/fstab
   ```

6. Добавьте в конец файла запись:

   ```
   /dev/<имя подключенного диска> /data/volumes/dumps/ ext4 defaults 0 0
   ```

7. Закройте текстовый редактор.

8. Перезапустите службу daemon-reload:

   ```
   systemctl daemon-reload
   ```

9. Смонтируйте диск:

   ```
   mount -a
   ```

10. Убедитесь, что диск смонтирован:

    ```
    df -h | grep /data/volumes/dumps
    ```

11. Выполните команду:

    rm -r /data/volumes/dumps/*

    Пропустите этот шаг, если вы хотите сохранить дампы трафика, записанные на диск ранее.

12. Выполните команду:

    ```
    rm -r /data/volumes/dumps/*
    ```

    В результате выполнения команд с подключенного диска будут удалены все данные.

13. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

14. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.

    Откроется окно с информацией о компоненте.

15. Нажмите на кнопку **Изменить**.

16. Перейдите на вкладку **Внешнее хранилище** и включите режим использования внешнего хранилища с помощью переключателя **Подключить внешнее хранилище для файлов дампа трафика**.

17. Задайте ограничение занимаемого объема для хранения файлов дампа трафика в блоке параметров **Максимальный объем**.

    Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

18. При необходимости в блоке **Фильтрация с использованием BPF** включите фильтрацию и введите выражение для фильтрации с использованием технологии BPF (Berkeley Packet Filter). Для написания выражения фильтрации BPF используется формат libpcap. Подробнее об описании синтаксиса см. в Руководстве pcap-filter.

19. При необходимости в блоке **Ограничение времени хранения** включите ограничение на минимальное время хранения файлов и укажите нужное количество дней для хранения.

20. Нажмите на кнопку **Сохранить**.

Внешнее хранилище для файлов дампа сетевого трафика на отдельном сервере с установленным компонентом Sensor будет подключено и настроено.

Настройка параметров масштабирования приложения

Вы можете изменить объем нагрузки на компонент Central Node. Например, подключить к нему дополнительные компоненты Endpoint Agent или Sensor. В этом случае вам нужно указать планируемый объем SPAN-трафика, почтового трафика, количество компонентов Endpoint Agent, а также размер Хранилища и базы событий. Kaspersky Anti Targeted Attack Platform определит оптимальную конфигурацию сервера Central Node с учетом указанных параметров.

Если компонент Central Node развернут в виде кластера, приложение определяет оптимальную конфигурацию всех серверов кластера.

Чтобы кластер был работоспособным после настройки параметров масштабирования, время на серверах кластера должно быть синхронизировано. Перед настройкой параметров масштабирования убедитесь, что для хотя бы одного сервера кластера настроена интеграция с работоспособным NTP-сервером.

Вы можете настроить интеграцию с NTP-сервером в веб-интерфейсе Kaspersky Anti Targeted Attack Platform или меню администратора компонента на любом сервере кластера. Если вы не настраивали ранее интеграцию с NTP-сервером, после ее настройки рекомендуется перезагрузить серверы кластера.

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

При изменении значений параметров **Количество Endpoint Agents**, **Почтовый трафик, сообщений в секунду**, **SPAN-трафик, Мбит/с** или **Хранилище, ГБ** в меньшую сторону возможна потеря объектов из очередей на обработку компонентами приложения.

Чтобы настроить конфигурацию серверов Central Node:

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, в адресной строке браузера введите IP-адрес сервера с компонентом Central Node.

   Если вы используете отказоустойчивую версию приложения, вы можете ввести IP-адрес любого сервера кластера Central Node или **полное доменное имя (FQDN) кластера**.

   Для обеспечения бесперебойного доступа к веб-интерфейсу программы вы можете настроить на сервере DNS функцию Round Robin. В этом случае осуществляется вход в веб-интерфейс первого работоспособного сервера кластера Central Node.

   Откроется окно ввода учетных данных пользователя Kaspersky Anti Targeted Attack Platform.

2. Введите имя admin и пароль, заданный при установке приложения.

3. Нажмите на кнопку **Войти**.

4. Перейдите в раздел **Конфигурация серверов**.

5. В поле **Количество Endpoint Agents** укажите эффективное для вашей инфраструктуры количество хостов с компонентом Endpoint Agent.

Подробнее о том, как рассчитать эффективное количество компонентов Endpoint Agent см. в руководстве по масштабированию.

Если вы не используете лицензионный ключ KEDR, укажите 0.

6. В поле **Почтовый трафик, сообщений в секунду** укажите планируемое количество сообщений электронной почты в секунду.

   Если вы не используете лицензионный ключ KATA или KATA/NDR, укажите 0.

7. В поле **SPAN-трафик, Мбит/с** укажите планируемое количество трафика со SPAN-портов на серверах с компонентом Sensor.

   Если вы не используете лицензионный ключ KATA или KATA/NDR, укажите 0.

8. Если вы установили компонент Central Node на сервере, укажите значения в разделе **Объем диска**, в полях **База событий, ГБ** и **Хранилище, ГБ**.

   Информация для расчета размера базы событий и Хранилища приведена в разделе Расчет объема базы событий и Хранилища для настройки параметров масштабирования приложения.

9. Если вы установили компонент Central Node в виде кластера, в разделе **Доступный объем диска** задайте размер базы событий и Хранилища одним из следующих способов:

   - Переместите ползунок, разделяющий части **База событий** и **Хранилище**, влево или вправо.

     Вам нужно учитывать, что при уменьшении размера базы событий и Хранилища самые старые данные удаляются безвозвратно в соответствии с правилами ротации. При увеличении размера базы событий и Хранилища данные сохраняются.

   - Укажите значения в полях **База событий, ГБ** и **Хранилище, ГБ**.

     Информация для расчета размера базы событий и Хранилища приведена в разделе Расчет объема базы событий и Хранилища для настройки параметров масштабирования приложения.

   - При необходимости вы можете оставить свободное пространство на диске, переместив последний ползунок справа.

   Для базы алертов дисковое пространство резервируется автоматически при установке компонента Central Node.

10. Нажмите на кнопку **Настроить**.

Если компонент Central Node установлен на сервере, Kaspersky Anti Targeted Attack Platform определит оптимальную конфигурацию сервера в соответствии с заданными параметрами. Если компонент Central Node установлен в виде кластера, приложение настроит серверы кластера.

Применение параметров масштабирования и запуск всех необходимых служб требует некоторого времени, поэтому рекомендуется входить в веб-интерфейс и продолжать работу с приложением приблизительно через 20 минут после завершения настройки параметров масштабирования.

Настройка правил сетевого экрана

Для правильной работы приложения и его компонентов вам нужно настроить правила сетевого экрана на сетевом оборудовании, которое связывает компьютеры с установленными компонентами приложения.

Операционные системы компонентов поставляются с уже настроенными правилами сетевого экрана. Мы настоятельно не рекомендуем менять правила iptables.

Порты, используемые на компьютерах с установленными компонентами Kaspersky Anti Targeted Attack Platform

Описанные правила распространяется на все типы узлов вне зависимости от конфигурации. Правила применяются через systemd-сервис kata-firewall, только для цепочек INPUT и DOCKER-USER.

Цепочка INPUT

Цепочка регламентирует все подключения, входящие на компьютеры с установленными компонентами Kaspersky Anti Targeted Attack Platform.

Правила сетевого взаимодействия представлены в таблице ниже.

Правила сетевого взаимодействия для цепочки INPUT

Целевой сервис или протокол	Порт	Протокол	sport	dport	Доступ из внешней сети
SSH	22	TCP	—	✓	✓
SMTP	25	TCP	—	✓	✓
DNS	53	TCP	—	✓	✓
HTTP	80	TCP	—	✓	✓
SNMPD	161	UDP	—	✓	✓
HTTPS	443	TCP	—	✓	✓
preprocessor_icap	1334	TCP	—	✓	✓
docker swarm	2377	TCP	✓	✓	—
etcd	2379	TCP	—	✓	✓
etcd	2380	TCP	—	✓	✓
ceph_mon	3300	TCP	—	✓	✓
VXLAN	4789	TCP/UDP	✓	✓	—
ceph_mon	6789	TCP	—	✓	✓
ceph OSD	6800:6900	TCP	—	✓	✓
docker swarm	7946	TCP/UDP	✓	✓	—

Целевой сервис или протокол	Порт	Протокол	sport	dport	Доступ из внешней сети
ipsec_manager	8084	TCP	✓	✓	—
pcap_manager	8085	TCP	—	✓	✓
HTTPS	8443	TCP/UDP	—	✓	✓
HTTPS	8444	TCP/UDP	—	✓	✓
suricata_metrics_exporter	9103	TCP	✓	✓	—
node_exporter	9141	TCP	✓	✓	—
cadvisor	9142	TCP	✓	✓	—
preprocessor_metrics_exporter	9191	TCP	✓	✓	—
pcap_manager_metrics_exporter	9192	TCP	✓	✓	—
ceph_mgr	9283	TCP	—	✓	✓
ceph_rgw	9284	TCP	—	✓	✓
NDR sensor	9443	TCP	—	✓	✓
kafka bootstrap	11000:11006	TCP	—	✓	✓

Цепочка DOCKER-USER

Цепочка регламентирует подключения к сети для адресации компонентов приложения. Правила сетевого взаимодействия представлены в таблице ниже.

Правила сетевого взаимодействия для цепочки DOCKER-USER

Целевой сервис или протокол	Порт	Протокол	sport	dport
SMTP	25	TCP	—	✓
DNS	53	TCP/UDP	—	✓
HTTP	80	TCP	—	✓
HTTPS	443	TCP	—	✓
preprocessor_icap	1344	UDP	—	✓
NDR NATS (KICKS NAT)	7423	TCP	—	✓
NDR public API	8070	TCP	—	✓
deployment API	8080	TCP	✓	✓
deployment management API	8090	TCP	✓	✓
authorization service	8091	TCP	✓	✓
HTTPS	8443	TCP	—	✓
apt collector ssl	9081	TCP	—	✓
Сенсор	9443	TCP	—	✓
NDR EKA	13520	TCP	—	✓

Порты, используемые сервисами Kaspersky Anti Targeted Attack Platform в кластерной конфигурации

Для правильной работы приложения в кластерной конфигурации необходимо настроить сетевые доступы для исходящих соединений согласно таблице ниже.

Порты для работы сервисов Kaspersky Anti Targeted Attack Platform в кластерной конфигурации

Сервис	Порт	Протокол
agent_database_configurator	2379	TCP
agent_database_configurator	5432	TCP
agent_database_synchronizer	2379	TCP
agent_database_synchronizer	5432	TCP
agent_database_synchronizer	9092	TCP
agent_database_synchronizer	9100	TCP
agent_database_synchronizer	10000:10010	TCP
agent_server	1080	TCP
agent_server	2379	TCP
agent_server	5432	TCP
agent_server	8100	TCP
agent_server	9090	TCP
agent_server	9284	TCP
antiapt_database_configurator	2379	TCP
antiapt_database_configurator	5432	TCP
authorization_service	2379	TCP
authorization_service	4567	TCP
authorization_service	8090	TCP
authorization_service	8443	TCP
authorization_service	8701	TCP
authorization_service	8899	TCP
cadvisor	Любой	Любой
ceph_management_api	2379	TCP
ceph_management_api	3300	TCP
ceph_management_api	6789	TCP
ceph_management_api	8765	TCP
ceph_management_api	8080	TCP
ceph_management_api	9283	TCP
ceph_management_api	9284	TCP
ceph_mgr	2379	TCP
ceph_mgr	3300	TCP
ceph_mgr	6789	TCP

Сервис	Порт	Протокол
ceph_mgr	6800:6900	TCP
ceph_mgr	9141	TCP
ceph_mgr	9142	TCP
ceph_mgr	9283	TCP
ceph_mgr	9284	TCP
ceph_mon	2379	TCP
ceph_mon	3300	TCP
ceph_mon	6789	TCP
ceph_mon	6800:6900	TCP
ceph_mon	9141	TCP
ceph_mon	9142	TCP
ceph_mon	9283	TCP
ceph_mon	9284	TCP
ceph_osd	2379	TCP
ceph_osd	3300	TCP
ceph_osd	6789	TCP
ceph_osd	6800:6900	TCP
ceph_osd	9141	TCP
ceph_osd	9142	TCP
ceph_osd	9283	TCP
ceph_osd	9284	TCP
ceph_rgw	2379	TCP
ceph_rgw	3300	TCP
ceph_rgw	6789	TCP
ceph_rgw	6800:6900	TCP
ceph_rgw	9141	TCP
ceph_rgw	9142	TCP
ceph_rgw	9283	TCP
ceph_rgw	9284	TCP
ceph_rgw_configurator	2379	TCP
ceph_rgw_configurator	3300	TCP
ceph_rgw_configurator	6789	TCP
ceph_rgw_configurator	6800:6900	TCP
ceph_rgw_configurator	9141	TCP
ceph_rgw_configurator	9142	TCP
ceph_rgw_configurator	9283	TCP
ceph_rgw_configurator	9284	TCP
clickhouse	2379	TCP
clickhouse	8123	TCP
clickhouse	9000	TCP
clickhouse_database_configurator	2379	TCP

Сервис	Порт	Протокол
clickhouse_database_configurator	9000	TCP
clickhouse_metrics_importer	2379	TCP
clickhouse_metrics_importer	6379	TCP
clickhouse_metrics_importer	8123	TCP
clickhouse_metrics_importer	9000	TCP
clickhouse_metrics_importer	9090	TCP
coredns	53	TCP
coredns	53	TCP
coredns	2379	TCP
deployment_api	22	TCP
deployment_api	2377	TCP
deployment_api	2379	TCP
deployment_api	4567	TCP
deployment_api	8080	TCP
deployment_api	8443	TCP
deployment_api	8701	TCP
deployment_api	9141	TCP
deployment_api	9284	TCP
deployment_management_api	53	TCP
deployment_management_api	2379	TCP
deployment_management_api	4567	TCP
deployment_management_api	8091	TCP
deployment_management_api	8443	TCP
deployment_management_api	8701	TCP
deployment_management_api	8702	TCP
deployment_management_api	8765	TCP
deployment_management_api	8899	TCP
deployment_management_api	9141	TCP
dhcp_server	Любой	Любой
edr_synchronizer	25	TCP
edr_synchronizer	80	TCP
edr_synchronizer	514	TCP
edr_synchronizer	514	UDP
edr_synchronizer	2379	TCP
edr_synchronizer	5432	TCP
edr_synchronizer	6379	TCP
edr_synchronizer	8081	TCP
edr_synchronizer	8082	TCP
edr_synchronizer	8083	TCP
edr_synchronizer	9092	TCP
edr_synchronizer	10000:10010	TCP

Сервис	Порт	Протокол
edr_synchronizer	33334	TCP
elasticsearch	2379	TCP
elasticsearch	9200	TCP
elasticsearch	9300	TCP
elasticsearch_data	2379	TCP
elasticsearch_data	9200	TCP
elasticsearch_data	9300	TCP
elasticsearch_exporter	2379	TCP
elasticsearch_exporter	9200	TCP
elasticsearch_exporter	9300	TCP
etcd	2379	TCP
etcd	2380	TCP
events_api	80	TCP
events_api	2379	TCP
events_api	5432	TCP
events_api	8080	TCP
events_api	8081	TCP
events_api	9092	TCP
events_api	9100	TCP
events_api	9284	TCP
events_api	10000:10010	TCP
fastsearch	2379	TCP
fastsearch	8080	TCP
fastsearch	8180	TCP
fastsearch_events_cleaner	9200	TCP
fastsearch_events_importer	2379	TCP
fastsearch_events_importer	8081	TCP
fastsearch_events_importer	9092	TCP
fastsearch_events_importer	9100	TCP
fastsearch_events_importer	9200	TCP
fastsearch_events_importer	10000:10010	TCP
hunts_database_configurator	2379	TCP
hunts_database_configurator	5432	TCP
hunts_database_synchronizer	2379	TCP
hunts_database_synchronizer	5432	TCP
hunts_database_synchronizer	9092	TCP
hunts_database_synchronizer	10000:10010	TCP
hunts_event_processor	2379	TCP
hunts_event_processor	5432	TCP
hunts_event_processor	8080	TCP
hunts_event_processor	8081	TCP

Сервис	Порт	Протокол
hunts_event_processor	9092	TCP
hunts_event_processor	9100	TCP
hunts_event_processor	10000:10010	TCP
hunts_statistics_api	2379	TCP
hunts_statistics_api	5432	TCP
hunts_statistics_api	8080	TCP
hunts_statistics_api	8081	TCP
hunts_statistics_api	9092	TCP
hunts_statistics_api	9100	TCP
hunts_statistics_api	10000:10010	TCP
hunts_statistics_processor	2379	TCP
hunts_statistics_processor	5432	TCP
hunts_statistics_processor	8080	TCP
hunts_statistics_processor	8081	TCP
hunts_statistics_processor	9092	TCP
hunts_statistics_processor	9100	TCP
hunts_statistics_processor	9200	TCP
hunts_statistics_processor	10000:10010	TCP
edr_synchronizer	25	TCP
edr_synchronizer	80	TCP
ids_alert_syncer	514	UDP
ids_alert_syncer	2379	TCP
ids_alert_syncer	5432	TCP
ids_alert_syncer	777	TCP
ids_alert_syncer	8083	TCP
ids_alert_syncer	9092	TCP
ids_alert_syncer	9200	TCP
ids_alert_syncer	10000:10010	TCP
ids_alert_syncer	33334	TCP
ioa_update_validator	2379	TCP
ipsec_manager	80	TCP
ipsec_manager	2379	TCP
kafka	2379	TCP
kafka	2181	TCP
kafka	9092	TCP
kafka	9095	TCP
kafka	10000:10010	TCP
kafka_configurator	2181	TCP
kafka_configurator	2379	TCP
kafka_configurator	9092	TCP
kafka_configurator	10000:10010	TCP

Сервис	Порт	Протокол
kafka_exporter	2379	TCP
kafka_exporter	9092	TCP
kafka_exporter	9100	TCP
kafka_exporter	10000:10010	TCP
kafka_proxy	Любой	Любой
kata_scanner	25	TCP
kata_scanner	80	TCP
kata_scanner	514	TCP
kata_scanner	514	UDP
kata_scanner	443	TCP
kata_scanner	2379	TCP
kata_scanner	5432	TCP
kata_scanner	6379	TCP
kata_scanner	7777	TCP
kata_scanner	8081	TCP
kata_scanner	8082	TCP
kata_scanner	8083	TCP
kata_scanner	9081	TCP
kata_scanner	9090	TCP
kata_scanner	9092	TCP
kata_scanner	9100	TCP
kata_scanner	9284	TCP
kata_scanner	10000:10010	TCP
kata_scanner	33334	TCP
ksb_agent_server	80	TCP
ksb_agent_server	2379	TCP
ksb_agent_server	5432	TCP
ksb_agent_server	8082	TCP
ksb_agent_server	8083	TCP
ksb_agent_server	9898	TCP
ksn_proxy	80	TCP
ksn_proxy	443	TCP
ksn_proxy	514	TCP
ksn_proxy	514	UDP
ksn_proxy	2379	TCP
ksn_proxy	7777	TCP
ksn_proxy	8083	TCP
ksn_proxy	9092	TCP
ksn_proxy	9102	TCP
ksn_proxy	10000:10010	TCP
ksn_proxy	1:65535	TCP

Сервис	Порт	Протокол
ksqldb_configurator	2379	TCP
ksqldb_configurator	5432	TCP
ksqldb_configurator	8083	TCP
ksqldb_configurator	8088	TCP
ksqldb_configurator	9092	TCP
ksqldb_configurator	10000:10010	TCP
ksqldb_server	2379	TCP
ksqldb_server	5432	TCP
ksqldb_server	9092	TCP
ksqldb_server	11000:11006	TCP
management_ui	2379	TCP
management_ui	8091	TCP
monitoring_grafana	3000	TCP
monitoring_prometheus	2379	TCP
monitoring_prometheus	9090	TCP
monitoring_prometheus	9100	TCP
monitoring_prometheus	9102	TCP
monitoring_prometheus	9141	TCP
monitoring_prometheus	9142	TCP
monitoring_prometheus	9191	TCP
monitoring_prometheus	9192	TCP
monitoring_prometheus	9283	TCP
multitenancy_management_api	2379	TCP
multitenancy_management_api	4567	TCP
multitenancy_management_api	8443	TCP
multitenancy_management_api	8701	TCP
multitenancy_management_api	8090	TCP
multitenancy_management_api	8899	TCP
nginx_exporter	2379	TCP
nginx_gateway	80	TCP
nginx_gateway	81	TCP
nginx_gateway	443	TCP
nginx_gateway	2379	TCP
nginx_gateway	4443	TCP
nginx_gateway	4567	TCP
nginx_gateway	6379	TCP
nginx_gateway	8080	TCP
nginx_gateway	8081	TCP
nginx_gateway	8082	TCP
nginx_gateway	8083	TCP
nginx_gateway	8085	TCP

Сервис	Порт	Протокол
nginx_gateway	8090	TCP
nginx_gateway	8100	TCP
nginx_gateway	8443	TCP
nginx_gateway	8444	TCP
nginx_gateway	8701	TCP
nginx_gateway	8702	TCP
nginx_gateway	8899	TCP
nginx_gateway	9393	TCP
nginx_gateway	9898	TCP
node_exporter	Любой	Любой
nta_core	25	TCP
nta_core	80	TCP
nta_core	2379	TCP
nta_core	5433	TCP
nta_core	8082	TCP
nta_core	8083	TCP
nta_core	9443	TCP
nta_database	-	-
nta_database_configurator	2379	TCP
nta_database_configurator	5432	TCP
nta_database_configurator	5432	TCP
nta_sensor_configurator	2379	TCP
nta_sensor_configurator	8084	TCP
nta_sensor_configurator	9443	TCP
nta_sensor_configurator	50051	TCP
nta_syncer	80	TCP
nta_syncer	2379	TCP
nta_syncer	5422	TCP
nta_syncer	5423	TCP
nta_syncer	7777	TCP
nta_syncer	8084	TCP
nta_syncer	9092	TCP
nta_syncer	10000:10010	TCP
nta_syncer	50051	TCP
postfix	25	TCP
postfix	2379	TCP
postgresql_exporter	2379	TCP
postgresql_exporter	5432	TCP
postgresql_exporter	9100	TCP
postgresql_server	2379	TCP
postgresql_server	5432	TCP

Сервис	Порт	Протокол
preprocessor	Любой	Любой
preprocessor_icap	80	TCP
preprocessor_icap	1514	TCP
preprocessor_icap	1514	UDP
preprocessor_icap	2379	TCP
preprocessor_icap	4223	TCP
preprocessor_icap	6379	TCP
preprocessor_icap	7777	TCP
preprocessor_icap	8081	TCP
preprocessor_icap	8082	TCP
preprocessor_icap	8083	TCP
preprocessor_icap	9092	TCP
preprocessor_icap	9192	TCP
preprocessor_icap	9284	TCP
preprocessor_icap	10000:10010	TCP
preprocessor_pop	110	TCP
preprocessor_pop	514	TCP
preprocessor_pop	514	UDP
preprocessor_pop	2379	TCP
preprocessor_pop	4223	TCP
preprocessor_pop	6379	TCP
preprocessor_pop	7777	TCP
preprocessor_pop	8081	TCP
preprocessor_pop	8082	TCP
preprocessor_pop	8083	TCP
preprocessor_pop	9081	TCP
preprocessor_pop	9092	TCP
preprocessor_pop	10000:10010	TCP
preprocessor_pop	1:65535	TCP
preprocessor_smtp	514	TCP
preprocessor_smtp	514	UDP
preprocessor_smtp	2379	TCP
preprocessor_smtp	4223	TCP
preprocessor_smtp	6379	TCP
preprocessor_smtp	7777	TCP
preprocessor_smtp	8081	TCP
preprocessor_smtp	8082	TCP
preprocessor_smtp	8083	TCP
preprocessor_smtp	9081	TCP
preprocessor_smtp	9092	TCP
preprocessor_smtp	10000:10010	TCP

Сервис	Порт	Протокол
preprocessor_span	Любой	Любой
primary_database_configurator	2379	TCP
primary_database_configurator	5432	TCP
redis	2379	TCP
redis	6379	TCP
response_actions_processor	514	TCP
response_actions_processor	514	UDP
response_actions_processor	2379	TCP
response_actions_processor	5432	TCP
response_actions_processor	8081	TCP
response_actions_processor	9092	TCP
response_actions_processor	9100	TCP
response_actions_processor	10000:10010	TCP
response_api	514	TCP
response_api	514	UDP
response_api	2379	TCP
response_api	5432	TCP
response_api	8080	TCP
response_api	9092	TCP
response_api	9100	TCP
response_api	10000:10010	TCP
s3rotator	80	TCP
s3rotator	1080	TCP
s3rotator	2379	TCP
s3rotator	9283	TCP
s3rotator	9284	TCP
schema_registry	2379	TCP
schema_registry	8081	TCP
schema_registry	9092	TCP
schema_registry	10000:10010	TCP
sensor_event_processor	2379	TCP
sensor_event_processor	8080	TCP
sensor_event_processor	8081	TCP
sensor_event_processor	9092	TCP
sensor_event_processor	9100	TCP
sensor_event_processor	10000:10010	TCP
services_configurator	2379	TCP
siem_proxy	80	TCP
siem_proxy	514	TCP
siem_proxy	514	UDP
siem_proxy	1080	TCP

Сервис	Порт	Протокол
siem_proxy	1514	TCP
siem_proxy	1514	UDP
siem_proxy	2080	TCP
siem_proxy	2379	TCP
siem_proxy	9284	TCP
siem_proxy	Любой	Любой
snmpd	161	TCP
snmpd	2379	TCP
updater	80	TCP
updater	443	TCP
updater	514	TCP
updater	514	TCP
updater	2379	TCP
updater	5432	TCP
updater	6379	TCP
updater	7777	TCP
updater	8083	TCP
updater	9100	TCP
updater	9500	TCP
updater	1:65535	TCP
updates_consistency_checker	80	TCP
updates_consistency_checker	2379	TCP
updates_consistency_checker	6379	TCP
updates_consistency_checker	8083	TCP
updates_consistency_checker	9092	TCP
updates_consistency_checker	10000:10010	TCP
web_backend	25	TCP
web_backend	80	TCP
web_backend	443	TCP
web_backend	514	TCP
web_backend	514	UDP
web_backend	1080	TCP
web_backend	2379	TCP
web_backend	5432	TCP
web_backend	6379	TCP
web_backend	7777	TCP
web_backend	8080	TCP
web_backend	8081	TCP
web_backend	8082	TCP
web_backend	8083	TCP
web_backend	8085	TCP

Сервис	Порт	Протокол
web_backend	8090	TCP
web_backend	8123	TCP
web_backend	8283	TCP
web_backend	8443	TCP
web_backend	8444	TCP
web_backend	8899	TCP
web_backend	9090	TCP
web_backend	9092	TCP
web_backend	9284	TCP
web_backend	9500	TCP
web_backend	10000:10010	TCP
web_backend	33334	TCP
zookeeper	2181	TCP
zookeeper	2379	TCP
zookeeper	2888	TCP
zookeeper	3888	TCP
zookeeper	9092	TCP
zookeeper	10000:10010	TCP

Порты, используемые сервисами Central Node, установленного на сервере

Для правильной работы приложения с компонентом Central Node, установленным на сервере, необходимо настроить сетевые доступы для исходящих соединений согласно таблице ниже.

Порты для работы сервисов в конфигурации с компонентом Central Node в виде сервера

Сервис	Порт	Протокол
agent_database_configurator	2379	TCP
agent_database_configurator	5432	TCP
agent_database_synchronizer	2379	TCP
agent_database_synchronizer	5432	TCP
agent_database_synchronizer	9092	TCP
agent_database_synchronizer	9100	TCP
agent_database_synchronizer	10000:10010	TCP
agent_server	1080	TCP
agent_server	2379	TCP
agent_server	5432	TCP
agent_server	8100	TCP
agent_server	9090	TCP
agent_server	9284	TCP

Сервис	Порт	Протокол
antiapt_database_configurator	2379	TCP
antiapt_database_configurator	5432	TCP
authorization_service	2379	TCP
authorization_service	4567	TCP
authorization_service	8090	TCP
authorization_service	8443	TCP
authorization_service	8701	TCP
authorization_service	8899	TCP
cadvisor	Любой	Любой
clickhouse	2379	TCP
clickhouse	8123	TCP
clickhouse	9000	TCP
clickhouse_database_configurator	2379	TCP
clickhouse_database_configurator	9000	TCP
clickhouse_metrics_importer	2379	TCP
clickhouse_metrics_importer	6379	TCP
clickhouse_metrics_importer	8123	TCP
clickhouse_metrics_importer	9000	TCP
clickhouse_metrics_importer	9090	TCP
coredns	53	TCP
coredns	53	TCP
coredns	2379	TCP
deployment_api	22	TCP
deployment_api	2377	TCP
deployment_api	2379	TCP
deployment_api	4567	TCP
deployment_api	8080	TCP
deployment_api	8443	TCP
deployment_api	8701	TCP
deployment_api	9141	TCP
deployment_api	9284	TCP
deployment_management_api	53	TCP
deployment_management_api	2379	TCP
deployment_management_api	4567	TCP
deployment_management_api	8091	TCP
deployment_management_api	8443	TCP
deployment_management_api	8701	TCP
deployment_management_api	8702	TCP
deployment_management_api	8765	TCP
deployment_management_api	8899	TCP
deployment_management_api	9141	TCP

Сервис	Порт	Протокол
dhcp_server	Любой	Любой
edr_synchronizer	25	TCP
edr_synchronizer	80	TCP
edr_synchronizer	514	TCP
edr_synchronizer	514	UDP
edr_synchronizer	2379	TCP
edr_synchronizer	5432	TCP
edr_synchronizer	6379	TCP
edr_synchronizer	8081	TCP
edr_synchronizer	8082	TCP
edr_synchronizer	8083	TCP
edr_synchronizer	9092	TCP
edr_synchronizer	10000:10010	TCP
edr_synchronizer	33334	TCP
elasticsearch	2379	TCP
elasticsearch	9200	TCP
elasticsearch	9300	TCP
elasticsearch_data	2379	TCP
elasticsearch_data	9200	TCP
elasticsearch_data	9300	TCP
elasticsearch_exporter	2379	TCP
elasticsearch_exporter	9200	TCP
elasticsearch_exporter	9300	TCP
etcd	2379	TCP
etcd	2380	TCP
events_api	80	TCP
events_api	2379	TCP
events_api	5432	TCP
events_api	8080	TCP
events_api	8081	TCP
events_api	9092	TCP
events_api	9100	TCP
events_api	9284	TCP
events_api	10000:10010	TCP
fastsearch	2379	TCP
fastsearch	8080	TCP
fastsearch	8180	TCP
fastsearch_events_cleaner	9200	TCP
fastsearch_events_importer	2379	TCP
fastsearch_events_importer	8081	TCP
fastsearch_events_importer	9092	TCP

Сервис	Порт	Протокол
fastsearch_events_importer	9100	TCP
fastsearch_events_importer	9200	TCP
fastsearch_events_importer	10000:10010	TCP
hunts_database_configurator	2379	TCP
hunts_database_configurator	5432	TCP
hunts_database_synchronizer	2379	TCP
hunts_database_synchronizer	5432	TCP
hunts_database_synchronizer	9092	TCP
hunts_database_synchronizer	10000:10010	TCP
hunts_event_processor	2379	TCP
hunts_event_processor	5432	TCP
hunts_event_processor	8080	TCP
hunts_event_processor	8081	TCP
hunts_event_processor	9092	TCP
hunts_event_processor	9100	TCP
hunts_event_processor	10000:10010	TCP
hunts_statistics_api	2379	TCP
hunts_statistics_api	5432	TCP
hunts_statistics_api	8080	TCP
hunts_statistics_api	8081	TCP
hunts_statistics_api	9092	TCP
hunts_statistics_api	9100	TCP
hunts_statistics_api	10000:10010	TCP
hunts_statistics_processor	2379	TCP
hunts_statistics_processor	5432	TCP
hunts_statistics_processor	8080	TCP
hunts_statistics_processor	8081	TCP
hunts_statistics_processor	9092	TCP
hunts_statistics_processor	9100	TCP
hunts_statistics_processor	9200	TCP
hunts_statistics_processor	10000:10010	TCP
edr_synchronizer	25	TCP
edr_synchronizer	80	TCP
ids_alert_syncer	514	UDP
ids_alert_syncer	2379	TCP
ids_alert_syncer	5432	TCP
ids_alert_syncer	777	TCP
ids_alert_syncer	8083	TCP
ids_alert_syncer	9092	TCP
ids_alert_syncer	9200	TCP
ids_alert_syncer	10000:10010	TCP

Сервис	Порт	Протокол
ids_alert_syncer	33334	TCP
ioa_update_validator	2379	TCP
ipsec_manager	80	TCP
ipsec_manager	2379	TCP
kafka	2379	TCP
kafka	2181	TCP
kafka	9092	TCP
kafka	9095	TCP
kafka	10000:10010	TCP
kafka_configurator	2181	TCP
kafka_configurator	2379	TCP
kafka_configurator	9092	TCP
kafka_configurator	10000:10010	TCP
kafka_exporter	2379	TCP
kafka_exporter	9092	TCP
kafka_exporter	9100	TCP
kafka_exporter	10000:10010	TCP
kafka_proxy	Любой	Любой
kata_scanner	25	TCP
kata_scanner	80	TCP
kata_scanner	514	TCP
kata_scanner	514	UDP
kata_scanner	443	TCP
kata_scanner	2379	TCP
kata_scanner	5432	TCP
kata_scanner	6379	TCP
kata_scanner	7777	TCP
kata_scanner	8081	TCP
kata_scanner	8082	TCP
kata_scanner	8083	TCP
kata_scanner	9081	TCP
kata_scanner	9090	TCP
kata_scanner	9092	TCP
kata_scanner	9100	TCP
kata_scanner	9284	TCP
kata_scanner	10000:10010	TCP
kata_scanner	33334	TCP
ksb_agent_server	80	TCP
ksb_agent_server	2379	TCP
ksb_agent_server	5432	TCP
ksb_agent_server	8082	TCP

Сервис	Порт	Протокол
ksb_agent_server	8083	TCP
ksb_agent_server	9898	TCP
ksn_proxy	80	TCP
ksn_proxy	443	TCP
ksn_proxy	514	TCP
ksn_proxy	514	UDP
ksn_proxy	2379	TCP
ksn_proxy	7777	TCP
ksn_proxy	8083	TCP
ksn_proxy	9092	TCP
ksn_proxy	9102	TCP
ksn_proxy	10000:10010	TCP
ksn_proxy	1:65535	TCP
ksqldb_configurator	2379	TCP
ksqldb_configurator	5432	TCP
ksqldb_configurator	8083	TCP
ksqldb_configurator	8088	TCP
ksqldb_configurator	9092	TCP
ksqldb_configurator	10000:10010	TCP
ksqldb_server	2379	TCP
ksqldb_server	5432	TCP
ksqldb_server	9092	TCP
ksqldb_server	11000:11006	TCP
management_ui	2379	TCP
management_ui	8091	TCP
monitoring_grafana	3000	TCP
monitoring_prometheus	2379	TCP
monitoring_prometheus	9090	TCP
monitoring_prometheus	9100	TCP
monitoring_prometheus	9102	TCP
monitoring_prometheus	9141	TCP
monitoring_prometheus	9142	TCP
monitoring_prometheus	9191	TCP
monitoring_prometheus	9192	TCP
monitoring_prometheus	9283	TCP
multitenancy_management_api	2379	TCP
multitenancy_management_api	4567	TCP
multitenancy_management_api	8443	TCP
multitenancy_management_api	8701	TCP
multitenancy_management_api	8090	TCP
multitenancy_management_api	8899	TCP

Сервис	Порт	Протокол
nginx_exporter	2379	TCP
nginx_gateway	80	TCP
nginx_gateway	81	TCP
nginx_gateway	443	TCP
nginx_gateway	2379	TCP
nginx_gateway	4443	TCP
nginx_gateway	4567	TCP
nginx_gateway	6379	TCP
nginx_gateway	8080	TCP
nginx_gateway	8081	TCP
nginx_gateway	8082	TCP
nginx_gateway	8083	TCP
nginx_gateway	8085	TCP
nginx_gateway	8090	TCP
nginx_gateway	8100	TCP
nginx_gateway	8443	TCP
nginx_gateway	8444	TCP
nginx_gateway	8701	TCP
nginx_gateway	8702	TCP
nginx_gateway	8899	TCP
nginx_gateway	9393	TCP
nginx_gateway	9898	TCP
node_exporter	Любой	Любой
nta_core	25	TCP
nta_core	80	TCP
nta_core	2379	TCP
nta_core	5433	TCP
nta_core	8082	TCP
nta_core	8083	TCP
nta_core	9443	TCP
nta_database	-	-
nta_database_configurator	2379	TCP
nta_database_configurator	5432	TCP
nta_database_configurator	5432	TCP
nta_sensor_configurator	2379	TCP
nta_sensor_configurator	8084	TCP
nta_sensor_configurator	9443	TCP
nta_sensor_configurator	50051	TCP
nta_syncer	80	TCP
nta_syncer	2379	TCP
nta_syncer	5422	TCP

Сервис	Порт	Протокол
nta_syncer	5423	TCP
nta_syncer	7777	TCP
nta_syncer	8084	TCP
nta_syncer	9092	TCP
nta_syncer	10000:10010	TCP
nta_syncer	50051	TCP
postfix	25	TCP
postfix	2379	TCP
postgresql_exporter	2379	TCP
postgresql_exporter	5432	TCP
postgresql_exporter	9100	TCP
postgresql_server	2379	TCP
postgresql_server	5432	TCP
preprocessor	Любой	Любой
preprocessor_icap	80	TCP
preprocessor_icap	1514	TCP
preprocessor_icap	1514	UDP
preprocessor_icap	2379	TCP
preprocessor_icap	4223	TCP
preprocessor_icap	6379	TCP
preprocessor_icap	7777	TCP
preprocessor_icap	8081	TCP
preprocessor_icap	8082	TCP
preprocessor_icap	8083	TCP
preprocessor_icap	9092	TCP
preprocessor_icap	9192	TCP
preprocessor_icap	9284	TCP
preprocessor_icap	10000:10010	TCP
preprocessor_pop	110	TCP
preprocessor_pop	514	TCP
preprocessor_pop	514	UDP
preprocessor_pop	2379	TCP
preprocessor_pop	4223	TCP
preprocessor_pop	6379	TCP
preprocessor_pop	7777	TCP
preprocessor_pop	8081	TCP
preprocessor_pop	8082	TCP
preprocessor_pop	8083	TCP
preprocessor_pop	9081	TCP
preprocessor_pop	9092	TCP
preprocessor_pop	10000:10010	TCP

Сервис	Порт	Протокол
preprocessor_pop	1:65535	TCP
preprocessor_smtp	514	TCP
preprocessor_smtp	514	UDP
preprocessor_smtp	2379	TCP
preprocessor_smtp	4223	TCP
preprocessor_smtp	6379	TCP
preprocessor_smtp	7777	TCP
preprocessor_smtp	8081	TCP
preprocessor_smtp	8082	TCP
preprocessor_smtp	8083	TCP
preprocessor_smtp	9081	TCP
preprocessor_smtp	9092	TCP
preprocessor_smtp	10000:10010	TCP
preprocessor_span	Любой	Любой
primary_database_configurator	2379	TCP
primary_database_configurator	5432	TCP
redis	2379	TCP
redis	6379	TCP
response_actions_processor	514	TCP
response_actions_processor	514	UDP
response_actions_processor	2379	TCP
response_actions_processor	5432	TCP
response_actions_processor	8081	TCP
response_actions_processor	9092	TCP
response_actions_processor	9100	TCP
response_actions_processor	10000:10010	TCP
response_api	514	TCP
response_api	514	UDP
response_api	2379	TCP
response_api	5432	TCP
response_api	8080	TCP
response_api	9092	TCP
response_api	9100	TCP
response_api	10000:10010	TCP
s3proxy	80	TCP
s3proxy	1080	TCP
s3proxy	2379	TCP
s3rotator	80	TCP
s3rotator	1080	TCP
s3rotator	2379	TCP
s3rotator	9283	TCP

Сервис	Порт	Протокол
s3rotator	9284	TCP
schema_registry	2379	TCP
schema_registry	8081	TCP
schema_registry	9092	TCP
schema_registry	10000:10010	TCP
sensor_event_processor	2379	TCP
sensor_event_processor	8080	TCP
sensor_event_processor	8081	TCP
sensor_event_processor	9092	TCP
sensor_event_processor	9100	TCP
sensor_event_processor	10000:10010	TCP
services_configurator	2379	TCP
siem_proxy	80	TCP
siem_proxy	514	TCP
siem_proxy	514	UDP
siem_proxy	1080	TCP
siem_proxy	1514	TCP
siem_proxy	1514	UDP
siem_proxy	2080	TCP
siem_proxy	2379	TCP
siem_proxy	9284	TCP
siem_proxy	Любой	Любой
snmpd	161	TCP
snmpd	2379	TCP
updater	80	TCP
updater	443	TCP
updater	514	TCP
updater	514	TCP
updater	2379	TCP
updater	5432	TCP
updater	6379	TCP
updater	7777	TCP
updater	8083	TCP
updater	9100	TCP
updater	9500	TCP
updater	1:65535	TCP
updates_consistency_checker	80	TCP
updates_consistency_checker	2379	TCP
updates_consistency_checker	6379	TCP
updates_consistency_checker	8083	TCP
updates_consistency_checker	9092	TCP

Сервис	Порт	Протокол
updates_consistency_checker	10000:10010	TCP
web_backend	25	TCP
web_backend	80	TCP
web_backend	443	TCP
web_backend	514	TCP
web_backend	514	UDP
web_backend	1080	TCP
web_backend	2379	TCP
web_backend	5432	TCP
web_backend	6379	TCP
web_backend	7777	TCP
web_backend	8080	TCP
web_backend	8081	TCP
web_backend	8082	TCP
web_backend	8083	TCP
web_backend	8085	TCP
web_backend	8090	TCP
web_backend	8123	TCP
web_backend	8283	TCP
web_backend	8443	TCP
web_backend	8444	TCP
web_backend	8899	TCP
web_backend	9090	TCP
web_backend	9092	TCP
web_backend	9284	TCP
web_backend	9500	TCP
web_backend	10000:10010	TCP
web_backend	33334	TCP
zookeeper	2181	TCP
zookeeper	2379	TCP
zookeeper	2888	TCP
zookeeper	3888	TCP
zookeeper	9092	TCP
zookeeper	10000:10010	TCP

Порты, используемые сервисами в конфигурации с компонентом Sensor, установленным на отдельном сервере

Для правильной работы приложения в конфигурации с компонентом Sensor, установленным на отдельном сервере, необходимо настроить сетевые доступы для исходящих соединений согласно таблице ниже.

Порты для работы сервисов в конфигурации с компонентом Sensor, установленным на отдельном сервере

Сервис	Порт	Протокол
cadvisor	Любой	Любой
ksn_proxy	80	TCP
ksn_proxy	443	TCP
ksn_proxy	514	TCP
ksn_proxy	514	UDP
ksn_proxy	2379	TCP
ksn_proxy	7777	TCP
ksn_proxy	8083	TCP
ksn_proxy	9092	TCP
ksn_proxy	9102	TCP
ksn_proxy	10000:10010	TCP
monitoring_prometheus	2379	TCP
monitoring_prometheus	9090	TCP
monitoring_prometheus	9100	TCP
monitoring_prometheus	9102	TCP
monitoring_prometheus	9141	TCP
monitoring_prometheus	9142	TCP
monitoring_prometheus	9191	TCP
monitoring_prometheus	9192	TCP
nginx_gateway	443	TCP
nginx_gateway	2379	TCP
nginx_gateway	8085	TCP
nginx_gateway	8100	TCP
nginx_gateway	8283	TCP
node_exporter	Любой	TCP
preprocessor_icap	443	TCP
preprocessor_icap	1080	TCP
preprocessor_icap	1344	TCP
preprocessor_icap	1514	TCP
preprocessor_icap	1514	UDP
preprocessor_icap	2379	TCP

Сервис	Порт	Протокол
preprocessor_icap	4223	TCP
preprocessor_icap	6379	TCP
preprocessor_icap	7777	TCP
preprocessor_icap	8081	UDP
preprocessor_icap	8082	TCP
preprocessor_icap	8082	UDP
preprocessor_icap	8083	TCP
preprocessor_icap	8085	TCP
preprocessor_icap	9092	TCP
preprocessor_pop3	1514	TCP
preprocessor_pop3	1514	UDP
preprocessor_pop3	2379	TCP
preprocessor_pop3	4223	TCP
preprocessor_pop3	6379	TCP
preprocessor_pop3	7777	TCP
preprocessor_pop3	8081	TCP
preprocessor_pop3	8081	UDP
preprocessor_pop3	8082	UDP
preprocessor_pop3	8083	TCP
preprocessor_pop3	9081	TCP
preprocessor_pop3	9092	TCP
preprocessor_pop3	11000	TCP
preprocessor_smtp	1514	TCP
preprocessor_smtp	1514	UDP
preprocessor_smtp	2379	TCP
preprocessor_smtp	4223	TCP
preprocessor_smtp	6379	TCP
preprocessor_smtp	7777	TCP
preprocessor_smtp	8081	TCP
preprocessor_smtp	8081	UDP
preprocessor_smtp	8082	UDP
preprocessor_smtp	8083	TCP
preprocessor_smtp	9081	TCP
preprocessor_smtp	9092	TCP
preprocessor_smtp	11000	TCP
preprocessor_span	Любой	Любой
preprocessor_span	13520	TCP
preprocessor_span	8081	UDP
preprocessor_span	8082	UDP
preprocessor_span	9081	TCP
preprocessor_span	7777	TCP

Сервис	Порт	Протокол
preprocessor_span	9092	TCP
preprocessor_span	8083	TCP
preprocessor_span	2379	TCP
preprocessor_span	6379	TCP
redis	2379	TCP
redis	6379	TCP
s3proxy	80	TCP
s3proxy	1080	TCP
s3proxy	2379	TCP
s3rotator	80	TCP
s3rotator	1080	TCP
s3rotator	2379	TCP
s3rotator	9284	TCP
sensor_management_api	Любой	Любой
services_configurator	2379	TCP
siem_proxy	80	TCP
siem_proxy	514	TCP
siem_proxy	514	UDP
siem_proxy	1080	TCP
siem_proxy	1514	TCP
siem_proxy	1514	UDP
siem_proxy	2080	TCP
siem_proxy	2379	TCP
siem_proxy	9284	TCP
snmpd	161	TCP
snmpd	2379	TCP

Порты для взаимодействия между сервисами анализа трафика сети

Для правильной работы приложения нужно убедиться, что сервисы анализа трафика сети могут взаимодействовать через порты, указанные в таблице ниже. Входящие соединения для сервисов разрешены по умолчанию.

Порты для взаимодействия между сервисами анализа трафика сети

Сервис	Порт	Целевой сервис	Протокол
nta_database_configurator	5433	nta_database	TCP
nta_core	5433	nta_database	TCP
nta_core	2379	etcd	TCP
nta_core	80	web_backend	TCP
nta_core	9443	internet	TCP

Сервис	Порт	Целевой сервис	Протокол
nta_syncer	9092	kafka	TCP
nta_syncer	2379	etcd	TCP
nta_syncer	5432	postgresql_server	TCP
nta_syncer	5433	nta_database	TCP
nta_syncer	50051	nta_core	TCP
nta_syncer	8084	nta_core	TCP
nta_sensor_configurator	50051	nta_core	UDP
nta_sensor_configurator	9443	nta_core	TCP
preprocessor_span	13520	nta_core	TCP
preprocessor_span	8081	kata_scanner	UDP
preprocessor_span	8082	kata_scanner	UDP
preprocessor_span	9081	kata_scanner	TCP
preprocessor_span	7777	ksn_proxy	TCP
preprocessor_span	9092	kafka	TCP
preprocessor_span	8083	updater	TCP
preprocessor_span	2379	etcd	TCP
preprocessor_span	6379	redis	TCP
preprocessor_icap	9092	kafka	TCP
preprocessor_icap	7777	ksn_proxy	TCP
preprocessor_icap	8081	kata_scanner	UDP
preprocessor_icap	8082	kata_scanner	UDP
preprocessor_icap	2379	etcd	TCP
preprocessor_icap	8083	updater	TCP
preprocessor_icap	4223	preprocessor_span	TCP
preprocessor_smtp	8081	kata_scanner	UDP
preprocessor_smtp	8082	kata_scanner	UDP
preprocessor_smtp	9081	kata_scanner	TCP
preprocessor_smtp	7777	ksn_proxy	TCP
preprocessor_smtp	9092	kafka	TCP
preprocessor_smtp	8083	updater	TCP
preprocessor_smtp	2379	etcd	TCP
preprocessor_smtp	6379	redis	TCP
preprocessor_smtp	4223	preprocessor_span	TCP
preprocessor_pop3	8081	kata_scanner	UDP
preprocessor_pop3	8082	kata_scanner	UDP
preprocessor_pop3	9081	kata_scanner	TCP
preprocessor_pop3	7777	ksn_proxy	TCP
preprocessor_pop3	9092	kafka	TCP
preprocessor_pop3	8083	updater	TCP
preprocessor_pop3	2379	etcd	TCP

Сервис	Порт	Целевой сервис	Протокол
preprocessor_pop3	6379	redis	TCP
preprocessor_pop3	4223	preprocessor_span	TCP

Управление параметрами MTU в iptables

Если вам известно, что провайдер ограничивает размер MTU на каналах связи между компонентами решения, вы можете настроить параметры MTU в iptables таким образом, чтобы размер MTU не превышал заданного значения. Например, если провайдер ограничивает размер MTU значением 1450, вы можете указать в iptables значение 1400.

Для упрощения настройки и для сохранения заданных параметров при перезагрузках компонентов решения рекомендуется использовать утилиту kata-firewall-persist-mtu. Утилита становится доступной при обновлении Kaspersky Anti Targeted Attack Platform до версии 7.1.

Чтобы настроить параметры MTU в iptables:

1. Войдите в консоль управления сервера Central Node по протоколу SSH или через терминал.

   Если Central Node развернут в виде кластера, войдите в консоль управления любого из серверов кластера с ролью manager в Docker swarm. Для просмотра роли используйте команду `$ docker node ls`.

2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке компонента.

   Отобразится меню администратора компонента приложения.

3. В меню администратора приложения выберите режим **Technical Support Mode**.

4. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Ok** и нажмите на клавишу **ENTER**.

6. Запустите утилиту с параметрами по образцу:

   ```
   kata-firewall-persist-mtu set --mss <MSS size> --ip <IP address 1> --ip <IP address 2>
   ```

   где

   - `<MSS size>` – величина MSS (англ. Maximum segment size), рассчитывается как величина MTU без учета длины заголовков TCP и IP.
   - `<IP address 1>` и `<IP address 2>` – IP-адреса серверов, к которым нужно применить настройку. Эту опцию можно указывать столько раз, сколько необходимо, по количеству серверов, к которым нужно применить настройку.

   В течение нескольких минут утилита сохранит указанные параметры в iptables и обеспечит их сохранение в случае перезагрузки серверов.

7. Выполните команду:

   ```
   systemctl restart kata-firewall
   ```

Параметры MTU будут настроены.

Дополнительные возможности утилиты kata-firewall-persist-mtu

Дополнительные возможности утилиты:

- Вызов справки:

  ```
  kata-firewall-persist-mtu --help
  ```

- Просмотр текущих настроек:

  ```
  kata-firewall-persist-mtu get
  ```

- Удаление настроек (настройки больше не восстанавливаются при перезагрузке серверов):

  ```
  kata-firewall-persist-mtu flush
  ```

Настройка интеграции компонента Endpoint Agent с функциональным блоком KEDR

В этом разделе содержится информация о том, как настроить интеграцию функционального блока KEDR с приложениями, которые используются в роли компонента Endpoint Agent.

Настройка доверенного соединения с приложением Kaspersky Endpoint Security

Действия по настройке доверенного соединения выполняются как на стороне Kaspersky Anti Targeted Attack Platform, так и на стороне Kaspersky Endpoint Security.

Вы можете использовать один из следующих вариантов доверенного соединения:

- **Настройка соединения с сервером Central Node без проверки TLS-сертификата Kaspersky Endpoint Security в Kaspersky Anti Targeted Attack Platform**.

  Kaspersky Endpoint Security устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Central Node. Kaspersky Anti Targeted Attack Platform не проверяет TLS-сертификат Kaspersky Endpoint Security при попытке подключения Kaspersky Endpoint Security.

  Если вы используете этот вариант настройки доверенного соединения, настройка состоит из следующих этапов:

  1. Генерация или загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node в веб-интерфейсе Central Node (если TLS-сертификат сервера Central Node не был создан ранее)
  2. Скачивание TLS-сертификата сервера Central Node на компьютер
  3. Подключение компьютера с Kaspersky Endpoint Security к серверу Central Node:
     - Подключение Kaspersky Endpoint Security для Windows.
     - Подключение Kaspersky Endpoint Security для Linux.
     - Подключение Kaspersky Endpoint Security для Mac.

- **Настройка соединения с сервером Central Node с проверкой TLS-сертификата Kaspersky Endpoint Security на стороне Kaspersky Anti Targeted Attack Platform**.

  Kaspersky Endpoint Security устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Central Node. В Kaspersky Endpoint Security настроена дополнительная защита соединения и загружен TLS-сертификат Kaspersky Endpoint Security. Kaspersky Anti Targeted Attack Platform проверяет TLS-сертификат Kaspersky Endpoint Security при попытке подключения Kaspersky Endpoint Security.

Если вы используете этот вариант настройки доверенного соединения, настройка состоит из следующих этапов:

1. Генерация или загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node в веб-интерфейсе Central Node (если TLS-сертификат сервера Central Node не был создан ранее)
2. Скачивание TLS-сертификата сервера Central Node на компьютер
3. Включение проверки TLS-сертификата Kaspersky Endpoint Security в веб-интерфейсе Kaspersky Anti Targeted Attack Platform
4. Генерация и скачивание криптоконтейнера с TLS-сертификатом Kaspersky Endpoint Security или загрузка самостоятельно подготовленного TLS-сертификата Kaspersky Endpoint Security через веб-интерфейс Kaspersky Anti Targeted Attack Platform

   Если вы подготавливаете TLS-сертификат Kaspersky Endpoint Security самостоятельно, вам нужно создать криптоконтейнер формата PFX с этим сертификатом. Подробнее о работе с TLS-сертификатами см. в документации OpenSSL.

5. Подключение компьютера с Kaspersky Endpoint Security к серверу Central Node:
   - Подключение Kaspersky Endpoint Security для Windows.
   - Подключение Kaspersky Endpoint Security для Linux.
   - Подключение Kaspersky Endpoint Security для Mac.

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Скачивание TLS-сертификата сервера Central Node на компьютер

Чтобы скачать TLS-сертификат сервера на компьютер:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сертификаты**.
2. В разделе **Сертификат сервера** нажмите на кнопку **Экспортировать**.

Файл сертификата сервера будет сохранен в папке загрузки браузера.

Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Если вы уже используете TLS-сертификат сервера Central Node и сгенерируете новый сертификат, сертификат, который используется в приложении, будет удален и заменен на сгенерированный сертификат.

Вам потребуется указать данные нового сертификата везде, где использовался старый.

Если вы замените TLS-сертификат на новый, вам потребуется:

- Повторно авторизовать почтовые сенсоры (KSMG, KLMS) на Central Node.
- Повторно настроить соединение Central Node, PCN и SCN с Sandbox.
- Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent.
- Загрузить новый сертификат в Active Directory (если вы используете Active Directory).

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

Чтобы сгенерировать TLS-сертификат сервера Central Node:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификат сервера** нажмите на кнопку **Сгенерировать**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Kaspersky Anti Targeted Attack Platform сгенерирует новый TLS-сертификат. Страница автоматически обновится.

Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Anti Targeted Attack Platform

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Anti Targeted Attack Platform.

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.

  Приложение не работает с сертификатами другого формата.

  Если вы подготовили сертификат в другом формате, вам нужно конвертировать его в формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Если вы уже используете TLS-сертификат сервера Central Node и загрузите новый сертификат, сертификат, который используется в приложении, будет удален и заменен на загруженный сертификат.

Вам потребуется указать данные нового сертификата везде, где использовался старый.

Если вы замените TLS-сертификат на новый, вам потребуется:

- Повторно авторизовать почтовые сенсоры (KSMG, KLMS) на Central Node.
- Повторно настроить соединение Central Node, PCN и SCN с Sandbox.
- Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent.

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

Чтобы загрузить самостоятельно подготовленный TLS-сертификат через веб-интерфейс Kaspersky Anti Targeted Attack Platform:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сертификаты**.

3. В разделе **Сертификат сервера** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

4. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

   TLS-сертификат будет добавлен в Kaspersky Anti Targeted Attack Platform.

   Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent.

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

Включение проверки TLS-сертификата компонента Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Чтобы включить использование доверенного соединения с приложением, которое выступает в роли компонента Endpoint Agent:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.

2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.

3. В разделе **Сертификаты Endpoint Agent** включите переключатель **Проверять TLS-сертификаты Endpoint Agent**.

Kaspersky Anti Targeted Attack Platform будет проверять данные TLS-сертификата при попытках подключения приложения, которое выступает в роли компонента Endpoint Agent, к Kaspersky Anti Targeted Attack Platform.

Генерация TLS-сертификата компонента Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и скачивание криптоконтейнера

Чтобы сгенерировать и загрузить TLS-сертификат соединения Kaspersky Anti Targeted Attack Platform с приложением, которое используется в роли компонента Endpoint Agent:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.

2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.

3. В разделе **Сертификаты Endpoint Agent** нажмите на кнопку **Сгенерировать и экспортировать**.

   Откроется окно **Экспорт сертификата**.

4. В разделе **Защитить файл паролем** укажите пароль в полях **Пароль** и **Подтвердите пароль**. Рекомендуется сохранить этот пароль для дальнейшего использования, так как в приложении пароль не сохраняется.

   > Криптоконтейнер должен быть защищен паролем. Добавить в Kaspersky Endpoint Security криптоконтейнер с пустым паролем невозможно.

5. Нажмите на кнопку **Экспортировать**.

   Новый TLS-сертификат отобразится в таблице TLS-сертификатов. На ваш локальный компьютер в папку загрузки браузера будет загружен файл криптоконтейнера с сертификатом приложения, которое выступает в роли компонента Endpoint Agent, в формате PFX.

Подробнее о работе с TLS-сертификатами см. в документации OpenSSL.

> В криптоконтейнере содержится только файл сертификата и не содержится файл закрытого ключа. Kaspersky Anti Targeted Attack Platform не хранит закрытые ключи TLS-шифрования соединения.

Загрузка самостоятельно подготовленного TLS-сертификата компонента Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Anti Targeted Attack Platform.

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Если вы подготавливаете TLS-сертификат компонента Endpoint Agent самостоятельно, вам нужно создать криптоконтейнер формата PFX с этим сертификатом и загрузить криптоконтейнер в приложение, выступающее в роли компонента Endpoint Agent.

Подробнее о работе с TLS-сертификатами см. в документации OpenSSL.

> В криптоконтейнере должен содержится только файл сертификата и не должен содержится файл закрытого ключа. Kaspersky Anti Targeted Attack Platform не хранит закрытые ключи TLS-шифрования соединения.

Чтобы загрузить самостоятельно подготовленный TLS-сертификат через веб-интерфейс Kaspersky Anti Targeted Attack Platform:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификаты Endpoint Agent** нажмите на кнопку **Импортировать**.

   Откроется окно выбора файлов.
4. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Anti Targeted Attack Platform.

Просмотр таблицы TLS-сертификатов компонента Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Чтобы просмотреть список TLS-сертификатов соединения с приложениями, которые выступают в роли компонента Endpoint Agent, через веб-интерфейс Kaspersky Anti Targeted Attack Platform:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификаты Endpoint Agent** отобразится список TLS-сертификатов со следующими данными по каждому сертификату:
   - **TLS-сертификат** - отпечаток сертификата.
   - **Серийный номер** - серийный номер сертификата.
   - **Истекает** - дата истечения срока действия сертификата.

Фильтрация и поиск TLS-сертификатов компонента Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Вы можете отфильтровать TLS-сертификаты для отображения в таблице по одной или обеим столбцам **TLS-сертификат** и **Серийный номер** или выполнить поиск TLS-сертификатов по этим столбцам таблицы по указанным вами показателям.

Чтобы выполнить фильтрацию и поиск TLS-сертификатов в таблице:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификаты Endpoint Agent** отобразится список TLS-сертификатов со следующими данными по каждому сертификату:
   - **TLS-сертификат** - отпечаток сертификата.
   - **Серийный номер** - серийный номер сертификата.
   - **Истекает** - дата истечения срока действия сертификата.
4. Если вы хотите отфильтровать или найти TLS-сертификаты по отпечатку сертификата:
   a. По ссылке **TLS-сертификат** откройте окно настройки фильтрации.
   b. В поле **TLS-сертификат** введите несколько символов отпечатка сертификата.
   c. Нажмите на кнопку **Применить**.
5. Если вы хотите отфильтровать или найти TLS-сертификаты по серийному номеру:
   a. По ссылке **Серийный номер** откройте окно настройки фильтрации.
   b. В поле **Серийный номер** введите несколько символов серийного номера.
   c. Нажмите на кнопку **Применить**.

В таблице отобразятся только TLS-сертификаты, соответствующие заданным вами условиям.

Чтобы сбросить фильтр по одному или нескольким условиям фильтрации,

нажмите на кнопку справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

> Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

Удаление TLS-сертификатов компонента Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Чтобы удалить один или несколько TLS-сертификатов соединения с приложениями, которые выступают в роли компонента Endpoint Agent, через веб-интерфейс Kaspersky Anti Targeted Attack Platform:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты Endpoint Agent**.

   В разделе **Сертификаты Endpoint Agent** отобразится список TLS-сертификатов.
3. Установите флажки рядом с одним или несколькими TLS-сертификатами, которые вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Выбранные TLS-сертификаты будут удалены.

Настройка перенаправления трафика от компонента Endpoint Agent на сервер Sensor

Вы можете использовать Sensor в качестве прокси-сервера при обмене данными между компонентами Endpoint Agent и Central Node, чтобы снизить нагрузку на Central Node. Для этого при подключении приложения, которое выступает в роли компонента Endpoint Agent, на стороне этого приложения вместо IP-адреса сервера Central Node вам нужно указать IP-адрес сервера Sensor. Sensor должен быть установлен на отдельном от Central Node сервере.

При настройке перенаправления трафика учитывайте следующие ограничения:

- Максимальный объем входящего трафика для Sensor не должен превышать 1 Гбит/с.
- Рекомендуемая ширина канала между серверами Central Node и Sensor составляет 15% от трафика на SPAN-порте.
- Максимально допустимые потери пакетов, пересылаемых между серверами Sensor и Central Node, составляют 10% при задержке отправки пакетов до 100 мс.

Для использования Sensor в качестве прокси-сервера подключите Sensor к Central Node.

Настройка интеграции компонента Endpoint Agent с функциональным блоком NDR

Если вы используете функциональность NDR, вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с компонентом Endpoint Agent, представленным Kaspersky Endpoint Security 12.7 для Windows и Kaspersky Endpoint Security 12.2 для Linux, и получать об устройствах, на которых установлен компонент, следующие данные:

- Информация о событиях NDR, записанных в базу событий в результате срабатывания технологии EPP (события защиты рабочих станций и серверов).
- Сведения об устройствах (например, версия операционной системы, сведения о модели или производителе).
- Сведения о соединениях устройств на карте сетевых взаимодействий.
- Сведения о протоколах, по которым осуществляется соединение между устройствами.

Вы можете подключить к одному компоненту Central Node до 2 000 компонентов Endpoint Agent.

Для интеграции с функциональным блоком NDR приложения Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Security Linux должны быть активированы с помощью лицензии *KESB Advanced* или *KESB Total*.

Данные от компьютеров с компонентом Endpoint Agent поступают в Kaspersky Anti Targeted Attack Platform через *серверы интеграции*. Функции сервера интеграции может выполнять любой сервер с установленным компонентом Kaspersky Anti Targeted Attack Platform (Central Node или Sensor). Для интеграции с Endpoint Agent вам нужно добавить серверы интеграции на те серверы, которые будут получать данные от компьютеров с Endpoint Agent.

Компьютеры с Endpoint Agent устанавливают защищенные соединения с серверами интеграции по протоколу HTTPS. Для обеспечения безопасности соединений используются сертификаты, выданные сервером Central Node. Для соединений могут использоваться следующие сертификаты:

- Сертификат сервера интеграции. Этот сертификат проверяет компьютер с Endpoint Agent при каждой установке соединения. Соединение не устанавливается до успешного завершения проверки сертификата.
- Сертификат клиента. Этот сертификат используется для аутентификации клиентов сервера интеграции, которыми являются компьютеры с Endpoint Agent. Один и тот же сертификат клиента может использоваться несколькими компьютерами с Endpoint Agent. По умолчанию сервер интеграции не выполняет проверку сертификатов клиентов, но вы можете ее включить для усиления защиты соединений.

Доставка сертификатов и открытых ключей на компьютеры с Endpoint Agent выполняется с помощью Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux. Для загрузки этих данных в Kaspersky Endpoint Security используется файл свертки, который нужно создать в Kaspersky Anti Targeted Attack Platform после добавления сервера интеграции.

В режиме распределенного решения и мультитенантности действия по настройке интеграции с функциональным блоком NDR должны выполняться на том сервере Central Node, с котором вы хотите настроить интеграцию.

Настраивать получение данных от компонентов Endpoint Agent могут только пользователи с ролью **Администратор**. Пользователи с ролью **Аудитор** могут просматривать список серверов интеграции.

Сценарий подготовки к получению данных от компонента Endpoint Agent

В режиме распределенного решения и мультитенантности действия, которые необходимо выполнить на стороне Kaspersky Anti Targeted Attack Platform должны выполняться на том сервере Central Node, для которого вы хотите настроить получение данных от компонента Endpoint Agent.

Сценарий подготовки к получению данных от компонента Endpoint Agent состоит из следующих этапов:

1. **Установка компонента Endpoint Agent на компьютеры контролируемой сети**

   На этом этапе вам нужно установить приложение Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux, выполняющее функции компонента Endpoint Agent, на все компьютеры, данные о которых вы хотите получать в Kaspersky Anti Targeted Attack Platform. Эти компьютеры должны находиться в той же сети, в которую входит один из серверов с компонентом Sensor.

   В текущей версии Kaspersky Anti Targeted Attack Platform поддерживает получение и обработку данных только при интеграции с Kaspersky Endpoint Security для Windows версии 12.7 и выше или Kaspersky Endpoint Security для Linux версии 12.2 и выше.

2. **Добавление серверов интеграции для компонентов Kaspersky Anti Targeted Attack Platform**

   На этом этапе выполняются процедуры добавления серверов интеграции на серверы с компонентами, к которым будут подключаться компоненты Endpoint Agent. Сетевые взаимодействия серверов с компонентами Endpoint Agent возможны только через сетевые интерфейсы, не используемые в качестве точек мониторинга. При этом для серверов интеграции не настраиваются конкретные сетевые интерфейсы и IP-адреса, поскольку для внешнего подключения к серверу интеграции может использоваться любой из доступных сетевых интерфейсов и IP-адресов компьютера.

3. **Создание файлов свертки для клиентов серверов интеграции**

   На этом этапе вам нужно создать и скачать файлы свертки, в которых приложение сохраняет сертификаты и ключи для подключений клиентов к серверам интеграции. Каждый файл свертки представляет собой архив, содержащий следующие данные:

   - Открытый ключ сертификата сервера интеграции.
   - Сертификат для клиентов сервера интеграции (с закрытым ключом). Этот сертификат добавляется, если на сервере интеграции включена проверка сертификатов клиентов. Сертификат и ключ сохраняются в зашифрованном виде с использованием пароля, указанного при создании файла свертки.

4. **Загрузка данных для подключения к серверам интеграции на компьютеры клиентов**

   Этот этап рекомендуется выполнять с использованием Kaspersky Security Center. Клиентами для серверов интеграции Kaspersky Anti Targeted Attack Platform являются компьютеры с компонентом Endpoint Agent. Вам нужно загрузить сертификаты и/или ключи из файлов свертки на Сервер администрирования Kaspersky Security Center с помощью плагина управления Endpoint Agent. После этого вам нужно создать политики в Kaspersky Security Center для загрузки данных на компьютеры с Endpoint Agent. Сведения о работе с данными и создании политик см. в документации приложений Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Security для Linux.

   Для каждого сервера интеграции должна быть создана как минимум одна политика, содержащая следующие данные для загрузки на компьютеры клиентов:

   - Открытый ключ сертификата сервера интеграции.
   - IP-адрес для подключения к серверу интеграции. Вы можете указать любой из доступных IP-адресов узла с сервером интеграции. IP-адреса можно просмотреть в веб-интерфейс в разделе **Параметры**, подразделе **Серверы подключений** на вкладке **Серверы интеграции**. Для подключения используется порт 8085.
   - Сертификат для клиентов сервера интеграции (с закрытым ключом). Этот сертификат добавляется, если на сервере интеграции включена проверка сертификатов клиентов.

5. **Включение серверов интеграции**

   Этот этап выполняется после применения политик и загрузки данных на компьютеры с компонентом Endpoint Agent. На этом этапе вам нужно включить все серверы интеграции, на которые будут передаваться данные от EPP-приложений.

В результате выполнения сценария Kaspersky Anti Targeted Attack Platform начнет получать и обрабатывать данные от EPP-приложений.

Таблица серверов интеграции

Таблица серверов интеграции отображается в разделе **Параметры**, подразделе **Серверы подключений** на вкладке **Серверы интеграции**. В этой таблице отображаются сведения о серверах интеграции, добавленных на серверах с установленными компонентами приложения.

Таблица серверов интеграции содержит следующие сведения:

- **Имя узла** – имя сервера с установленным компонентом приложения.
- **IP-адреса** – список IP-адресов на всех сетевых интерфейсах сервера с компонентом Kaspersky Anti Targeted Attack Platform (для серверов интеграции не настраиваются конкретные сетевые интерфейсы и IP-адреса, поскольку для внешнего подключения к серверу интеграции может использоваться любой из доступных сетевых интерфейсов и IP-адресов компьютера).
- **Запросов в секунду** – среднее количество успешно обработанных запросов, поступивших от клиентов на сервер интеграции.
- **Статус** – текущий статус сервера интеграции.
- **Проверка сертификата клиента** – признак включенной или выключенной проверки сертификатов клиентов (если проверка выключена, ячейка таблицы пустая).

В режиме распределенного решения и мультитенантности в таблице отображается информация только о серверах интеграции, добавленных на том сервере Central Node, в веб-интерфейсе которого вы находитесь.

Добавление сервера интеграции

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы добавить сервер интеграции:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения перейдите в раздел **Параметры**, подраздел **Серверы подключений**.
3. На вкладке **Серверы интеграции** нажмите на кнопку **Добавить сервер интеграции с Endpoint Agent**.
4. В раскрывающемся списке **Узел** выберите сервер с установленным компонентом Central Node или Sensor, на который требуется добавить сервер интеграции.

   Вы можете выбрать только тот узел, на который еще не добавлен сервер интеграции.
5. При необходимости добавьте один или несколько сертификатов для клиентов сервера интеграции. Для создания сертификата в блоке параметров **Сертификаты для клиентов (режим TCP)** нажмите на кнопку **Создать новый сертификат**. Для интеграции с компонентом Endpoint Agent используются только сертификаты в режиме TCP.

   Вы можете удалить лишние сертификаты из списка с помощью значка ×, который расположен справа от поля с отпечатком сертификата.

   Если вы создали несколько сертификатов клиентов, вы сможете выбирать нужный сертификат при создании файла свертки.
6. Нажмите на кнопку **Сохранить**.

Сервер интеграции будет добавлен.

Создание файла свертки для клиентов сервера интеграции

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

После добавления сервера интеграции или после изменения его параметров вам нужно создать и скачать файл свертки для клиентов этого сервера.

Чтобы создать новый файл свертки для клиентов сервера интеграции:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения перейдите в раздел **Параметры**, подраздел **Серверы подключений**.
3. На вкладке **Серверы интеграции** выберите сервер, для клиентов которого вы хотите создать новый файл свертки.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку ⋮.
5. Выберите **Получить файл свертки для клиентов**.
6. Если для сервера интеграции включена проверка сертификатов клиентов, откроется окно **Генерация нового файла свертки**. Выполните следующие действия:

   a. В раскрывающемся списке **Тип соединения** выберите **TCP**.

   b. В раскрывающемся списке **Сертификат для клиентов** выберите нужный сертификат, который будет использоваться для аутентификации клиентов сервера интеграции.

   c. Укажите пароль для доступа к выбранному сертификату. С использованием заданного пароля будет зашифрован сертификат в файле свертки коннектора.

   d. Нажмите на кнопку **Создать файл свертки**.

Central Node сформирует новый файл свертки для клиентов выбранного сервера интеграции, после чего браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Содержимое полученного файла свертки вам нужно загрузить на компьютеры клиентов сервера интеграции. Вы можете выполнить загрузку с помощью политик Сервера администрирования Kaspersky Security Center. В политиках Kaspersky Security Center нужно указать IP-адрес для подключения к серверу интеграции (для этого вы можете использовать один из доступных IP-адресов, указанных в области деталей выбранного сервера интеграции). Подробнее о создании и настройке политик Kaspersky Security Center см. в документации Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux.

Включение и выключение сервера интеграции

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Серверы интеграции могут быть включены или выключены. По умолчанию после создания сервер интеграции выключен, поэтому данные от клиентов этого сервера не обрабатываются в Kaspersky Anti Targeted Attack Platform.

Чтобы включить или выключить сервер интеграции:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения перейдите в раздел **Параметры**, подраздел **Серверы подключений**.
3. На вкладке **Серверы интеграции** выберите сервер, который вы хотите включить или выключить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Включить** или **Выключить**.

Сервер интеграции будет включен или выключен.

Изменение параметров сервера интеграции

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

При изменении параметров сервера интеграции вы можете заменить сертификат для самого сервера интеграции, а также включить или выключить проверку сертификатов клиентов и изменить список сертификатов для клиентов.

Чтобы изменить параметры сервера интеграции:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения перейдите в раздел **Параметры**, подраздел **Серверы подключений**.
3. На вкладке **Серверы интеграции** выберите сервер, для клиентов которого вы хотите изменить параметры.

   В правой части окна веб-интерфейса появится область деталей.
4. На панели инструментов нажмите на кнопку **Изменить**.
5. Если вы хотите заменить (выпустить новый) сертификат для самого сервера интеграции, нажмите на кнопку **Перевыпустить сертификат**.

   После замены сертификата сервера интеграции его старый сертификат становится недействительным.
6. Если вы хотите изменить список сертификатов для клиентов, используйте кнопку **Создать новый сертификат**, чтобы добавить новый сертификат к уже имеющимся, и/или значок ×, располагающийся справа от поля с отпечатком сертификата, чтобы удалить ранее добавленные сертификаты.

   Чтобы параметры успешно сохранились, в списке должен быть хотя бы один сертификат.
7. Нажмите на кнопку **Сохранить**.

Параметры сервера интеграции будут изменены.

Если для сервера интеграции выпущен новый сертификат или созданы новые сертификаты клиентов, вам нужно снова создать и скачать файл свертки для отправки данных об этих сертификатах на компьютеры клиентов.

Удаление сервера интеграции

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы удалить сервер интеграции:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения перейдите в раздел **Параметры**, подраздел **Серверы подключений**.
3. На вкладке **Серверы интеграции** выберите сервер, который вы хотите удалить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку ⋮.
5. Выберите **Удалить**.

   Откроется окно с запросом подтверждения.
6. В окне запроса нажмите на кнопку **ОК**.

Сервер интеграции будет удален.

Интеграция с почтовыми сенсорами

Вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с *почтовыми сенсорами*. Почтовый сенсор – это сервер или виртуальная машина, на которой установлено приложение Kaspersky Secure Mail Gateway (далее также "KSMG") или Kaspersky Security для Linux Mail Server (далее также "KLMS").

В результате интеграции приложения отправляют копии сообщений электронной почты на проверку Kaspersky Anti Targeted Attack Platform и могут блокировать отдельные сообщения по результатам проверки. При обнаружении угрозы Kaspersky Anti Targeted Attack Platform создает алерт.

Если вы настроили правила исключений из проверки по получателям сообщений и MD5-суммам файлов на стороне Kaspersky Anti Targeted Attack Platform, эти правила не применяются при обработке сообщений почтовыми сенсорами.

Начало работы с приложением

Этот раздел содержит информацию о том, как начать работу с приложением в веб-интерфейсе, в меню администратора и в режиме Technical Support Mode.

Начало работы в веб-интерфейсе приложения под учетной записью администратора

Веб-интерфейс Kaspersky Anti Targeted Attack Platform защищен от **CSRF-атак** и работает только в том случае, если браузер пользователя веб-интерфейса приложения предоставляет заголовок Referrer HTTP-запроса POST. Убедитесь, что браузер, который вы используете для работы с веб-интерфейсом Kaspersky Anti Targeted Attack Platform, не модифицирует заголовок Referrer HTTP-запроса POST. Если соединение с веб-интерфейсом Kaspersky Anti Targeted Attack Platform осуществляется через прокси-сервер вашей организации, убедитесь, что прокси-сервер не модифицирует заголовок Referrer HTTP-запроса POST.

Cross-Site Request Forgery (также "XSRF-атака"). Атака на пользователей веб-сайтов, использующая уязвимости HTTP-протокола. Атака позволяет производить действия от имени авторизованного пользователя уязвимого веб-сайта. Например, от имени авторизованного пользователя уязвимого веб-сайта злоумышленник может тайно отправлять запрос на сервер сторонней платежной системы для перевода денег на счет злоумышленника.

После установки Kaspersky Anti Targeted Attack Platform вам требуется настроить параметры масштабирования приложения.

Если параметры масштабирования Kaspersky Anti Targeted Attack Platform не настроены, вход в веб-интерфейс приложения недоступен.

Чтобы начать работу в веб-интерфейсе приложения под учетной записью администратора приложения:

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, в адресной строке браузера введите IP-адрес сервера с компонентом Central Node.

   Если вы используете отказоустойчивую версию приложения, вы можете ввести IP-адрес любого сервера кластера Central Node или **полное доменное имя (FQDN) кластера**.

   Для обеспечения бесперебойного доступа к веб-интерфейсу программы вы можете настроить на сервере DNS функцию Round Robin. В этом случае осуществляется вход в веб-интерфейс первого работоспособного сервера кластера Central Node.

   Откроется окно ввода учетных данных пользователя Kaspersky Anti Targeted Attack Platform.

2. Введите имя admin и пароль, заданный при развертывании компонента Central Node.

3. Нажмите на кнопку **Войти**.

   Откроется страница **Мониторинг** веб-интерфейса приложения.

Вы можете начать работу с приложением под учетной записью администратора.

Количество одновременных сеансов работы с приложением под одной учетной записью ограничено одним IP-адресом. При попытке входа в приложение под этим же именем пользователя с другого IP-адреса, первый сеанс работы с приложением завершается.

Начало работы в меню администратора приложения

Вы можете работать с параметрами компонентов Sensor, Central Node и Sandbox в меню администратора в консоли управления каждого сервера, на котором установлен компонент приложения.

Убедитесь что доступ к меню администратора и консоли управления серверами Kaspersky Anti Targeted Attack Platform есть только с тех компьютеров, которым вы разрешили этот доступ.

Убедитесь, что компьютеры, которым вы разрешаете доступ, находятся в защищенном периметре вашей сети.

Вы можете настроить доступ к меню администратора и консоли управления серверами Kaspersky Anti Targeted Attack Platform с определенных компьютеров с помощью утилиты командной строки iptables. Подробнее о работе с iptables см. документацию к iptables.

Чтобы начать работу в меню администратора компонента в консоли управления сервером с нужным компонентом:

1. Войдите в консоль управления того сервера, параметры которого вы хотите изменить, по протоколу SSH или через терминал.

   Отобразится меню администратора компонента приложения.

2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке приложения.

   Отобразится меню администратора компонента приложения.

Вы можете начать работу в меню администратора компонента приложения.

Начало работы с приложением в режиме Technical Support Mode

Любые действия в режиме технической поддержки, не согласованные и / или не рекомендованные специалистами технической поддержки, запрещены и являются основанием для отказа в технической поддержке.

Вы можете работать с компонентами приложения Sensor, Central Node и Sandbox в режиме Technical Support Mode.

Режим Technical Support Mode предоставляет администратору Kaspersky Anti Targeted Attack Platform неограниченные права (root) доступа к приложению и всем данным (в том числе персональным), которые в нем хранятся.

Работа с Kaspersky Anti Targeted Attack Platform из консоли управления в режиме Technical Support Mode с правами учетной записи суперпользователя позволяет выполнять следующие действия:

- Управлять параметрами работы приложения с помощью конфигурационных файлов.

  При этом могут быть изменены параметры шифрования данных при передаче между узлами приложения, параметры хранения и обработки объектов проверки.

  В этом случае данные передаются в открытом виде. Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность серверов с этими данными самостоятельно. Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за изменение конфигурационных файлов приложения.

- Управлять параметрами журнала трассировки.

  Файлы трассировки могут содержать конфиденциальные данные пользователя. Такие файлы хранятся бессрочно и могут быть удалены администратором Kaspersky Anti Targeted Attack Platform вручную. Путь к папке для записи файлов трассировки указывает администратор Kaspersky Anti Targeted Attack Platform.

Чтобы начать работу с компонентами Central Node, Sensor или Sandbox в режиме Technical Support Mode:

1. Войдите в консоль управления того сервера, параметры которого вы хотите изменить, по протоколу SSH или через терминал.

2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке компонента.

   Отобразится меню администратора компонента приложения.

3. В меню администратора приложения выберите режим **Technical Support Mode**.

4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.

Вы можете начать работу с компонентами Central Node, Sensor или Sandbox в режиме Technical Support Mode.

Управление учетными записями администраторов и пользователей приложения

В Kaspersky Anti Targeted Attack Platform предусмотрены учетные записи для серверов со следующими компонентами:

- Sensor. Учетная запись администратора для работы в веб-интерфейсе компонента, меню администратора и в консоли управления сервером (в режиме Technical Support Mode).

  По умолчанию используется учетная запись admin, созданная при установке компонента.

- Sandbox. Учетная запись администратора для работы в веб-интерфейсе компонента, меню администратора и в консоли управления сервером (в режиме Technical Support Mode).

  По умолчанию используется учетная запись admin, созданная при установке компонента.

- Central Node. Следующие учетные записи:

  - Учетная запись администратора для работы в меню администратора приложения и в консоли управления сервером (в режиме Technical Support Mode).

    По умолчанию используется учетная запись admin, созданная при установке компонента.

  - Учетная запись администратора веб-интерфейса приложения.

  - Учетные записи пользователей веб-интерфейса приложения с ролями **Аудитор**, **Сотрудник службы безопасности** и **Старший сотрудник службы безопасности**.

Данные каждой из этих учетных записей хранятся на том сервере с компонентом приложения, к которому она относится.

В режиме распределенного решения и мультитенантности данные каждой из этих учетных записей хранятся на PCN и на том сервере с компонентом приложения, к которому она относится.

Учетная запись администратора для работы в консоли управления сервером обладает неограниченными правами на управление сервером с компонентом приложения, к которому она относится (правами суперпользователя). Под этой учетной записью вы можете выключить или перезагрузить сервер, а также изменить параметры приложения в режиме Technical Support Mode в консоли управления сервером.

Учетная запись администратора для работы в консоли управления сервером (admin) имеет неограниченный доступ к данным на этом сервере. Пароль учетной записи администратора для работы в консоли управления сервером должен быть надежным. Администратору требуется обеспечить безопасность серверов самостоятельно. Администратор несет ответственность за доступ к данным, хранящимся на серверах.

Под учетной записью с ролью **Администратор** вы можете управлять параметрами приложения, доступными администраторам веб-интерфейса приложения, а также учетными записями пользователей приложения. В режиме распределенного решения и мультитенантности управление учетными записями пользователей осуществляется на PCN.

Под учетной записью с ролью **Аудитор** вы можете просматривать все разделы веб-интерфейса, доступные администраторам и сотрудникам службы безопасности. Пользователь с ролью **Аудитор** может просматривать данные без возможности редактирования.

Роли **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** предназначены для сотрудников вашей организации, в чьи обязанности входит работа с событиями, алертами, задачами Kaspersky Anti Targeted Attack Platform и управление действиями по реагированию. При входе в приложение под учетными записями с этими ролями отображаются разделы веб-интерфейса приложения, доступные сотрудникам службы безопасности. Пользователи с ролью **Старший сотрудник службы безопасности** доступны все операции. Ограничения доступа для пользователей с ролями **Сотрудник службы безопасности** представлены в таблице ниже.

Ограничения доступа для пользователей приложения с ролью **Сотрудник службы безопасности**

Функциональная область / Раздел веб-интерфейса	Ограничения
Мониторинг	Недоступны виджеты событий группы VIP. Нет возможности перейти по ссылке на виджет в раздел **Алерты**.
Алерты	Недоступны следующие действия: • просмотр информации об алерте; • отметка о завершении обработки алерта группы VIP; • операции над несколькими алертами; • экспорт списка всех алертов.
Активы: **Устройства**	Недоступна группировка устройств.
Активы: **Endpoint Agents**	Доступ к просмотру таблицы рабочих станций с Endpoint Agent, ограничения по просмотру данных о задачах, политиках и сетевой изоляции.
События в трафике сети	Недоступны операции с событиями, которые связаны с алертами группы VIP.
Поиск угроз	Недоступны следующие действия: • просмотр событий, которые относятся к рабочим станциям из алертов группы VIP; • создание правил TAA (IOA) на основе условий поиска событий.
Задачи	Нет доступа.
Правила запрета	Нет доступа.
Пользовательские правила: IOC	Доступ на чтение.
Пользовательские правила: YARA	Доступ только на экспорт правил.
Пользовательские правила: TAA	Доступ на чтение.
Пользовательские правила Sandbox и правила обнаружения вторжений	Нет доступа.
Журналы	Нет доступа к журналу аудита и журналу активности пользователей в веб-интерфейсе приложения.
Хранилище	Нет доступа к объектам, помещенным в Хранилище в результате выполнения задач. Полный доступ к объектам, загруженным пользователем вручную.
Карантин	Нет доступа.
Отчеты	Нет доступа.
Параметры	Недоступны следующие действия: • создание правил уведомления об алертах (полный доступ к правилам для отправки уведомлений о проблемах в работе приложения); • управление исключениями из правил TAA (IOA) "Лаборатории Касперского" и исключениями из проверки (доступ на чтение). Нет доступа к следующим функциям: • управление компонентом Endpoint Agent; • параметры подключения к локальной репутационной базе KPSN; • правила присвоения VIP-статуса алертам; • разрешающие правила; • параметры подключения Sandbox; • параметры операционных систем для проверки объектов в Sandbox; • пароли для архивов.

Если вы используете режим распределенного решения и мультитенантности, то для каждой учетной записи вы можете разрешить или запретить доступ к тенантам и веб-интерфейсу сервера SCN.

Создание учетной записи администратора веб-интерфейса приложения

Чтобы создать учетную запись администратора веб-интерфейса приложения:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новый пользователь**.
4. Если вы хотите включить учетную запись, включите переключатель **Состояние**.

   По умолчанию учетная запись включена.

   > Если учетная запись включена, доступ к веб-интерфейсу приложения разрешен. Если учетная запись отключена, доступ к веб-интерфейсу приложения запрещен.
5. В раскрывающемся списке **Роль** выберите **Администратор**.
6. В блоке параметров **Тип аутентификации** выберите один из вариантов:

   - **Учетная запись KATA**.

     В этом случае для подключения к веб-интерфейсу приложения пользователю потребуется ввести имя пользователя и пароль, которые были указаны при создании учетной записи.
   - **Доменная учетная запись**.

     В этом случае для подключения к веб-интерфейсу приложения пользователю не требуется вводить имя пользователя и пароль: аутентификация осуществляется с помощью доменной учетной записи пользователя.

   > Блок параметров **Тип аутентификации** отображается, если настроена интеграция с Active Directory.
7. Если вы выбрали **Учетная запись KATA**, выполните следующие действия:

   a. В поле **Имя пользователя** введите имя пользователя, учетную запись которого вы хотите создать.

      Имя пользователя должно удовлетворять следующим требованиям:

      - должно быть уникальным в списке имен пользователей (регистр имеет значение);
      - должно содержать максимум 32 символа;
      - может содержать буквы A–Z, a–z, цифры 0–9, дефис (-) или символ подчеркивания (_);
      - должно начинаться с буквы (A–Z или a–z).

b. В поле **Новый пароль** введите пароль доступа пользователя к веб-интерфейсу.

Пароль должен удовлетворять следующим требованиям:

- не должен полностью или в значительной части совпадать с именем пользователя;
- не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
- должен содержать минимум 8 символов;
- должен содержать символы минимум трех типов:
  - символ верхнего регистра (A–Z);
  - символ нижнего регистра (a–z);
  - цифру;
  - специальный символ.

По мере ввода пароля приложение предварительно проверяет этот пароль на соответствие основным требованиям. Окончательная проверка выполняется после нажатия на кнопку **Добавить**. Даже если предварительная проверка показала, что пароль соответствует требованиям, в результате окончательной проверки пароль может быть отклонен, и в веб-интерфейсе приложения отобразится сообщение об ошибке. В этом случае вам нужно придумать другой пароль с учетом информации об ошибке.

c. В поле **Подтвердите пароль** повторно введите пароль доступа пользователя к веб-интерфейсу.

8. Если вы выбрали **Доменная учетная запись**, в поле **Имя пользователя** укажите доменное имя пользователя.

9. Нажмите на кнопку **Добавить**.

Учетная запись администратора приложения будет создана.

Если вы используете режим распределенного решения и мультитенантности, учетная запись администратора сервера PCN имеет доступ к данным всех тенантов, связанных с этим сервером.

Создание учетной записи пользователя веб-интерфейса приложения

Вы можете создавать учетные записи пользователей с ролями **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** и **Аудитор**.

Чтобы создать учетную запись пользователя веб-интерфейса приложения:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.

2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.

3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новый пользователь**.

4. При необходимости с помощью переключателя **Состояние** отключите учетную запись пользователя.

   По умолчанию учетная запись включена.

   Если учетная запись включена, доступ к веб-интерфейсу приложения разрешен. Если учетная запись отключена, доступ к веб-интерфейсу приложения запрещен.

5. В блоке параметров **Тип аутентификации** выберите один из вариантов:

   - **Учетная запись KATA**.

     В этом случае для подключения к веб-интерфейсу приложения пользователю потребуется ввести имя пользователя и пароль, которые были указаны при создании учетной записи.

   - **Доменная учетная запись**.

     В этом случае для подключения к веб-интерфейсу приложения пользователю не требуется вводить имя пользователя и пароль: аутентификация осуществляется с помощью доменной учетной записи пользователя.

     Если вы выбрали тип аутентификации **Доменная учетная запись**, требуется учитывать, что пользователь не сможет войти в веб-интерфейс приложения под другой учетной записью.

   Поля **Учетная запись KATA** и **Доменная учетная запись** доступны, если настроена интеграция с Active Directory.

6. В раскрывающемся списке **Роль** выберите одну из следующих ролей:

   - **Старший сотрудник службы безопасности**.
   - **Сотрудник службы безопасности**.
   - **Аудитор**.

7. Если вы выбрали **Учетная запись KATA**, выполните следующие действия:

   a. В поле **Имя пользователя** введите имя пользователя, учетную запись которого вы хотите создать.

      Имя пользователя должно удовлетворять следующим требованиям:

      - должно быть уникальным в списке имен пользователей (регистр имеет значение);
      - должно содержать максимум 32 символа;
      - может содержать буквы A–Z, a–z, цифры 0–9, дефис (-) или символ подчеркивания (_);
      - должно начинаться с буквы (A–Z или a–z).

   b. В поле **Новый пароль** введите пароль доступа пользователя к веб-интерфейсу.

Пароль должен удовлетворять следующим требованиям:

- не должен полностью или в значительной части совпадать с именем пользователя;
- не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
- должен содержать минимум 8 символов;
- должен содержать символы минимум трех типов:
  - символ верхнего регистра (A–Z);
  - символ нижнего регистра (a–z);
  - цифру;
  - специальный символ.

По мере ввода пароля приложение предварительно проверяет этот пароль на соответствие основным требованиям. Окончательная проверка выполняется после нажатия на кнопку **Добавить**. Даже если предварительная проверка показала, что пароль соответствует требованиям, в результате окончательной проверки пароль может быть отклонен, и в веб-интерфейсе приложения отобразится сообщение об ошибке. В этом случае вам нужно придумать другой пароль с учетом информации об ошибке.

c. В поле **Подтвердите пароль** повторно введите пароль доступа пользователя к веб-интерфейсу.

8. Если вы выбрали **Доменная учетная запись**, в поле **Имя пользователя** укажите доменное имя пользователя.

9. Если вы используете режим распределенного решения и мультитенантности, в разделе **Доступ** настройте права доступа:

   a. С помощью переключателя включите параметр **Веб-интерфейс SCN**, если вы хотите предоставить пользователю доступ не только к веб-интерфейсу этого сервера PCN, но и к веб-интерфейсам всех доступных серверов SCN.

   b. Справа от названия параметра **Тенанты** установите флажки рядом с названиями одного или нескольких тенантов, к веб-интерфейсам серверов которых вы хотите предоставить доступ.

   Вы можете использовать ссылки **Выбрать все** и **Отменить выбор** для выбора или отмены выбора всех тенантов.

10. Нажмите на кнопку **Добавить**.

Учетная запись будет создана.

Настройка отображения таблицы учетных записей

Вы можете настроить отображение столбцов, а также порядок их следования в таблице учетных записей пользователей веб-интерфейса приложения.

Чтобы настроить отображение таблицы учетных записей пользователей веб-интерфейса приложения:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.
3. В заголовочной части таблицы нажмите на кнопку  .

   Отобразится окно **Настройка таблицы**.
4. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.
5. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку  и переместите строку с параметром в нужное место.
6. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.
7. Нажмите на кнопку **Применить**.

Отображение таблицы учетных записей пользователей будет настроено.

Просмотр таблицы учетных записей

Таблица учетных записей отображается в разделе **Параметры**, подразделе **Пользователи** окна веб-интерфейса приложения. Вы можете сортировать события в таблице по столбцам **Имя пользователя**, **Роль**, **Тенанты** и **Состояние**.

В таблице содержится следующая информация:

1. **Имя пользователя** – имя пользователя, заданное при создании учетной записи.
2. **Тип аутентификации** – тип аутентификации пользователя. Может иметь следующие значения:

   - **Учетная запись KATA**.

     Если выбран этот тип аутентификации, для подключения к веб-интерфейсу приложения пользователю потребуется ввести имя пользователя и пароль, которые были указаны при создании учетной записи.
   - **Доменная учетная запись**.

     Если выбран этот тип аутентификации, для подключения к веб-интерфейсу приложения пользователю не требуется вводить имя пользователя и пароль: аутентификация осуществляется с помощью доменной учетной записи пользователя.
3. **Роль** – роль, назначенная пользователю.
4. **Тенанты** – тенанты, к которым пользователь имеет доступ.

   Столбец отображается только в режиме распределенного решения и мультитенантности.

5. **Состояние** – статус учетной записи. может иметь следующие значения:

   - **Включено**.

     Если учетная запись включена, доступ к веб-интерфейсу приложения разрешен.

   - **Выключено**.

     Если учетная запись отключена, доступ к веб-интерфейсу приложения запрещен.

Фильтрация учетных записей

Чтобы отфильтровать или найти учетные записи пользователей по требуемым критериям:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.
3. Выполните следующие действия в зависимости от критерия фильтрации:

   - **По имени пользователя**

     a. По ссылке **Имя пользователя** откройте меню фильтрации.

     b. В раскрывающемся списке выберите один из следующих операторов фильтрации:

        - **Содержит**.
        - **Не содержит**.

     c. В поле ввода введите имя пользователя или несколько символов из имени пользователя.

     d. Нажмите на кнопку **Применить**.

   - **По типу аутентификации**

     a. По ссылке **Тип аутентификации** откройте меню фильтрации.

     b. Установите флажок напротив типа учетной записи, которую вы хотите включить в критерии фильтрации:

        - **Учетная запись KATA**.
        - **Доменная учетная запись**.

     c. Нажмите на кнопку **Применить**.

- **По роли**

  a. По ссылке **Роль** откройте меню фильтрации.

  b. Установите флажки напротив тех ролей, которые вы хотите включить в критерии фильтрации:

  - **Администратор**.
  - **Старший сотрудник службы безопасности**.
  - **Сотрудник службы безопасности**.
  - **Аудитор**.

  Вы можете установить несколько флажков.

  c. Нажмите на кнопку **Применить**.

- **По названию тенантов, к которым у пользователя есть доступ**

  a. По ссылке **Тенанты** откройте меню фильтрации.

  b. Установите флажки напротив тенантов, которые вы хотите включить в критерии фильтрации.
  Вы можете установить несколько флажков.

  c. Нажмите на кнопку **Применить**.

- **По состоянию**

  a. По ссылке **Состояние** раскройте список настройки фильтрации.

  b. Выберите один из следующих вариантов:

  - **Все**.
  - **Включено**.
  - **Выключено**.

В таблице отобразятся учетные записи, соответствующие заданным критериям фильтрации.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра учетных записей

Чтобы сбросить фильтр учетных записей по одному или нескольким условиям фильтрации:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.

3. Нажмите на кнопку справа от того заголовка столбца таблицы учетных записей, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только учетные записи, соответствующие заданным условиям.

Изменение прав доступа учетной записи к данным PCN и SCN

Если вы используете режим распределенного решения и мультитенантности, вы можете изменить права доступа пользователей с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** к данным серверов PCN и SCN, а также тенантов, связанных с этими серверами.

Чтобы изменить права доступа учетной записи пользователя веб-интерфейса приложения, выполните следующие действия в веб-интерфейсе PCN:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.
3. Выберите учетную запись, права доступа которой вы хотите изменить.

   Откроется окно **Изменить учетную запись**.
4. Если вы хотите включить или отключить учетную запись, измените положение переключателя **Состояние**.
5. Если нужно, в разделе **Доступ** измените положение переключателя **Веб-интерфейс SCN**:

   - Переведите переключатель в положение **Включено**, если вы хотите предоставить пользователю доступ не только к веб-интерфейсу этого сервера PCN, но и к веб-интерфейсам всех доступных серверов SCN.
   - Переведите переключатель в положение **Выключено**, если вы хотите предоставить пользователю доступ только к веб-интерфейсу этого сервера PCN.
6. Справа от названия параметра **Тенанты** установите или снимите флажки рядом с названиями тенантов, к веб-интерфейсам серверов которых вы хотите изменить доступ.

   Вы можете использовать ссылки **Выбрать все** и **Отменить выбор** для выбора или отмены выбора всех тенантов.
7. Нажмите на кнопку **Сохранить**.

Права доступа учетной записи будут изменены.

Включение и отключение учетной записи

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнить шаги этой инструкции в веб-интерфейсе PCN. Управление состоянием учетной записи в веб-интерфейсе SCN недоступно.

Чтобы включить или отключить учетную запись:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.
3. В списке учетных записей выберите учетную запись пользователя, которую вы хотите включить или отключить.
4. Выполните одно из следующих действий в столбце **Состояние**:
   - Переместите переключатель рядом с именем учетной записи в положение **Включено**, если вы хотите включить учетную запись.
   - Переместите переключатель рядом с именем учетной записи в положение **Выключено**, если вы хотите отключить учетную запись.

   Отобразится окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Состояние учетной записи будет изменено.

Отключение учетной записи администратора с именем admin недоступно.

Изменение пароля учетной записи

Изменение пароля учетной записи доступно только для пользователей с типом аутентификации **Учетная запись KATA**.

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнить шаги этой инструкции в веб-интерфейсе PCN. В веб-интерфейсе SCN доступно только изменение пароля своей учетной записи.

Чтобы изменить пароль учетной записи:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**. В списке учетных записей выберите учетную запись, пароль которой вы хотите изменить.

   Откроется окно **Изменить учетную запись**.
3. В поле **Новый пароль** введите новый пароль доступа к веб-интерфейсу приложения.

   Пароль должен удовлетворять следующим требованиям:

   - не должен полностью или в значительной части совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A–Z);
     - символ нижнего регистра (a–z);
     - цифру;
     - специальный символ.

   По мере ввода пароля приложение предварительно проверяет этот пароль на соответствие основным требованиям. Окончательная проверка выполняется после нажатия на кнопку **Добавить**. Даже если предварительная проверка показала, что пароль соответствует требованиям, в результате окончательной проверки пароль может быть отклонен, и в веб-интерфейсе приложения отобразится сообщение об ошибке. В этом случае вам нужно придумать другой пароль с учетом информации об ошибке.
4. В поле **Подтвердите пароль** повторно введите новый пароль.
5. Нажмите на кнопку **Сохранить**.

Пароль учетной записи администратора или пользователя приложения будет изменен.

Изменение пароля своей учетной записи

Изменение пароля учетной записи доступно только для пользователей с типом аутентификации **Учетная запись KATA**.

Чтобы изменить пароль своей учетной записи:

1. Войдите в веб-интерфейс под своей учетной записью.
2. Нажмите на ссылку с именем вашей учетной записи в левой нижней части окна веб-интерфейса приложения.

3. Выберите действие **Изменить пароль**.

   Откроется окно **Изменить пароль**.

4. В поле **Старый пароль** введите текущий пароль доступа к веб-интерфейсу приложения.

5. В поле **Новый пароль** введите новый пароль доступа к веб-интерфейсу приложения.

   Пароль должен удовлетворять следующим требованиям:

   - не должен полностью или в значительной части совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A–Z);
     - символ нижнего регистра (a–z);
     - цифру;
     - специальный символ.

   По мере ввода пароля приложение предварительно проверяет этот пароль на соответствие основным требованиям. Окончательная проверка выполняется после нажатия на кнопку **Добавить**. Даже если предварительная проверка показала, что пароль соответствует требованиям, в результате окончательной проверки пароль может быть отклонен, и в веб-интерфейсе приложения отобразится сообщение об ошибке. В этом случае вам нужно придумать другой пароль с учетом информации об ошибке.

6. В поле **Подтвердите пароль** повторно введите новый пароль.

7. Нажмите на кнопку **Изменить пароль**.

Пароль доступа к веб-интерфейсу приложения вашей учетной записи будет изменен.

Аутентификация с помощью доменных учетных записей

Если аутентификация с помощью доменных учетных записей настроена, пользователям не требуется вводить данные учетной записи Kaspersky Anti Targeted Attack Platform для подключения к веб-интерфейсу приложения.

Для включения аутентификации с помощью доменных учетных записей вам требуется:

1. Настроить интеграцию с Active Directory.

   Для настройки интеграции с Active Directory требуется создать keytab-файл, содержащий имя субъекта-службы (далее также "SPN") для сервера Central Node, на котором выполняется настройка интеграции.

2. Выбрать для пользователя тип аутентификации **Доменная учетная запись** при создании учетной записи.

Создание keytab-файла

Kaspersky Anti Targeted Attack Platform поддерживает два способа аутентификации: одна часть пользователей может использовать для аутентификации внутреннюю учетную запись, другая часть пользователей может использовать доменную учетную запись.

Подробную информацию о доменной аутентификации в Kaspersky Anti Targeted Attack Platform см. в разделе Аутентификация с помощью доменных учетных записей.

Вы можете использовать одну учетную запись Active Directory для аутентификации на нескольких Central Node. Для этого требуется создать keytab-файл, содержащий *имена субъекта-службы (далее также "SPN")* для каждого из этих серверов. При создании keytab-файла потребуется использовать атрибут для генерации *соли* (salt, модификатор входа хеш-функции).

> Сгенерированную соль необходимо сохранить любым удобным способом для дальнейшего добавления новых SPN в keytab-файл.

Вы также можете создать отдельную учетную запись Active Directory для каждого сервера Central Node, для которого вы хотите настроить Kerberos-аутентификацию.

Создание keytab-файла для аутентификации на нескольких Central Node под одной учетной записью

Чтобы создать keytab-файла для аутентификации на нескольких Central Node под одной учетной записью:

1. На сервере контроллера домена в оснастке **Active Directory Users and Computers** создайте учетную запись пользователя (например, с именем `control-user`).

   При создании учетной записи вы можете установить флажок **Password never expires**. Опция позволяет задать неограниченный срок действия пароля для учетной записи и тем самым избежать ошибок аутентификации после его истечения, так как криптографические ключи, сформированные на основе пароля и сохраненные в keytab-файле, также станут недействительными.

2. Если вы хотите задать неограниченный срок действия пароля для уже существующей учетной записи, то в оснастке **Active Directory Users and Computers** выполните следующие действия:

   a. Откройте свойства созданной учетной записи.

   b. На закладке **Account** установите флажок **Password never expires**.

3. Если вы хотите использовать алгоритм шифрования AES256-SHA1, то в оснастке **Active Directory Users and Computers** выполните следующие действия:

   a. Откройте свойства созданной учетной записи.

   b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.

4. Создайте keytab-файл для пользователя `control-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) сервера Central Node>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <путь к файлу>\<имя файла>.keytab
   ```

   Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

   В созданный keytab-файл будет добавлено SPN выбранного сервера. На экране отобразится сгенерированная соль: `Hashing password with salt "<хеш-значение>".`

5. Добавьте в keytab-файл запись SPN для каждого следующего сервера Central Node. Для этого выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) сервера Central Node>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab -setupn -setpass -rawsalt "<хеш-значение соли, полученное при создании keytab-файла на шаге 3>"
   ```

   Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

Keytab-файл будет создан. Этот файл будет содержать все добавленные SPN выбранных серверов.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 серверов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN сервера, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out C:\keytabs\filename1.keytab
```

Допустим, вы получили соль `"TEST.LOCALHTTPcontrol-01.test.local"`.

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab -setupn -setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab -setupn -setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

Создание keytab-файла для аутентификации на каждом Central Node под отдельной учетной записью

Чтобы создать keytab-файл для аутентификации на каждом Central Node под отдельной учетной записью:

1. На сервере контроллера домена в оснастке **Active Directory Users and Computers** создайте отдельную учетную запись пользователя для каждого сервера (например, учетные записи с именами `control-user`, `secondary1-user`, `secondary2-user` и т.д.).

   При создании учетной записи вы можете установить флажок **Password never expires**. Опция позволяет задать неограниченный срок действия пароля для учетной записи и тем самым избежать ошибок аутентификации после его истечения, так как криптографические ключи, сформированные на основе пароля и сохраненные в keytab-файле, также станут недействительными.

2. Если вы хотите задать неограниченный срок действия пароля для уже существующей учетной записи, то в оснастке **Active Directory Users and Computers** выполните следующие действия:

   a. Откройте свойства созданной учетной записи.

   b. На закладке **Account** установите флажок **Password never expires**.

3. Если вы хотите использовать алгоритм шифрования AES256-SHA1, то в оснастке **Active Directory Users and Computers** выполните следующие действия:

   a. Откройте свойства созданной учетной записи.

   b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.

4. Создайте keytab-файл для пользователя `control-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) сервера Central Node>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out <путь к файлу>\<имя файла>.keytab
   ```

   Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

В созданный keytab-файл будет добавлено SPN выбранного сервера.

5. Добавьте в keytab-файл запись SPN для каждого следующего сервера Central Node. Для этого выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) сервера Central Node>@<realm имя домена Active Directory в верхнем регистре> -mapuser secondary1-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab
   ```

   Утилита запросит пароль пользователя `secondary1-user` в процессе выполнения команды.

Keytab-файл будет создан. Этот файл будет содержать все добавленные SPN выбранных серверов.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 серверов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN сервера, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\keytabs\filename1.keytab
```

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser secondary1-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser secondary2-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

Настройка интеграции с Active Directory

Подробную информацию о доменной аутентификации в Kaspersky Anti Targeted Attack Platform см. в разделе Аутентификация с помощью доменных учетных записей.

Чтобы настроить интеграцию с Active Directory:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.
3. Перейдите на закладку **Интеграция с Active Directory**.
4. Установите флажок **Интеграция**, если вы хотите включить интеграцию с Active Directory.
5. Нажмите на кнопку **Обзор**, чтобы загрузить keytab-файл.
6. Выберите keytab-файл и нажмите на кнопку **Открыть**.

После загрузки файла отобразятся следующие поля:

- **Статус keytab-файла**. Может принимать следующие значения:
  - **Файл содержит SPN-идентификатор для этого сервера** – в загруженном keytab-файле есть SPN для этого сервера Kaspersky Anti Targeted Attack Platform.
  - **Отсутствует SPN-идентификатор для этого сервера** – в загруженном keytab-файле отсутствует SPN для этого сервера Kaspersky Anti Targeted Attack Platform.
- **Файл содержит** – список SPN, которые содержит файл.

7. Нажмите на кнопку **Применить**.

Интеграция с Active Directory будет настроена.

В режиме распределенного решения и мультитенантности параметры интеграции с Active Directory, заданные на сервере PCN, **не** распространяются на подключенные к нему серверы SCN. Если вы хотите настроить интеграцию с Active Directory на серверах SCN, вам требуется выполнить описанные выше шаги на каждом выбранном сервере SCN.

Отключение интеграции с Active Directory

Подробную информацию о доменной аутентификации в Kaspersky Anti Targeted Attack Platform см. в разделе Аутентификация с помощью доменных учетных записей.

При отключении интеграции с Active Directory аутентификация пользователей с помощью доменных учетных данных будет недоступна.

Чтобы отключить интеграцию с Active Directory:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.
3. Перейдите на закладку **Интеграция с Active Directory**.
4. Снимите флажок **Интеграция**.
5. Нажмите на кнопку **Применить**.

Интеграция с Active Directory будет отключена. Загруженный keytab-файл будет удален без возможности восстановления.

В режиме распределенного решения и мультитенантности настройки интеграции с Active Directory, заданные на сервере PCN, **не** распространяются на подключенные к нему серверы SCN. Если вы хотите отключить интеграцию с Active Directory на отдельных серверах SCN, вам требуется выполнить описанные выше шаги на каждом выбранном сервере SCN.

Участие в Kaspersky Security Network и использование Kaspersky Private Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Anti Targeted Attack Platform использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (далее также "KSN") – это инфраструктура облачных служб, предоставляющая пользователям доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Anti Targeted Attack Platform на объекты, информация о которых еще не вошла в базы антивирусных приложений, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие пользователей в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, данные о которых еще не вошли в базы антивирусных приложений, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний приложения, а также помогает другим пользователям Kaspersky Security Network оперативно получать информацию об угрозах IT-инфраструктуре предприятий.

Когда вы участвуете в Kaspersky Security Network, Kaspersky Anti Targeted Attack Platform отправляет в Kaspersky Security Network запросы о репутации файлов, интернет-ресурсов и программного обеспечения и получает ответ, содержащий данные о репутации этих объектов.

Сбор, обработка и хранение персональных данных пользователя не производится. О данных, которые Kaspersky Anti Targeted Attack Platform передает в Kaspersky Security Network, вы можете прочитать в Положении о KSN.

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается на этапе установки Kaspersky Anti Targeted Attack Platform, его можно изменить в любой момент.

Если вы не хотите участвовать в KSN, вы можете использовать Kaspersky Private Security Network (далее также "KPSN") – решение, позволяющее пользователям получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные со своих компьютеров в Kaspersky Security Network.

По вопросам приобретения приложения Kaspersky Private Security Network вы можете связаться со специалистами компании-партнера "Лаборатории Касперского" в вашем регионе.

Настройка участия в KSN производится на сервере Central Node и распространяется на все подключаемые серверы Sensor.

Если вы используете режим распределенного решения и мультитенантности, настраивайте участие в KSN на сервере PCN. Настройка участия в KSN распространится на все серверы SCN, подключаемые к PCN.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

Просмотр Положения о KSN и настройка участия в KSN

Чтобы настроить участие в Kaspersky Security Network:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. Справа от названия параметра **Репутационная база** нажмите на кнопку **KSN**.
4. Ознакомьтесь с Положением о Kaspersky Security Network и выберите один из следующих вариантов:
   - **Я согласен участвовать в KSN**, если вы согласны с условиями Положения о KSN и хотите участвовать в KSN.
   - **Я не согласен участвовать в KSN**, если вы не согласны с условиями Положения о KSN и не хотите участвовать в KSN.

     Если вы не согласны с условиями Положения, использование Kaspersky Security Network не будет включено.
5. Нажмите на кнопку **Применить**.

Участие в Kaspersky Security Network будет настроено.

Включение использования KPSN

Для корректного соединения с KPSN вам нужно использовать порты, которые указаны для сервиса ksn_proxy в разделе *Порты, используемые сервисами Central Node, установленного на сервере*. При настройке интеграции с KPSN через другие порты попытка соединения завершается ошибкой.

Чтобы включить использование KPSN:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. Справа от названия параметра **Репутационная база** нажмите на кнопку **KPSN**.
4. В блоке **Конфигурационные файлы KPSN** загрузите файлы kc_private.xms, kh_private.xms, ksncli_private.dat с помощью кнопки **Обзор**.
5. Нажмите на кнопку **Применить**.

Использование Kaspersky Private Security Network будет включено.

Настройка подключения к локальной репутационной базе KPSN

Приложение может сохранять информацию об алертах, созданных компонентом Sandbox в локальную репутационную базу KPSN. В этом случае объектам присваивается статус *Недоверенный*. Данные локальных репутационных баз доступны только для компьютеров локальной сети организации.

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить подключение Kaspersky Anti Targeted Attack Platform к локальной репутационной базе KPSN:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **Репутационная база KPSN**.
3. В поле **Хост** укажите IP-адрес сервера KPSN, на котором хранится локальная репутационная база KPSN.
4. Нажмите на кнопку **Обзор** справа от поля **TLS-сертификат**.

   Откроется окно выбора файлов.
5. Выберите файл сертификата для аутентификации пользователей в KPSN и нажмите на кнопку **Открыть**.

6. Нажмите на кнопку **Обзор** справа от поля **TLS-ключ шифрования**.

   Откроется окно выбора файлов.

7. Выберите файл, содержащий закрытый ключ шифрования, и нажмите на кнопку **Открыть**.

Подключение к локальной репутационной базе KPSN будет настроено.

Настройка сохранения информации в локальную репутационную базу KPSN

Приложение может сохранять MD5- и SHA256-хеши объектов, обнаруженных компонентом Sandbox, в локальную репутационную базу KPSN. В этом случае объектам присваивается статус *Недоверенный*. Данные локальных репутационных баз доступны только для компьютеров локальной сети организации.

Чтобы настроить сохранение информации об объектах, обнаруженных компонентом Sandbox, в локальную репутационную базу KPSN:

1. Войдите в веб-интерфейс приложения под учетной записью старшего сотрудника службы безопасности.
2. Выберите раздел **Параметры**, подраздел **Репутационная база KPSN**.
3. Выполните одно из следующих действий:

   - Включите переключатель **Присваивать объектам статус "Недоверенный"**, если вы хотите, чтобы приложение присваивало объектам статус *Недоверенный* и сохраняло информацию о них в локальную репутационную базу KPSN.
   - Выключите переключатель **Присваивать объектам статус "Недоверенный"**, если вы не хотите сохранять информацию об обнаруженных объектах в локальную репутационную базу KPSN.

4. Нажмите на кнопку **Сохранить**.

Настройка сохранения информации в локальную репутационную базу KPSN будет выполнена.

Отказ от участия в KSN и использования KPSN

Чтобы отказаться от участия в Kaspersky Security Network и использования KPSN:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. Справа от названия параметра **Репутационная база** нажмите на кнопку **Не используется**.
4. Нажмите на кнопку **Применить**.

Вы не будете участвовать в KSN и использовать KPSN.

Работа с компонентом Sandbox через веб-интерфейс

Веб-интерфейс Sandbox расположен на сервере с компонентом Sandbox.

Веб-интерфейс Sandbox защищен от **CSRF-атак** и работает только в том случае, если браузер пользователя веб-интерфейса предоставляет заголовок Referrer HTTP-запроса POST. Убедитесь, что браузер, который вы используете для работы с веб-интерфейсом Sandbox, не модифицирует заголовок Referrer HTTP-запроса POST. Если соединение с веб-интерфейсом осуществляется через прокси-сервер вашей организации, проверьте параметры и убедитесь, что прокси-сервер не модифицирует заголовок Referrer HTTP-запроса POST.

Cross-Site Request Forgery (также "XSRF-атака"). Атака на пользователей веб-сайтов, использующая уязвимости HTTP-протокола. Атака позволяет производить действия от имени авторизованного пользователя уязвимого веб-сайта. Например, от имени авторизованного пользователя уязвимого веб-сайта злоумышленник может тайно отправлять запрос на сервер сторонней платежной системы для перевода денег на счет злоумышленника.

Чтобы начать работу в веб-интерфейсе Sandbox:

1. В браузере на любом компьютере, на котором разрешен доступ к серверу с компонентом Sandbox, введите IP-адрес сервера с компонентом Sandbox.

   Откроется окно ввода учетных данных администратора компонента Sandbox.

2. Введите имя пользователя и пароль администратора компонента Sandbox, который вы задали при установке компонента Sandbox.

Вы можете начать работу в веб-интерфейсе Sandbox.

Количество одновременных сеансов работы с Sandbox под одной учетной записью ограничено одним IP-адресом. При попытке входа в Sandbox под этим же именем пользователя с другого IP-адреса, первый сеанс работы с Sandbox завершается.

Если вы используете несколько серверов с компонентом Sandbox, производите настройку параметров каждого компонента Sandbox из веб-интерфейса Sandbox этого сервера.

Обновление баз компонента Sandbox

Базы компонента Sandbox представляют собой файлы с записями, которые позволяют обнаруживать в проверяемых объектах вредоносный код и признаки подозрительного поведения объектов.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, создают для них идентифицирующие записи и включают их в *пакет обновлений баз* (далее также "пакет обновлений"). Пакет обновлений представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента выпуска предыдущего пакета обновлений. Рекомендуется регулярно получать пакеты обновлений.

В течение срока действия лицензии вы можете получать пакеты обновлений автоматически один раз в час или обновлять базы вручную.

Если вы развернули Kaspersky Anti Targeted Attack Platform в изолированной сети или в сети с ограниченной пропускной способностью канала выхода в интернет, вы можете настроить обновление баз компонента с помощью утилиты Kaspersky Update Utility. Sandbox также может получать обновления баз от Central Node, к которому он подключен, если этот Central Node выбран в качестве источника обновлений.

Запуск обновления баз вручную

Чтобы запустить обновление баз вручную:

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.

   В блоке параметров **Последнее обновление** отобразятся время и статус последней попытки обновления баз Sandbox.

2. Нажмите на кнопку **Запустить**.

Выбор источника обновления баз

Чтобы выбрать источник обновления баз:

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.

2. В блоке параметров **Источник обновлений** выберите источник, из которого вы хотите получать пакет обновлений:

   - **Сервер обновлений "Лаборатории Касперского"**.

     Приложение будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTP и загружать актуальные базы.

   - **Сервер обновлений "Лаборатории Касперского" (безопасное подключение)**.

     Приложение будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTPS и загружать актуальные базы. Рекомендуется выполнять обновления баз по протоколу HTTPS.

   - **Другой сервер**.

     Приложение будет подключаться к вашему FTP- или HTTP-серверу или к папке с базами приложения на вашем компьютере и загружать актуальные базы. Вы также можете выбрать в качестве источника обновлений Central Node, к которому подключен Sandbox.

     Обмен данными между вашим HTTP-сервером и Sandbox должен осуществляться по протоколу HTTP. HTTPS в этом случае не поддерживается.

3. Если вы выбрали **Другой сервер**, выполните следующие действия:

   - Если вы хотите указать в качестве источника обновлений FTP- или HTTP-сервер, в поле под названием этого параметра укажите полный путь к папке с пакетом обновлений баз приложения.

   - Если вы хотите указать в качестве источника обновления Central Node, к которому подключен Sandbox, нажмите левой кнопки мыши на требуемый IP-адрес сервера Central Node под полем. В поле отобразится адрес сервера Central Node в формате http://<Central Node IP address>/retranslation.

4. Нажмите на кнопку **Применить** в нижней части окна.

Источник обновления баз будет выбран.

Обновление баз компонента с помощью Kaspersky Update Utility

Если вы развернули Kaspersky Anti Targeted Attack Platform в изолированной сети или в сети с ограниченной пропускной способностью канала выхода в интернет, вы можете настроить обновление баз компонента с помощью утилиты Kaspersky Update Utility. В этом случае пакеты обновлений с помощью утилиты скачиваются на компьютер, который находится вне локальной сети организации, и копируются на ваш FTP- или HTTP-сервер. Sandbox получает пакеты обновлений с этого сервера.

Настройка обновления баз компонента с помощью утилиты состоит из следующих этапов:

1. Скачивание пакетов обновлений с помощью Kaspersky Update Utility.

   Предварительно вам потребуется запросить в Службе технической поддержки "Лаборатории Касперского" дистрибутив утилиты и список серверов для загрузки обновлений.

2. Загрузка пакетов обновлений, полученных с помощью утилиты Kaspersky Update Utility, на ваш FTP- или HTTP-сервер.

3. Выбор вашего FTP- или HTTP-сервера в качестве источника обновления баз.

Скачивание пакетов обновлений с помощью Kaspersky Update Utility

Для выполнения шагов инструкции вам нужно запросить в Службе технической поддержки "Лаборатории Касперского" дистрибутив утилиты и список серверов для загрузки обновлений.

Чтобы установить утилиту Kaspersky Update Utility:

1. Загрузите на компьютер папку с дистрибутивом утилиты.

2. Запустите файл UpdateUtility-Gui.exe.

3. В открывшемся окне нажмите на кнопку **Applications** и установите флажок слева от версии **7.0-7.1**.
4. Нажмите на кнопки **OK** и **Apply**.

Утилита будет установлена. Вы можете скачать пакеты обновлений, выполнив шаги инструкции ниже.

Чтобы скачать пакеты обновлений с помощью Kaspersky Update Utility:

1. В главном окне утилиты нажмите на кнопку **Settings** и выберите **Download**.
2. В блоке параметров **Updates source** выберите **Other** и введите адрес сервера для загрузки обновлений.
3. Нажмите на кнопки **OK** и **Apply**.
4. Нажмите на кнопку **Start**.

Пакеты обновлений будут скачаны на компьютер, где располагается утилита. Файлы будут готовы к загрузке на ваш FTP- или HTTP-сервер.

Включение и отключение использования прокси-сервера для обновления баз

Чтобы включить или отключить использование прокси-сервера для обновления баз компонента Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.
2. В рабочей области выполните одно из следующих действий:
   - Включите переключатель рядом с названием блока параметров **Прокси-сервер**, если вы хотите использовать прокси-сервер при обновлении баз компонента Sandbox.
   - Выключите переключатель рядом с названием блока параметров **Прокси-сервер**, если вы не хотите использовать прокси-сервер при обновлении баз компонента Sandbox.

Настройка параметров соединения с прокси-сервером для обновления баз

Чтобы настроить параметры соединения с прокси-сервером для обновления баз компонента Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.
2. Включите переключатель рядом с названием блока параметров **Прокси-сервер**.
3. В поле **Адрес** введите адрес прокси-сервера.
4. В поле **Порт** укажите номер порта прокси-сервера.
5. В поле **Имя пользователя** введите имя пользователя прокси-сервера.

6. В поле **Пароль** введите пароль подключения к прокси-серверу.

7. Выполните одно из следующих действий:

   - Установите флажок **Не использовать прокси-сервер для локальных адресов**, если вы не хотите использовать прокси-сервер для внутренних IP-адресов вашей организации.

   - Снимите флажок **Не использовать прокси-сервер для локальных адресов**, если вы хотите использовать прокси-сервер независимо от принадлежности IP-адресов к вашей организации.

8. Нажмите на кнопку **Применить** в нижней части окна.

Настройка соединения компонентов Sandbox и Central Node

Предусмотрен следующий порядок настройки соединения Sandbox с Central Node:

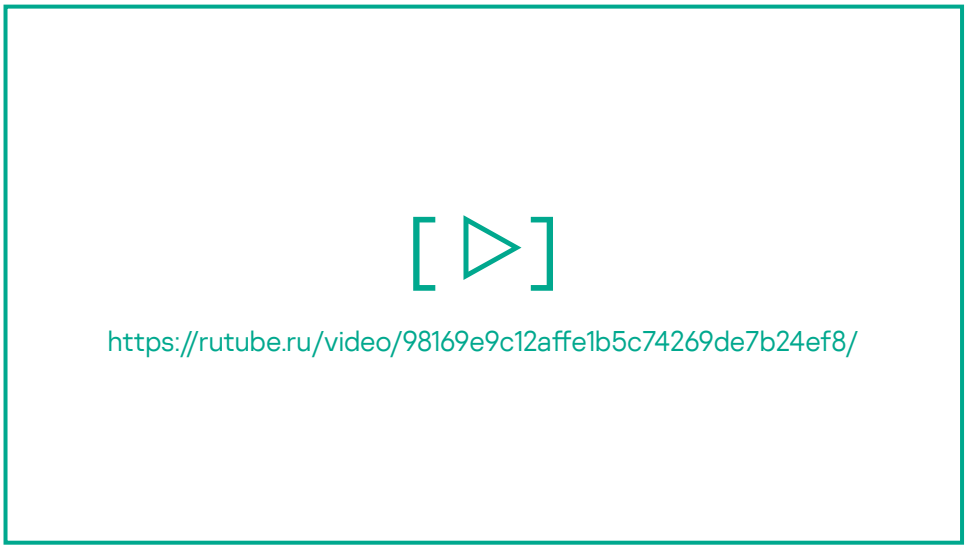
1. В веб-интерфейсе приложения создается запрос на подключение к компоненту Sandbox.

2. В веб-интерфейсе Sandbox отображаются запросы на подключение.

   Вы можете принять или отклонить запрос.

После настройки соединения серверу Sandbox требуется 5–10 минут для подготовки к работе. В течение этого времени в окне **Работоспособность системы** веб-интерфейса приложения отображается предупреждение *Возникла проблема со стандартной конфигурацией*. Когда сервер будет готов к работе, предупреждение исчезнет.

Посмотрите обучающее видео о процессе подключения компонентов Sandbox и Sensor. Для воспроизведения видео вы можете запустить его на странице справки (см. ниже) или перейти по ссылке https://rutube.ru/video/98169e9c12affe1b5c74269de7b24ef8/?playlist=891497.



Процесс подключения компонентов Sandbox и Sensor, проверка работоспособности

Обработка запросов на подключение от серверов Central Node в веб-интерфейсе Sandbox

Вы можете принять, отклонить или отозвать ранее принятый запрос на подключение от серверов Central Node в веб-интерфейсе Sandbox.

Чтобы принять, отклонить или отозвать запрос на подключение от серверов Central Node:

1. В окне веб-интерфейса Sandbox выберите раздел **Авторизация**.

   В разделе **Запросы на подключение от Central Node** отобразится список запросов на подключение от компонентов Central Node.

   В каждом запросе на подключение содержится следующая информация:

   - **IP** – IP-адрес сервера Central Node.
   - **Отпечаток сертификата** – отпечаток TLS-сертификата Central Node, с помощью которого устанавливается шифрованное соединение между серверами.
   - **Состояние** – состояние запроса на подключение.

     Может иметь значения **Ожидание** или **Принят**.

2. Убедитесь, что отпечаток сертификата Central Node соответствует отпечатку сертификата на стороне Central Node.

   Вы можете проверить отпечаток сертификата Central Node в меню администратора сервера Central Node в разделе **Manage server certificate**.

3. Нажмите на одну из следующих кнопок в строке с запросом на подключение от компонента Central Node:

   - **Принять**, если вы хотите принять запрос на подключение.
   - **Отклонить**, если вы хотите отклонить запрос на подключение.
   - **Отозвать**, если вы хотите отозвать ранее принятый запрос на подключение.

4. Нажмите на кнопку **Применить** в нижней части окна.

Настройка сетевых интерфейсов компонента Sandbox

В этом разделе содержится информация о настройке сетевых интерфейсов компонента Sandbox.

Настройка параметров DNS

Чтобы настроить параметры DNS:

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В поле **Имя хоста** введите имя сервера, на который вы устанавливаете компонент Sandbox, в формате FQDN (например, sandbox).
3. Справа от названия параметра **DNS-серверы** нажмите на кнопку **Добавить**.

   Добавится пустое поле ввода IP-адреса DNS-сервера.
4. Введите IP-адрес основного DNS-сервера в формате IPv4.
5. Нажмите на кнопку ✓ справа от поля ввода.

   DNS-сервер будет добавлен.
6. Если вы хотите добавить дополнительный DNS-сервер, повторите действия 2-5.
7. Если вы хотите удалить добавленный DNS-сервер, нажмите на кнопку 🗑 справа от строки с IP-адресом DNS-сервера.

   Вы можете удалить только дополнительные DNS-серверы. Вы не можете удалить основной DNS-сервер. Если вы добавили 2 и более DNS-сервера, вы можете удалить любой из них, при этом оставшийся DNS-сервер будет использоваться в качестве основного.

Настройка параметров управляющего сетевого интерфейса

Управляющий сетевой интерфейс предназначен для доступа к серверу с компонентом Sandbox по протоколу SSH, также через этот интерфейс компонент Sandbox будет принимать объекты от компонента Central Node.

Вы можете настроить управляющий сетевой интерфейс во время установки компонента Sandbox.

Вы также можете настроить управляющий сетевой интерфейс в веб-интерфейсе Sandbox.

Чтобы настроить управляющий сетевой интерфейс в веб-интерфейсе Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Управляющий интерфейс** в раскрывающемся списке **Интерфейс** выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.
3. В поле **IP** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу, если IP-адрес не назначен.
4. В поле **Маска** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. Нажмите на кнопку **Применить** в нижней части окна.

Настройка параметров сетевого интерфейса для доступа обрабатываемых объектов в интернет

Объекты, которые обрабатывает компонент Sandbox, могут предпринимать попытки действий в интернете через сетевой интерфейс для доступа обрабатываемых объектов в интернет. Компонент Sandbox может анализировать поведение этих объектов.

Если вы запретите доступ в интернет, компонент Sandbox не сможет анализировать поведение объектов в интернете, и будет анализировать поведение объектов без доступа в интернет.

Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть изолирован от локальной сети вашей организации.

Если в соответствии с политикой безопасности вашей организации с компьютеров пользователей локальной сети запрещен доступ в интернет, и вы настроили сетевой интерфейс Sandbox для доступа обрабатываемых объектов в интернет, есть риск возникновения следующего сценария:

Злоумышленник может прикрепить вредоносное приложение к произвольному файлу и запустить Sandbox-проверку этого файла с компьютера пользователя локальной сети. Этот файл будет выведен за пределы локальной сети через сетевой интерфейс для доступа обрабатываемых объектов в интернет в процессе проверки файла компонентом Sandbox.

Отсутствие сетевого интерфейса Sandbox для доступа обрабатываемых объектов в интернет исключает риски подобной передачи информации, однако снижает качество обнаружений.

Чтобы настроить сетевой интерфейс для доступа обрабатываемых объектов в интернет:

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Интерфейс для выхода в интернет** в списке **Интерфейс** выберите сетевой интерфейс, который вы хотите использовать для доступа обрабатываемых объектов в интернет.

   Управляющий сетевой интерфейс, который вы настроили ранее, недоступен для выбора в этом списке сетевых интерфейсов.
3. В поле **IP** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.
4. В поле **Маска** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. В поле **Шлюз по умолчанию** введите адрес шлюза сети, в которой вы хотите использовать этот сетевой интерфейс.
6. Нажмите на кнопку **Применить** в нижней части окна.

Добавление, изменение и удаление статических сетевых маршрутов

Вы можете настроить статические сетевые маршруты во время установки компонента Sandbox.

Вы также можете добавить, удалить или изменить статические сетевые маршруты в веб-интерфейсе Sandbox.

Чтобы добавить статический сетевой маршрут:

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** нажмите на кнопку **Добавить**.

   В списке статических сетевых маршрутов добавится строка с пустыми полями.
3. В поле **IP** введите IP-адрес сервера, для которого вы хотите настроить статический сетевой маршрут.
4. В поле **Маска** введите маску подсети.
5. В поле **Шлюз** введите IP-адрес шлюза.
6. В списке **Интерфейс** выберите сетевой интерфейс, для которого вы хотите добавить статический сетевой маршрут.
7. Нажмите на кнопку ✓.
8. Нажмите на кнопку **Применить** в нижней части окна.

Чтобы удалить статический сетевой маршрут, выполните следующие действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** в строке со статическим сетевым маршрутом, который вы хотите удалить, нажмите на кнопку 🗑.
3. Нажмите на кнопку **Применить** в нижней части окна.

Чтобы изменить статический сетевой маршрут:

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** в строке со статическим сетевым маршрутом, который вы хотите изменить, нажмите на кнопку ✎.

   Строка статического сетевого маршрута станет доступна для редактирования. Вы можете изменить один или несколько параметров статического сетевого маршрута.
3. В поле **IP** измените IP-адрес сервера, для которого вы хотите настроить статический сетевой маршрут.
4. В поле **Маска** измените маску подсети.
5. В поле **Шлюз** измените IP-адрес шлюза.

6. В списке **Интерфейс** выберите сетевой интерфейс, для которого вы редактируете сетевой маршрут.
7. Нажмите на кнопку ✓.
8. Нажмите на кнопку **Применить** в нижней части окна.

Политики аутентификации на Sandbox

Вы можете настроить политики аутентификации на Sandbox для пользователей Kaspersky Anti Targeted Attack Platform. Действие политик распространяется на всех пользователей Kaspersky Anti Targeted Attack Platform с типом учетной записи **Учетная запись KATA** независимо от назначенной роли.

Завершение неактивных сессий

Если пользователь не выполняет никаких действий (сессия неактивна), рекомендуется завершать такую сессию. Это снижает риск несанкционированного доступа к Kaspersky Anti Targeted Attack Platform, когда пользователь фактически закончил работу с приложением, но его сессия осталась незавершенной.

Информирование о неуспешных попытках аутентификации

Частые неудачные попытки входа в веб-интерфейс или консоль управления могут быть признаком того, что к Kaspersky Anti Targeted Attack Platform пытается получить доступ злоумышленник путем подбора паролей. Для предотвращения несанкционированного доступа в таких случаях рекомендуется включить информирование о превышении заданного ограничения на неуспешные попытки аутентификации.

Завершение неактивных сессий на Sandbox

Если пользователь не выполняет никаких действий (сессия неактивна), рекомендуется завершать такую сессию. Это снижает риск несанкционированного доступа к Kaspersky Anti Targeted Attack Platform, когда пользователь фактически закончил работу с приложением, но его сессия осталась незавершенной.

Чтобы включить и настроить завершение неактивных сессий:

1. В окне веб-интерфейса Sandbox выберите раздел **Политики аутентификации**.
2. В разделе **Завершение неактивных сессий** укажите время, по истечении которого нужно завершать пользовательскую сессию, если пользователь не выполняет никаких действий. Время в минутах введите в поле **Завершать неактивные сессии через**.
3. Нажмите на кнопку **Применить**.

Неактивные пользовательские сессии будут завершаться по истечении указанного интервала времени.

Информирование о неуспешных попытках аутентификации на Sandbox

Частые неудачные попытки входа в веб-интерфейс или консоль управления могут быть признаком того, что к Kaspersky Anti Targeted Attack Platform пытается получить доступ злоумышленник путем подбора паролей. Для предотвращения несанкционированного доступа в таких случаях рекомендуется включить информирование о превышении заданного ограничения на неуспешные попытки аутентификации.

Чтобы включить и настроить информирование о неуспешных попытках аутентификации:

1. В окне веб-интерфейса Sandbox выберите раздел **Политики аутентификации**.

2. В разделе **Подсчет попыток аутентификации** переместите переключатель **Считать попытки** в положение **Включено**.

3. В поле **Период подсчета** введите время, в течение которого должны подсчитываться неуспешные попытки аутентификации. Время указывается в минутах. Если в течение этого времени пользователь неуспешно пытается войти в веб-интерфейс или консоль управления более двух раз подряд, происходит следующее:

   - В журнал активности пользователей вносится запись о неуспешных попытках аутентификации пользователя.

   - Если создано правило отправки уведомлений о превышении количества неудачных попыток аутентификации (см. ниже инструкцию о создании правила), отправляется сообщение электронной почты на адреса, указанные в правиле уведомления. В сообщении содержится информация о неуспешных попытках аутентификации пользователя.

   В поле **Период подсчета** допускается указать `0`, в этом случае подсчитываются все неуспешные попытки аутентификации, вне зависимости от временного интервала между ними.

4. Нажмите на кнопку **Применить**.

   Неуспешные попытки аутентификации будут подсчитываться, при превышении заданного порога (две неуспешные попытки аутентификации подряд) информация об этом будет сохранена и доступна для ознакомления.

Для отправки уведомлений о превышении количества неудачных попыток аутентификации нужно включить и настроить отправку уведомлений в веб-интерфейсе Central Node, к которому подключен Sensor. Если Sensor подключен к нескольким Central Node, настроить отправку уведомлений можно в любом из них.

Чтобы включить и настроить отправку уведомлений о превышении количества неудачных попыток аутентификации,

Следуйте инструкции по созданию правила для отправки уведомлений о работе компонентов приложения. В процессе создания правила в блоке параметров **Компоненты** установите флажок **Попытки авторизации**.

На адреса электронной почты, указанные в правиле уведомления, будет отправляться сообщение с информацией о неуспешных попытках аутентификации пользователя, если таких попыток более двух подряд за заданный интервал времени (см. выше параметр **Период подсчета**).

Установка даты и времени системы Sandbox

Чтобы установить дату и время сервера с компонентом Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Дата и время**.
2. В раскрывающемся списке **Часовой пояс** выберите нужный часовой пояс.
3. Если вы хотите синхронизировать время с NTP-сервером, включите переключатель справа от названия параметра **Синхронизация с NTP-серверами**.
4. Если вы хотите установить дату и время вручную, не включайте переключатель справа от названия параметра **Синхронизация с NTP-серверами** и выполните следующие действия:
   a. В поле **Дата** введите текущую дату или нажмите на кнопку 🗓 и выберите дату в календаре.
   b. В поле **Время** введите текущее время.
5. Нажмите на кнопку **Применить** в нижней части окна.

Подготовка виртуальных машин к работе

Sandbox использует виртуальные машины для запуска объектов в различных операционных системах с целью анализа поведения объектов и обнаружения их вредоносной активности.

Вы можете устанавливать виртуальные машины двух типов:

- Преднастроенные. Это виртуальные машины на основе образов операционных систем (файлы с расширением ISO) из дистрибутива. Эти образы или установленные на них приложения недоступны для изменения.

  > Вам потребуется активировать некоторые операционные системы и приложения. Активация производится с помощью ваших лицензий.

- Пользовательские. Это виртуальные машины на основе выбранных вами операционных систем. На эти операционные системы можно устанавливать любые приложения для имитации реалистичной рабочей среды.

  Пользовательские операционные системы должны быть настроены в соответствии с инструкциями, приведенными в разделе *Настройка операционной системы и программного обеспечения*. Для проверки объектов в этих операционных системах необходимо создать пользовательские правила Sandbox.

Вы можете использовать пользовательские и преднастроенные образы операционных систем одновременно.

Мы настоятельно рекомендуем на каждом сервере Sandbox использовать все доступные преднастроенные образы операционных систем из комплекта поставки. Если используется только часть образов из комплекта поставки или только пользовательские образы, качество проверки объектов может снизиться.

Создание преднастроенных виртуальных машин на основе образов операционных систем из комплекта поставки

Процесс создания виртуальных машин на основе образов операционных систем из комплекта поставки состоит из следующих этапов:

1. Импорт шаблона.
2. Создание виртуальной машины.
3. Установка виртуальной машины.

Создание пользовательских виртуальных машин на основе своих образов операционных систем

Процесс создания виртуальных машин на основе своих образов операционных систем состоит из следующих этапов:

1. Загрузка в Хранилище Sandbox образа операционной системы и приложений, которые вы хотите установить в этой операционной системе.

   Вы можете пропустить этот шаг и загрузить образы в процессе создания и редактирования шаблона.

2. Создание или импорт пользовательского шаблона.
3. Настройка операционной системы согласно инструкциям, приведенным в разделе *Настройка операционной системы и программного обеспечения*, если она не была настроена ранее. Настройка выполняется при редактировании шаблона.
4. Создание виртуальной машины.
5. Установка виртуальной машины.

Если вы столкнулись с проблемами при работе с установленными виртуальными машинами, вы можете обратиться к Базе знаний Технической поддержки "Лаборатории Касперского".

При возникновении проблем с активацией преднастроенных операционных систем или приложений в веб-интерфейсе компонента Sandbox отобразится сообщение об ошибке. В этом случае рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Работа с образами операционных систем и приложений в Хранилище Sandbox

В Хранилище Sandbox помещаются пользовательские образы операционных систем и приложений, которые вы хотите установить в этих операционных системах.

Мы настоятельно рекомендуем использовать оригинальные ISO-образы от Microsoft.

Вы можете загрузить в Хранилище следующие пользовательские образы операционных систем:

- Windows XP SP3 и выше.
- Windows 7.
- Windows 8.1 64-разрядная.
- Windows 10 64-разрядная (до версии 1909).

Загружаемые файлы должны иметь расширение .ISO.

Загрузка пользовательских образов серверных операционных систем семейства Windows и любых операционных систем семейства Linux не поддерживается.

Если вы хотите использовать в шаблоне пользовательские образы операционных систем, вам нужно настроить эти операционные системы.

Просмотр таблицы образов операционных систем и приложений в Хранилище Sandbox

Чтобы просмотреть таблицу образов операционных систем и приложений в Хранилище Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Хранилище**.

   Отобразится таблица образов операционных систем и приложений в Хранилище Sandbox.

В таблице содержится следующая информация:

- **Загружено** – время загрузки образа.
- **Имя** – имя образа.

- **Размер** – размер образа.
- **Действия** – доступные для образа операции. Возможные значения: **Создать VM**, **Экспортировать**, **Удалить**.

Загрузка образов операционных систем и приложений в Хранилище

Чтобы загрузить в Хранилище пользовательские образы операционных систем и приложений, которые вы хотите установить в этих операционных системах:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Хранилище**.
3. Нажмите на кнопку **Загрузить**.
4. Откроется окно загрузки файла.
5. Выберите файл с расширением .ISO, который вы хотите загрузить в Хранилище.
6. Нажмите на кнопку **Open**.

   Если вы хотите загрузить несколько образов, повторите шаги 1–6 для каждого образа.

Образ будет загружен в Хранилище и отобразится в таблице объектов.

Активация образов операционных систем и приложений в Хранилище Sandbox

Вы можете создать виртуальную машину с неактивированными образами операционных систем Windows 7 (64-разрядная), Windows 10 (64-разрядная) и приложений, необходимых для работы компонента Sandbox, и активировать их с помощью своей лицензии после установки виртуальной машины.

Активация образов операционных систем Windows и пакета приложений Microsoft Office выполняется с помощью файла kata_images.py. Чтобы получить файл, обратитесь в Службу технической поддержки.

Для корректной активации образов операционных систем Windows и пакета приложений Microsoft Office требуется доступ в интернет. Убедитесь в том, что вы правильно настроили доступ в интернет.

Во время выполнения процедуры активации в разделе **Мониторинг** приложение проинформирует вас об ошибке самодиагностики Sandbox. После успешной активации ошибка самодиагностики перестанет отображаться. Во время активации объекты не будут отправляться на проверку в Sandbox.

Чтобы активировать образы операционных систем Windows и пакет приложений Microsoft Office:

1. Убедитесь, что были созданы и установлены виртуальные машины с неактивированными образами операционных систем Windows 7 (64-разрядная), Windows 10 (64-разрядная) и пакетом приложений Microsoft Office.

2. Войдите в консоль управления сервера с компонентом Sandbox по протоколу SSH или через терминал.

3. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке приложения.

   Отобразится меню администратора сервера Sandbox.

4. В меню администратора приложения выберите режим **Technical Support Mode**.

5. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

6. Выберите **Yes** и нажмите на клавишу **ENTER**.

7. Активируйте образы операционных систем Windows и пакет приложений Microsoft Office, выполнив последовательность команд:

   a. `cd /opt/kaspersky/sandbox/bin/`

   b. `sudo -s`

   c. `./sbimages_cli activate --vm_id Win7_x64 --component Win7 --key <код активации образа 64-разрядной операционной системы Windows 7>`

   d. `./sbimages_cli activate --vm_id Win7_x64 --component Office2010 --key <код активации приложения Microsoft Office 2010>`

   e. `./sbimages_cli activate --vm_id Win10_x64 --component Win10 --key <код активации образа 64-разрядной операционной системы Windows 10>`

   f. `./sbimages_cli activate --vm_id Win10_x64 --component Office2016 --key <код активации приложения Microsoft Office 2016>`

   Код активации имеет следующий формат: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX.

8. Создайте точки восстановления для виртуальных машин с добавленными лицензионными ключами, выполнив команду:

   `./sbimages_cli snapshot --vm_ids Win7_x64,Win10_x64`

   Процесс может занять некоторое время.

9. Убедитесь, что в разделе **Мониторинг** веб-интерфейса приложения отсутствуют предупреждения о неработоспособности компонента Sandbox.

Образы операционных систем Windows и пакет приложений Microsoft Office будут активированы. Активацию образов операционных систем Windows и пакета приложений Microsoft Office необходимо провести на всех серверах Sandbox.

Если при попытке активации возникают проблемы, рекомендуем обратиться в Службу технической поддержки.

Удаление образов операционных систем и приложений из Хранилища Sandbox

Чтобы удалить образ операционной системы или приложения из Хранилища Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Хранилище**.
3. В столбце **Действие** напротив нужного образа нажмите на ссылку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Образ будет удален.

Работа с шаблонами виртуальных машин

Виртуальные машины создаются на основе шаблонов. Чтобы создать виртуальную машину, вам нужно предварительно импортировать или создать для нее шаблон. На основе одного шаблона может быть создано несколько виртуальных машин.

Вы можете выполнять с шаблонами следующие операции: просматривать таблицу шаблонов, включать и выключать шаблоны, редактировать, экспортировать и удалять шаблоны.

Операции с шаблоном недоступны, если на основе этого шаблона создается или устанавливается пользовательская виртуальная машина. После завершения процесса создания и установки виртуальной машины вы снова сможете выполнять операции с шаблоном.

Создание шаблона виртуальной машины

Чтобы создать виртуальную машину, вам нужно предварительно создать для нее шаблон.

Чтобы создать шаблон для виртуальной машины:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. В раскрывающемся списке **Добавить** выберите **Создать шаблон**.

   Откроется окно создания шаблона.

4. На этапе **Подготовка образа** выполните следующие действия:

   a. В поле **Имя** введите имя шаблона.

   b. В поле **Описание** введите описание шаблона. Поле не является обязательным.

   c. В раскрывающемся списке **Образ ОС** выполните одно из следующих действий:

   - Выберите образ операционной системы, который вы хотите использовать для шаблона, в списке доступных образов.

     Чтобы образ отображался в списке, вам нужно загрузить его в Хранилище.

   - Загрузите образ операционной системы, нажав на ссылку **Загрузить**, выберите нужный файл и нажмите на кнопку **Open**.

     Загружаемый файл должен иметь расширение ISO.

5. Нажмите на кнопку **Продолжить**.

6. На этапе **Настройка шаблона** выполните следующие действия:

   a. В раскрывающемся списке **Подключить ISO** выберите образ приложения, которое вы хотите установить в операционной системе.

   Чтобы образ отображался в списке, вам нужно выполнить одно из следующих действий:

   - Загрузить образ в Хранилище.

   - В раскрывающемся списке **Подключить ISO** нажать на ссылку **Загрузить**, выбрать нужный файл и нажать на кнопку **Open**.

     Загружаемый файл должен иметь расширение ISO.

   b. Если вы хотите размонтировать установленный образ, в раскрывающемся списке **Подключить ISO** нажмите на значок ⏏ напротив этого образа.

   c. Настройте операционную систему и программное обеспечение, установленное в ней.

   d. В раскрывающемся списке **Выключить** вы можете выполнить одно из следующих действий:

   - **Выключить**, если вы хотите завершить работу системы с сохранением результата работы запущенных приложений.

   - **Отключить питание**, если вы хотите завершить работу системы без сохранения результатов работы.

     Если шаблон включен, на его основе нельзя создать виртуальную машину и нельзя экспортировать шаблон. Если вы хотите продолжить настройку шаблона, включите его.

Создание шаблона виртуальной машины будет завершено. Вы можете создать на его основе виртуальную машину.

Просмотр таблицы шаблонов

Чтобы просмотреть таблицу шаблонов:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.

   Отобразится таблица шаблонов.

В таблице содержится следующая информация:

- **Создано** – время создания шаблона.
- **Тип** – тип операционной системы: пользовательская или преднастроенная.
- **Имя** – имя шаблона.
- **Состояние** – состояние шаблона, например, **Включить** или **Выключено**.
- **Размер** – размер шаблона.
- **ОС** – версия операционной системы, которая используется для шаблона.
- **ВМ** – виртуальная машина, созданная на основе этого шаблона.
- **Действия** – доступные для шаблона операции. Доступны следующие операции: **Создать VM**, **Экспортировать** (), **Удалить** ().
- **Описание** – описание, заданное при создании шаблона.

Включение и выключение шаблона

Если шаблон выключен, вы можете выполнять с ним следующие операции: создать на его основе виртуальную машину, экспортировать, удалить. Если шаблон включен, вы можете редактировать его.

Чтобы включить или выключить шаблон:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.

4. В разделе **Настройка шаблона** выполните одно из следующих действий:

   - Если вы хотите включить шаблон, в консоли управления шаблоном нажмите на кнопку **Включить**.
   - Если вы хотите выключить шаблон, в консоли управления шаблоном в раскрывающемся списке **Выключить** выберите один из вариантов:
     - **Выключить**, если вы хотите завершить работу системы с сохранением результата работы запущенных приложений.
     - **Отключить питание**, если вы хотите завершить работу системы без сохранения результатов работы.

Шаблон будет включен или выключен.

Редактирование шаблона

Чтобы отредактировать шаблон:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.
4. Если шаблон выключен, включите его, нажав на кнопку **Включить**.
5. Если вы хотите установить приложение в операционной системе, которая используется для шаблона, в раскрывающемся списке **Подключить ISO** выберите образ приложения.

   Чтобы образ отображался в списке, вам нужно загрузить образ в Хранилище.
6. Если вы хотите размонтировать установленный образ, в раскрывающемся списке **Подключить ISO** нажмите на значок **Размонтировать** ⏏ напротив этого образа.
7. Настройте операционную систему и программное обеспечение, установленное в ней.

Шаблон будет отредактирован.

Настройка операционной системы и программного обеспечения

Подготовка операционных систем к работе

При установке операционных систем Windows 7, 8.1 или 10 выполните следующие требования:

- Отключите экранную заставку.
- Выберите схему питания *Всегда включено*.

- Отключите автоматическое обновление.
- Отключите брандмауэр Windows.

При использовании операционной системы Windows 7 требуется поддержка хеш-алгоритма SHA-2. Для поддержки этого хеш-алгоритма установите обновление Security Update for Windows 7 for x64-based Systems (KB3033929). Для 32-битных операционных систем Windows 7 также требуется установить обновление KB3033929.

> Не устанавливайте обновление KB4474419. Это обновление может вызвать сбой во время развертывания виртуальной машины.

Для использования Windows 7 необходимо в настройках операционной системы включить использование TLS 1.1 и TLS 1.2. Для этого в Windows 7 в разделе **Панель управления** → **Свойства браузера** → **Дополнительно** установите флажок **Использовать TLS 1.1** и **Использовать TLS 1.2**.

При использовании операционных систем Windows 8.1 и 10 требуется отключить функцию быстрой загрузки (fast boot) и включить функцию автоматического входа в систему (автологин).

Локализация операционных систем

Вы можете выбрать язык локализации при установке системы или установить систему с английской локализацией и дополнительно установить пакет локализации в эту систему. Вы можете выбрать один из следующих языков: русский, английский, китайский (Simplified), арабский, испанский (Мексика). При выборе другой локализации качество проверки объектов будет снижено.

> Для операционной системы Windows XP поддерживаются только русский и английский языки.

Настройка операционных систем

С установленной операционной системой требуется выполнить следующие действия:

- Убедиться, что включено использование командной оболочки по умолчанию.
- Активировать операционную систему и другое лицензионное программное обеспечение.

> При использовании операционной системы Windows 10 требуется устранить уязвимости типа Spectre и Meltdown и отключить Защитник Windows.

Вы можете выполнить с установленной операционной системой следующие действия:

- Присвоить статичное имя компьютеру.
- Создать учетные записи пользователей.

  В этом случае требуется настроить автоматический вход в систему.

- Установить программное обеспечение.

  Ограничения, действующие при установке программного обеспечения:

  - К одному шаблону единовременно можно подключить только один образ. После того как шаблон будет сохранен, вы можете отключить один образ и подключить другой.
  - Поддерживаются следующие версии Microsoft Office: Microsoft Office Professional Plus 2010 для Windows 7 и Microsoft Office Professional Plus 2016 для Windows 10.
  - Настоятельно не рекомендуется устанавливать программное обеспечение следующих типов:
    - Программное обеспечение, внедряющее свой код в другой запущенный процесс.
    - Драйверы для защиты.
    - Антивирусные приложения, включая Защитник Windows.
  - Не гарантируется обнаружение вредоносной активности файлов, которые запускаются с помощью узкоспециального программного обеспечения.

Kaspersky Anti Targeted Attack Platform не уведомляет о проблемах с установленным в операционной системе программным обеспечением.

Устранение уязвимостей типа Spectre и Meltdown

Для успешной установки пользовательской виртуальной машины на основе операционной системы Windows 10 требуется устранить уязвимости типа Spectre и Meltdown.

Чтобы устранить уязвимости типа Spectre и Meltdown:

1. В терминале гостевой операционной системы выполните следующую последовательность команд:

   ```
   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 3 /f
   ```

   ```
   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f
   ```

2. Перезагрузите виртуальную машину.

Уязвимости типа Spectre и Meltdown будут устранены.

Удаление Защитника Windows

Для успешной установки пользовательской виртуальной машины на основе операционной системы Windows 10 требуется удалить Защитник Windows.

> Все действия необходимо выполнять в гостевой операционной системе.

Чтобы удалить Защитник Windows:

1. Создайте параметр DWORD32 в ветке реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender.
2. Добавьте следующие значения для параметра DWORD32, созданного на шаге 1:
   - AllowFastServiceStartup = 0.
   - ServiceKeepAlive = 0.
   - DisableAntiSpyware = 1.
3. Создайте подраздел Real-Time Protection в ветке реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender.
4. Создайте параметр DWORD32 в подразделе Real-Time Protection.
5. Добавьте следующие значения для параметра DWORD32, созданного на шаге 4:
   - DisableIOAVProtection = 1.
   - DisableRealtimeMonitoring = 1.
6. Создайте подраздел Spynet в ветке реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender.
7. Создайте параметр DWORD32 в подразделе Spynet.
8. Добавьте следующие значения для параметра DWORD32, созданного на шаге 6:
   - DisableBlockAtFirstSeen = 1.
   - LocalSettingOverrideSpynetReporting = 1.
   - SubmitSamplesConsent = 1.
9. Отключите Защитник Windows средствами групповых политик. Для этого выполните следующие действия:
   a. Нажмите комбинацию клавиш Win+R.
   b. В открывшемся диалоговом окне **Выполнить** в поле **Открыть** введите gpedit.msc.
   c. Нажмите на кнопку **OK**.

d. Перейдите к параметру **Выключить антивирусную программу Microsoft Defender**: **Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Антивирусная программа Microsoft Defender → Выключить антивирусную программу Microsoft Defender → Изменить параметры политики**.

e. Выберите **Отключено**.

10. Войдите в безопасный режим:

a. Нажмите комбинацию клавиш Win+R.

b. В диалоговом окне **Выполнить** в поле **Открыть** введите msconfig.

c. Нажмите на кнопку **OK**.

d. В открывшемся окне перейдите на вкладку **Загрузка**.

e. Установите флажок **Безопасный режим**.

f. В блоке параметров под флажком **Безопасный режим** выберите **Минимальная**.

g. Последовательно нажмите на кнопки **Применить** и **OK**.

h. В открывшемся окне выберите **Перезагрузить**.

11. После перезагрузки удалите раздел WinDefend из реестра:

a. Нажмите комбинацию клавиш Win+R.

b. В открывшемся диалоговом окне **Выполнить** в поле **Открыть** введите regedit.

c. Нажмите на кнопку **OK**.

d. Удалите раздел раздел WinDefend в ветке реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services.

12. Отключите безопасный режим:

a. Нажмите комбинацию клавиш Win+R.

b. В диалоговом окне **Выполнить** в поле **Открыть** введите msconfig.

c. Нажмите на кнопку **OK**.

d. В открывшемся окне перейдите на вкладку **Загрузка**.

e. Снимите флажок **Безопасный режим**.

f. Последовательно нажмите на кнопки **Применить** и **OK**.

g. В открывшемся окне выберите **Перезагрузить**.

Защитник Windows будет удален.

Экспорт шаблона

Вы можете экспортировать шаблон одним из следующих способов:

- В таблице шаблонов.
- При просмотре шаблона.

Шаблон должен быть выключен.

Чтобы экспортировать шаблон в таблице шаблонов:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. В столбце **Действие** напротив нужного шаблона нажмите на значок .

   Шаблон будет экспортирован. Загрузка файла начнется автоматически.

Чтобы экспортировать шаблон при просмотре шаблона:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.
4. В раскрывающемся списке **Действия** выберите **Экспортировать**.

   Загрузка файла начнется автоматически.

Импорт шаблона

Вы можете импортировать шаблон, созданный ранее.

Чтобы импортировать шаблон:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. В раскрывающемся списке **Добавить** выберите **Импортировать шаблон**.
4. Откроется окно загрузки файла.

5. Выберите файл, который вы хотите импортировать.
6. Нажмите на кнопку **Open**.

   Шаблон отобразится в списке шаблонов.

Вы можете отредактировать шаблон, создать из него виртуальную машину, экспортировать или удалить.

Удаление шаблона

При удалении шаблона удаляются все созданные на его основе виртуальные машины.

Вы можете удалить шаблон одним из следующих способов:

- В таблице шаблонов.
- При просмотре шаблона.

Шаблон должен быть выключен.

Чтобы удалить шаблон в таблице шаблонов:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. В столбце **Действие** напротив нужного шаблона нажмите на значок .

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

   Шаблон будет удален.

Чтобы удалить шаблон при просмотре шаблона:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.
4. В раскрывающемся списке **Действия** выберите **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

   Шаблон будет удален.

Управление виртуальными машинами

Вы можете создавать, устанавливать и удалять установленные и ожидающие установки виртуальные машины. Также вы можете просматривать списки виртуальных машин с преднастроенными и пользовательскими операционными системами.

Создание виртуальной машины

Вы можете создать виртуальную машину в веб-интерфейсе Sandbox одним из следующих способов:

- В разделе **Виртуальные машины**.
- В таблице шаблонов.
- В окне просмотра шаблона.

Шаблон для виртуальной машины должен быть выключен. После создания виртуальную машину требуется установить.

Создание виртуальной машины в веб-интерфейсе Sandbox может завершаться ошибкой из-за ограничений браузера. Если вы столкнулись с такими ограничениями, вы можете создать и установить виртуальную машину через командную строку.

Для создания пользовательской виртуальной машины требуется доступ в интернет.

Создание виртуальной машины в разделе Виртуальные машины

*Чтобы создать виртуальную машину с преднастроенным образом операционной системы в разделе **Виртуальные машины**:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Виртуальные машины**.
3. Нажмите на кнопку **Создать VM**.

   Откроется окно создания виртуальной машины.
4. В раскрывающемся списке **Шаблон** выберите шаблон для виртуальной машины.

   Если в списке нет подходящего шаблона, вы можете импортировать или создать шаблон в разделе **Шаблоны** окна веб-интерфейса Sandbox.
5. В поле **Имя** введите имя виртуальной машины.
6. В поле **Описание** введите описание виртуальной машине. Поле необязательно для заполнения.

7. Нажмите на кнопку **Сохранить**.

8. Для некоторых операционных систем из комплекта поставки необходимо принятие условий лицензионного соглашения. Ознакомьтесь с текстом лицензионного соглашения и нажмите на кнопку **Принять**.

Виртуальная машина с преднастроенным образом операционной системы будет создана.

*Чтобы создать виртуальную машину с пользовательским образом операционной системы в разделе **Виртуальные машины**:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.

2. Перейдите в раздел **Виртуальные машины**.

3. Нажмите на кнопку **Создать VM**.

   Откроется окно создания виртуальной машины.

4. В раскрывающемся списке **Шаблон** выберите шаблон для виртуальной машины.

   Если в списке нет подходящего шаблона, вы можете импортировать или создать шаблон в разделе **Шаблоны** окна веб-интерфейса Sandbox.

5. В поле **Имя** введите имя виртуальной машины.

   > Имя должно быть указано на латинице.

6. В поле **Описание** введите описание виртуальной машине. Поле необязательно для заполнения.

7. Нажмите на кнопку **Сохранить**.

8. Если для сервера, на котором создается виртуальная машина, не настроен доступ в интернет, в окне **Шаблоны** отобразится окно с ошибкой *Нет доступа в интернет*. Для завершения создания виртуальной машины вам нужно загрузить отладочные символы.

Виртуальная машина с пользовательским образом операционной системы будет создана.

Создание виртуальной машины в таблице шаблонов

Чтобы создать виртуальную машину с преднастроенным образом операционной системы в таблице шаблонов:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.

   Перейдите в раздел **Шаблоны**.

2. В столбце **Действия** напротив нужно шаблона нажмите на ссылку **Создать VM**.

   Откроется окно создания виртуальной машины.

3. В раскрывающемся списке **Шаблон** выберите шаблон для виртуальной машины.

   Если в списке нет подходящего шаблона, вы можете импортировать или создать шаблон в разделе **Шаблоны** окна веб-интерфейса Sandbox.

4. В поле **Имя** введите имя виртуальной машины.

5. В поле **Описание** введите описание виртуальной машине. Поле необязательно для заполнения.

6. Нажмите на кнопку **Сохранить**.

7. Для некоторых операционных систем из комплекта поставки необходимо принятие условий лицензионного соглашения. Ознакомьтесь с текстом лицензионного соглашения и нажмите на кнопку **Принять**.

Виртуальная машина с преднастроенным образом операционной системы будет создана.

Чтобы создать виртуальную машину с пользовательским образом операционной системы в таблице шаблонов:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.

   Перейдите в раздел **Шаблоны**.

2. В столбце **Действия** напротив нужно шаблона нажмите на ссылку **Создать VM**.

   Откроется окно создания виртуальной машины.

3. В раскрывающемся списке **Шаблон** выберите шаблон для виртуальной машины.

   Если в списке нет подходящего шаблона, вы можете импортировать или создать шаблон в разделе **Шаблоны** окна веб-интерфейса Sandbox.

4. В поле **Имя** введите имя виртуальной машины.

   > Имя должно быть указано на латинице.

5. В поле **Описание** введите описание виртуальной машине. Поле необязательно для заполнения.

6. Нажмите на кнопку **Сохранить**.

7. Если для сервера, на котором создается виртуальная машина, не настроен доступ в интернет, в окне **Шаблоны** отобразится окно с ошибкой *Нет доступа в интернет*. Для завершения создания виртуальной машины вам нужно загрузить отладочные символы.

Виртуальная машина с пользовательским образом операционной системы будет создана.

Создание виртуальной машины в окне просмотра шаблона

Чтобы создать виртуальную машину с преднастроенным образом операционной системы в окне просмотра шаблона:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.

2. Перейдите в раздел **Шаблоны**.

3. Выберите нужный шаблон.

4. Нажмите на кнопку **Создать VM**.

   Откроется окно создания виртуальной машины.

5. В раскрывающемся списке **Шаблон** выберите шаблон для виртуальной машины.

   Если в списке нет подходящего шаблона, вы можете импортировать или создать шаблон в разделе **Шаблоны** окна веб-интерфейса Sandbox.

6. В поле **Имя** введите имя виртуальной машины.

7. В поле **Описание** введите описание виртуальной машине. Поле необязательно для заполнения.

8. Нажмите на кнопку **Сохранить**.

9. Для некоторых операционных систем из комплекта поставки необходимо принятие условий лицензионного соглашения. Ознакомьтесь с текстом лицензионного соглашения и нажмите на кнопку **Принять**.

Виртуальная машина с преднастроенным образом операционной системы будет создана.

Чтобы создать виртуальную машину с пользовательским образом операционной системы в окне просмотра шаблона:

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.

2. Перейдите в раздел **Шаблоны**.

3. Выберите нужный шаблон.

4. Нажмите на кнопку **Создать VM**.

   Откроется окно создания виртуальной машины.

5. В раскрывающемся списке **Шаблон** выберите шаблон для виртуальной машины.

   Если в списке нет подходящего шаблона, вы можете импортировать или создать шаблон в разделе **Шаблоны** окна веб-интерфейса Sandbox.

6. В поле **Имя** введите имя виртуальной машины.

   > Имя должно быть указано на латинице.

7. В поле **Описание** введите описание виртуальной машине. Поле необязательно для заполнения.

8. Нажмите на кнопку **Сохранить**.

9. Если для сервера, на котором создается виртуальная машина, не настроен доступ в интернет, в окне **Шаблоны** отобразится окно с ошибкой *Нет доступа в интернет*. Для завершения создания виртуальной машины вам нужно загрузить отладочные символы.

Виртуальная машина с пользовательским образом операционной системы будет создана.

Создание и установка виртуальной машины через командую строку

Создание виртуальной машины в веб-интерфейсе Sandbox может завершаться ошибкой из-за ограничений браузера. Если вы столкнулись с такими ограничениями, вы можете создать и установить виртуальную машину через командную строку.

Для создания пользовательской виртуальной машины требуется доступ в интернет.

Виртуальные машины нужно создавать поочередно.

Чтобы создать и установить виртуальную машину через командную строку:

1. Войдите в консоль управления сервера Sandbox по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке Sandbox.

   Отобразится меню администратора компонента.
3. В меню администратора компонента выберите режим Technical Support Mode.
4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Подтвердите, что хотите выполнять действия с компонентом в режиме Technical Support Mode. Для этого выберите **Ok** и нажмите на клавишу **Enter**.
6. Просмотрите список всех доступных в системе ISO-образов:

   ```
   sb-vm-iso --list-iso
   ```

   Список отображается в виде JSON-массива, где перечислены имена ISO-образов. Далее в инструкции для обозначения имени ISO-образа используется переменная `<ISO name>`.
7. Убедитесь, что ISO-образ находится в рабочем состоянии и готов к развертыванию:

   ```
   sb-vm-iso --check-install <ISO name>
   ```

   После выполнения команды должен отобразиться статус `success`.
8. Установите виртуальную машину:

   ```
   sb-vm-iso --install <ISO name>
   ```

   Выполнение команды займет некоторое время. Система не уведомляет об успешном или неуспешном статусе установки.
9. Сохраните параметры:

   ```
   sb-vms --apply-all
   ```

   Выполнение команды займет некоторое время. После выполнения команды должен отобразиться статус `success`.

10. Убедитесь, что виртуальная машина, созданная в результате выполнения шагов 7-9 этой инструкции, отображается в списке виртуальных машин. Инструкции для просмотра списка виртуальных машин приведены в разделах Просмотр таблицы преднастроенных виртуальных машин и Просмотр таблицы пользовательских виртуальных машин.

11. Повторите шаги 7-10 этой инструкции для каждого ISO-образа, на основе которого вы хотите создать и установить виртуальную машину.

Виртуальная машина будет создана и установлена. Имя этой виртуальной машины отобразится в списке виртуальных машин.

Просмотр таблицы преднастроенных виртуальных машин

Чтобы просмотреть список преднастроенных виртуальных машин:

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.

2. Выберите закладку **Преднастроенные**.

Отобразится таблица преднастроенных виртуальных машин.

В таблице содержится следующая информация:

- **Имя** – имя виртуальной машины.
- **Состояние** – состояние виртуальной машины, например, **Включено** или **Выключено**.
- **Действия** – доступные для виртуальной машины операции. Могут быть доступны следующие операции: **Удалить**.

В разделе **Не установленные виртуальные машины** отображаются готовые к установке, но еще не установленные виртуальные машины.

Просмотр таблицы пользовательских виртуальных машин

Чтобы просмотреть список пользовательских виртуальных машин:

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.

2. Выберите закладку **Пользовательские**.

Отобразится таблица пользовательских виртуальных машин.

В таблице содержится следующая информация:

- **Создано** – время создания виртуальной машины.
- **Имя** – имя виртуальной машины.
- **Состояние** – состояние виртуальной машины, например, **Включено** или **Выключено**.

- **Действия** – доступные для виртуальной машины операции. Могут быть доступны следующие операции: **Удалить**.
- **Описание** – описание, заданное при создании виртуальной машины.

Установка виртуальной машины

После создания виртуальной машины ее нужно установить.

Чтобы установить виртуальную машину с преднастроенным образом операционной системы:

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. Выберите закладку **Преднастроенные**.
3. В разделе **Не установленные виртуальные машины** нажмите на кнопку **Установить готовые VM**.

   Все виртуальные машины, ожидающие установки, будут установлены.

Чтобы установить виртуальную машину с пользовательским образом операционной системы:

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. Выберите закладку **Пользовательские**.
3. Напротив нужной виртуальной машины в столбце **Действия** нажмите на ссылку **Установить**.
4. Когда виртуальная машина установится, в столбце **Действия** нажмите на ссылку **Включить**.

   Виртуальная машина будет установлена и готова к работе.

Удаление виртуальной машины

Чтобы удалить установленную виртуальную машину:

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. Выберите закладку **Преднастроенные** или **Пользовательские**.
3. В столбце **Действия** напротив нужной виртуальной машины нажмите на ссылку **Удалить**.

   Виртуальная машина будет удалена.

Чтобы удалить еще не установленную виртуальную машину с преднастроенным образом операционной системы:

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. В разделе **Не установленные виртуальные машины** нажмите на кнопку **Удалить все ожидающие VM**.

   Все виртуальные машины с преднастроенными образами операционных систем, ожидающие установки, будут удалены.

Чтобы удалить еще не установленную виртуальную машину с пользовательским образом операционной системы:

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. Выберите закладку **Пользовательские**.
3. Напротив нужной виртуальной машины в столбце **Действия** нажмите на ссылку **Удалить**.

   Виртуальная машина с пользовательским образом операционной системы, ожидающая установки, будет удалена.

Загрузка отладочных символов

Если для сервера, на котором устанавливается виртуальная машина с пользовательским образом, не настроен доступ в интернет, для корректного завершения установки виртуальной машины вам нужно загрузить отладочные символы Microsoft.

Вы можете загрузить отладочные символы в процессе установки виртуальной машины в окне **Шаблоны** только после того, как виртуальная машина получит статус **Сбой** в списке виртуальных машин.

Для корректной загрузки отладочных символов в операционной системе, которая используется для шаблона виртуальной машины, должны быть установлены средства для отладки Windows (Windows Debug Tools) и имя хоста, подключенного к сети (hostname), должно содержать только латинские буквы, цифры и специальные символы.

*Чтобы загрузить отладочные символы в процессе установки виртуальной машины в окне **Шаблоны**:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.
4. В окне с ошибкой *Нет доступа в интернет* нажмите на кнопку **Скачать манифест**.

   Кнопка **Скачать манифест** не будет доступна, пока виртуальная машина не получит статус **Сбой**.

   На ваш компьютер будет загружен архив.

5. Распакуйте скачанный архив.
6. Запустите файл sbsymtool.ps1 с помощью Windows PowerShell.

   Архив с отладочными символами будет загружен в папку с этим файлом.
7. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
8. Перейдите в раздел **Шаблоны**.
9. Выберите шаблон, для которого вы загрузили отладочные символы.
10. В раскрывающемся списке **Действия** выберите **Загрузить символы**.
11. В открывшемся окне выберите архив с отладочными символами и нажмите на кнопку **Open**.

Отладочные символы будут загружены. Виртуальная машина будет установлена и отобразится в списке виртуальных машин с пользовательскими операционными системами.

*Чтобы загрузить отладочные символы после того, как виртуальная машина получила статус **Сбой** в списке виртуальных машин:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.
4. В раскрывающемся списке **Действия** выберите **Скачать манифест**.

   На ваш компьютер будет загружен архив.
5. Распакуйте скачанный архив.
6. Запустите файл sbsymtool.ps1 с помощью Windows PowerShell.

   Архив с отладочными символами будет загружен в папку с этим файлом.
7. В окне **Шаблоны** раскройте список **Действия** и выберите **Загрузить символы**.
8. В открывшемся окне выберите архив с отладочными символами и нажмите на кнопку **Open**.

Отладочные символы будут загружены. Виртуальная машина будет установлена и отобразится в списке виртуальных машин с пользовательскими операционными системами.

Установка максимального количества одновременно запускаемых виртуальных машин

Задайте ограничение для количества одновременно запускаемых виртуальных машин с операционными системами, в которых компонент Sandbox будет обрабатывать объекты. Мы рекомендуем использовать значения, приведенные в разделе *Расчеты для компонента Sandbox*. Если вы хотите использовать другие значения, вам нужно убедиться, что сервер, на котором установлен Sandbox, обладает достаточным количеством аппаратных ресурсов.

Вы можете рассчитать количество одновременно запускаемых виртуальных машин с образами операционных систем по следующей формуле: <количество логических ядер> * 1,5.

По умолчанию максимальное количество одновременно запускаемых виртуальных машин – 100. Вы можете увеличить его до 200, выполнив шаги инструкции *Изменение количества лицензионных ключей для пользовательской виртуальной машины* перед установкой нового лимита одновременно запускаемых виртуальных машин.

Количество одновременно запускаемых виртуальных машин не может превышать 200.

Чтобы установить максимальное количество одновременно запускаемых виртуальных машин:

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В блоке параметров **Гостевые виртуальные машины** в поле **Максимум VM одновременно** введите количество одновременно запускаемых виртуальных машин.

   По умолчанию вы можете ввести число от 1 до 100. Если вы предварительно изменили количество лицензионных ключей для пользовательской виртуальной машины на 200, вы можете указать число от 1 до 200.
3. Нажмите на кнопку **Сохранить**.

Изменение количества лицензионных ключей для пользовательской виртуальной машины

При создании пользовательской виртуальной машины Kaspersky Anti Targeted Attack Platform указывает количество лицензионных ключей для программного обеспечения, которое используется внутри этой виртуальной машины. По умолчанию количество лицензионных ключей равно количеству одновременно запускаемых виртуальных машин. Ваша лицензия должна покрывать это число. При необходимости вы можете изменить количество лицензионных ключей для виртуальной машины.

Если количество лицензионных ключей, которое вы задали для виртуальной машины, меньше количества одновременно запускаемых виртуальных машин, то возможно снижение общей производительности сервера Sandbox.

Менять заданное количество одновременно запускаемых виртуальных машин не рекомендуется.

Чтобы изменить количество лицензионных ключей для пользовательской виртуальной машины:

1. Войдите в консоль управления сервера Sandbox по протоколу SSH или через терминал.
2. Получите список серверов, выполнив команду `sb-custom-images list-vm`

Отобразится таблица виртуальных машин, где:

- `id` – идентификатор виртуальной машины;
- `name` – имя виртуальной машины;
- `licenses` – количество лицензионных ключей.

3. Задайте количество лицензионных ключей для выбранной виртуальной машины, выполнив команду `sb-custom-images licenses -id <идентификатор виртуальной машины> -ln <количество лицензий>`.

Количество лицензионных ключей будет изменено.

Вы можете вызвать справку скрипта, выполнив команду `sb-custom-images --help`.

Экспорт параметров Sandbox

Чтобы экспортировать параметры системы Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Параметры** нажмите на кнопку **Экспортировать**.

   Откроется окно **Предупреждение**, содержащее предупреждение об особенностях экспорта параметров системы.

   Параметры системы Sandbox зависят от аппаратных и программных параметров сервера, на котором установлен компонент Sandbox. Экспортируемые параметры системы Sandbox предназначены для импорта на этот же или строго идентичный по конфигурации сервер. Попытки восстановить конфигурацию системы Sandbox значениями параметров, сохраненными на другой системе Sandbox, могут нарушить работу системы Sandbox.

3. Нажмите на кнопку **Сохранить**.

Файл формата tar.gz загрузится на жесткий диск вашего компьютера в ту директорию, которая указана в качестве директории загрузки файлов из интернета в параметрах браузера, который вы используете для работы приложения. В файле содержатся все текущие параметры системы Sandbox.

Архивы с резервной копией параметров системы могут содержать такие конфиденциальные данные, как, например, пароли, закрытые ключи. Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность этих данных самостоятельно.

Импорт параметров Sandbox

Чтобы импортировать параметры Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Параметры** нажмите на кнопку **Импортировать**.

   Откроется окно **Предупреждение**, содержащее предупреждение об особенностях импорта параметров системы.

   Параметры компонента Sandbox зависят от аппаратных и программных параметров сервера, на котором установлен Sandbox. Экспортируемые параметры Sandbox предназначены для импорта на этот же или строго идентичный по конфигурации сервер. Попытки восстановить конфигурацию одной системы Sandbox настройками параметров, сохраненными на другой системе Sandbox, могут нарушить работу системы.

3. Нажмите на кнопку **Восстановить**.

   Откроется окно выбора файлов.

4. Выберите файл формата tar.gz с параметрами Sandbox, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

   Если импорт параметров Sandbox прошел успешно, сервер Sandbox перезагрузится. Через несколько минут вам нужно обновить окно браузера и повторить вход.

Архивы с резервной копией конфигурации системы могут содержать такие конфиденциальные данные, как, например, пароли, закрытые ключи. Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность хранения этих данных самостоятельно.

Перезагрузка сервера Sandbox

Чтобы перезагрузить сервер Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Питание** нажмите на кнопку **Перезагрузить**.

   Откроется окно подтверждения перезагрузки сервера Sandbox.

3. Нажмите на кнопку **Да**.

Сервер Sandbox перезагрузится. Через несколько минут вы сможете войти в систему.

Выключение сервера Sandbox

Чтобы выключить сервер Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Питание** нажмите на кнопку **Выключить**.

   Откроется окно подтверждения выключения сервера Sandbox.
3. Нажмите на кнопку **Да**.

Сервер Sandbox выключится.

Изменение пароля учетной записи администратора Sandbox

Чтобы изменить пароль учетной записи администратора Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В блоке параметров **Изменить пароль** отобразится имя учетной записи администратора Sandbox, которое вы задали при установке Sandbox и поля для изменения пароля.
3. В поле **Текущий пароль** введите текущий пароль учетной записи администратора Sandbox.
4. В поле **Новый пароль** введите новый пароль учетной записи администратора Sandbox.
5. В поле **Подтвердить пароль** введите новый пароль учетной записи администратора Sandbox повторно.
6. Нажмите на кнопку **Изменить пароль**.

   Пароль учетной записи администратора Sandbox будет изменен.

Администратору: работа в веб-интерфейсе приложения

Этот раздел адресован специалистам, которые осуществляют установку и администрирование Kaspersky Anti Targeted Attack Platform, а также управление серверами PCN и SCN и тенантами в режиме распределенного решения и мультитенантности.

Интерфейс Kaspersky Anti Targeted Attack Platform

Работа с приложением осуществляется через веб-интерфейс. Разделы веб-интерфейса приложения различаются в зависимости от роли пользователя – администратор или сотрудник службы безопасности (**Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Аудитор**).

Окно веб-интерфейса приложения содержит следующие элементы:

- разделы в левой части и в нижней части окна веб-интерфейса приложения;
- закладки в верхней части окна веб-интерфейса приложения для некоторых разделов приложения;
- рабочую область в нижней части окна веб-интерфейса приложения.

Разделы окна веб-интерфейса приложения

Веб-интерфейс приложения для роли **Администратор** содержит следующие разделы:

- **Мониторинг**. Содержит данные мониторинга Kaspersky Anti Targeted Attack Platform.
- **Режим работы**. Содержит информацию о серверах PCN и SCN и о тенантах в режиме распределенного решения и мультитенантности.
- **Активы**. Содержит информацию о подключенных компьютерах с компонентом Endpoint Agent и их параметрах.
- **Журналы**: **Активность пользователей**, **Сообщения приложения**, **Аудит**. Содержит информацию о работе приложения и аудит действий пользователей в веб-интерфейсе.
- **Параметры**. Содержит параметры сервера с компонентом Central Node.
- **Серверы Sensor**. Содержит информацию о подключенных компонентах Sensor и их параметры.
- **Серверы Sandbox**. Содержит информацию о подключении компонента Central Node к компонентам Sandbox.
- **Внешние системы**. Содержит информацию об интеграции приложения с почтовыми сенсорами.
- **Конфигурация серверов**. Содержит информацию о параметрах масштабирования приложения.

Рабочая область окна веб-интерфейса приложения

В рабочей области отображается информация, просмотр которой вы выбираете в разделах и на закладках окна веб-интерфейса приложения, а также элементы управления, с помощью которых вы можете настроить отображение информации.

Пользователи с ролью **Аудитор** также могут просматривать эти разделы веб-интерфейса приложения.

Мониторинг работы приложения

Вы можете осуществлять мониторинг работы приложения с помощью виджетов в разделе **Мониторинг** окна веб-интерфейса приложения. Вы можете добавлять, удалять, перемещать виджеты, настраивать масштаб отображения виджетов и выбирать период отображения данных.

О виджетах и схемах расположения виджетов

С помощью виджетов вы можете осуществлять мониторинг работы приложения.

Схема расположения виджетов – вид рабочей области окна веб-интерфейса приложения в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать виджеты на схеме расположения виджетов.

В приложении доступны следующие виджеты:

- **Общая информация**:
  - **Время обработки в Sandbox**. Отображение среднего времени, за которое были получены результаты проверки объектов в Sandbox.
  - **Обработано**. Отображение состояния обработки трафика, поступающего от Sensor и Endpoint Agent на Central Node.
  - **Очереди**. Отображение сведений о количестве и объеме объектов, ожидающих проверки модулями и компонентами приложения.

  Если вы используете режим распределенного решения и мультитенантности, в разделе отображаются данные по выбранному вами тенанту и серверу.
- **NDR**:
  - **Пользовательский виджет**. Виджет с произвольно заданным статическим содержанием. С помощью пользовательских виджетов вы можете, например, логически разделять группы виджетов в разделе **Мониторинг**.
  - **Трафик**. Скорость поступления входящего трафика. Виджет может отображать данные по всем точкам мониторинга всех узлов с установленными компонентами приложения, по точкам мониторинга выбранного узла или только по одной точке мониторинга.

- **Уровень загрузки ЦП**. Загруженность процессора на выбранном узле с установленным компонентом приложения.

- **Уровень загрузки ОЗУ**. Объем потребления физической оперативной памяти на выбранном узле с установленным компонентом приложения.

- **Работоспособность NDR**. Информация о текущем состоянии работоспособности приложения. Виджет может отображать следующие значения:

  - **OK** – нет сообщений о нарушении работоспособности или все проблемы работоспособности устранены.

  - **Некритический сбой** – есть сообщения о некритических сбоях. Значение отображается до момента устранения проблемы работоспособности.

  - **Нарушена работа** – есть сообщения о нарушении работы приложения. Значение отображается до момента устранения проблемы работоспособности.

  - **Режим обслуживания** – приложение находится в режиме обслуживания.

- **Хранилище** – данные о диске, который находится в локальной файловой системе на выбранном узле с установленным компонентом программы. В этом виджете вы можете выбрать следующие данные для отображения:

  - **Использование диска** – процентное значение времени на обработку операций чтения и записи данных.

  - **Занято на диске** – объем занятого дискового пространства.

  - **Чтение с диска** – скорость чтения данных с диска.

  - **Запись на диск** – скорость записи данных на диск.

- **Задержка обработки трафика**. Текущее время задержки при обработке трафика с момента его поступления на точку мониторинга узла. Выводится максимальное время задержки, полученное со всех включенных точек мониторинга. Виджет может отображать данные по всем точкам мониторинга всех узлов с установленными компонентами приложения или по точкам мониторинга выбранного узла.

- **Статус функций защиты**. Общая информация о текущем состоянии функций защиты в составе приложения. Виджет может отображать следующие значения:

  - **Включены все** – работают все технологии и методы, предназначенные для постоянного использования, а также включены все созданные точки мониторинга.

  - **Не все включены** – некоторые функции защиты выключены или включены в режиме обучения, либо включены не все точки мониторинга.

- **Время работы**. Время работы Kaspersky Anti Targeted Attack Platform. В этом виджете вы можете выбрать следующие данные для отображения:

  - Эффективное время работы – время нормальной работы приложения (без сбоев) с последнего запуска до текущего момента.
  - Общее время работы – время работы с первого запуска приложения до текущего момента. Включает периоды нормальной работы приложения и периоды работы со сбоями.
  - С первого запуска приложения – общее время, прошедшее с первого запуска приложения до текущего момента. Включает периоды нормальной работы приложения, периоды работы со сбоями и периоды неработоспособного состояния.

Для виджетов предусмотрены различные средства привлечения внимания в зависимости от поступающих данных. Например, виджеты с информацией о приложении и аппаратных ресурсах могут автоматически изменять цвет, если информация требует внимания (в частности, при нагрузке на аппаратный ресурс близкой к критической).

В виджетах отображается только основная информация, которая изменяется динамически. Если вам нужно просмотреть более подробную информацию, вы можете перейти из раздела **Мониторинг** к другим разделам веб-интерфейса приложения. Переходы можно выполнять путем выбора элементов интерфейса виджетов с помощью мыши.

Чтобы на виджетах NDR отображались корректные данные, требуется настроить синхронизацию даты и времени между компонентами Central Node и Sensor.

Выбор тенанта и сервера для работы в разделе Мониторинг

Если вы используете режим распределенного решения и мультитенантности, перед началом работы в разделе **Мониторинг** вам нужно выбрать тенант и сервер, данные по которым вы хотите просмотреть. В виджетах функциональности NDR при этом будут отображаться данные по текущему узлу или по тому узлу, который выбран в параметрах виджета.

*Чтобы выбрать тенант и сервер для отображения данных в виджетах раздела **Мониторинг**:*

1. В правой верхней части окна веб-интерфейса приложения нажмите на стрелку рядом с именем сервера.
2. В раскрывшемся меню выберите тенант и нужный вам сервер из списка.

Отобразятся данные по выбранному вами серверу. Если вы хотите изменить тенант и сервер, вам нужно повторить действия по выбору тенанта и сервера.

Добавление виджета на текущую схему расположения виджетов

Чтобы добавить виджет на текущую схему расположения виджетов:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .

3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на кнопку **Виджеты**.
5. В появившемся окне **Настроить виджеты** выполните следующие действия:
   - Если вы хотите добавить виджет **Время обработки в Sandbox**, включите переключатель рядом с названием этого виджета.
   - Если вы хотите добавить другой виджет, нажмите на кнопку + рядом с названием этого виджета.
6. Закройте окно **Настроить виджеты** и нажмите на кнопку **Применить**.

Выбранный виджет будет добавлен на текущую схему расположения виджетов.

Перемещение виджета на текущей схеме расположения виджетов

Чтобы переместить виджет на текущей схеме расположения виджетов:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Изменить**.
4. Выберите виджет, который вы хотите переместить на схеме расположения виджетов.
5. Удерживая левую клавишу мыши на верхней части виджета, перетащите виджет на другое место схемы расположения виджетов.
6. Нажмите на кнопку **Применить**.

Текущая схема расположения виджетов будет сохранена.

Изменение отображения данных в виджетах NDR

После добавления виджета NDR для отображения данных используются параметры, заданные по умолчанию. При необходимости вы можете изменить параметры отображения.

Чтобы настроить параметры отображения виджета NDR:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Изменить**.

4. В правом верхнем углу виджета NDR, параметры отображения которого вы хотите поменять, нажмите на кнопку .

   Откроется окно для настройки параметров отображения.

5. Настройте параметры виджета NDR.

   В зависимости от выбранного виджета NDR окно может содержать следующие параметры:

   - **Изменить название** – если установлен флажок **Изменить название**, вы можете задать произвольное название виджета (отличающееся от заданного по умолчанию) в поле **Название виджета**. Параметр **Изменить название** отсутствует для пользовательских виджетов.
   - **Название виджета** – поле для ввода названия виджета, отличающегося от названия по умолчанию.
   - **Изменить описание** – если установлен флажок **Изменить описание**, вы можете задать произвольное описание виджета (отличающееся от заданного по умолчанию) в поле **Описание виджета**. Параметр **Изменить описание** отсутствует для пользовательских виджетов.
   - **Описание виджета** – поле для ввода названия виджета, отличающегося от названия по умолчанию.
   - **Период обновления** – задает период времени в секундах, после которого обновляются отображаемые данные.
   - **Отображать** – задает тип отображаемых данных (для виджетов с возможностью выбора данных для отображения).
   - **Источник данных** – задает узел с установленными компонентами приложения, данные от которого отображаются в виджете. Если выбран вариант **Вся программа**, виджет отображает данные со всех узлов.
   - **Изменять цвет по статусу** – если флажок установлен, цвет фона виджета автоматически изменяется в зависимости от уровня важности поступивших данных. Критическому (максимальному) уровню важности данных соответствует красный цвет фона. Если флажок снят, закрашивание фона выключено.
   - **Заданный фон** – определяет цвет фона пользовательского виджета. Вы можете выбрать вариант закрашивания цветом, который соответствует одному из уровней важности (**Информационный**, **Важный**, **Критический**), или выключить закрашивание фона с помощью варианта **Бесцветный**.

6. Нажмите на кнопку **Применить**.

Удаление виджета с текущей схемы расположения виджетов

Чтобы удалить виджет с текущей схемы расположения виджетов:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку .
3. В раскрывающемся списке выберите **Изменить**.

4. Нажмите на значок × в правом верхнем углу виджета, который вы хотите удалить со схемы расположения виджетов.

   Виджет будет удален из рабочей области окна веб-интерфейса приложения.

5. Нажмите на кнопку **Применить**.

Виджет будет удален с текущей схемы расположения виджетов.

Сохранение схемы расположения виджетов в PDF

Виджеты функциональности NDR в схеме расположения в PDF не сохраняются.

Чтобы сохранить схему расположения виджетов в PDF:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Сохранить как PDF**.

   Откроется окно **Сохранение в PDF**.

4. В нижней части окна в раскрывающемся списке **Ориентация** выберите ориентацию страницы.
5. Нажмите на кнопку **Скачать**.

   Схема расположения виджетов в формате PDF будет сохранена на жесткий диск вашего компьютера в папку загрузки браузера.

6. Нажмите на кнопку **Закрыть**.

Настройка периода отображения данных на виджетах

Вы можете настроить отображение данных на виджетах за следующие периоды:

- **День**.
- **Неделя**.
- **Месяц**.

Для виджетов NDR доступны следующие периоды:

- **1ч**.
- **12ч**.
- **24ч**.
- **7д**.

Вы можете указать период отображения данных для каждого виджета NDR отдельно.

Настройка отображения данных в виджетах

Чтобы настроить отображение данных на виджетах за сутки (с 00:00 до 23:59):

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в раскрывающемся списке периодов отображения данных выберите **День**.
3. В календаре справа от названия периода **День** выберите дату, за которую вы хотите получить данные на виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Чтобы настроить отображение данных на виджетах за неделю (с понедельника по воскресенье):

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в раскрывающемся списке периодов отображения данных выберите **Неделя**.
3. В календаре справа от названия периода **Неделя** выберите неделю, за которую вы хотите получить данные на виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Чтобы настроить отображение данных на виджетах за месяц (календарный месяц):

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в раскрывающемся списке периодов отображения данных выберите **Месяц**.
3. В календаре справа от названия периода **Месяц** выберите месяц, за который вы хотите получить данные на виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Настройка отображения данных в виджетах NDR

Чтобы настроить отображение данных на виджете NDR:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу виджета NDR, параметры отображения которого вы хотите поменять, нажмите на кнопку с отображением нужного временного интервала.

На виджете NDR отобразятся данные за выбранный вами период.

Мониторинг приема и обработки входящих данных

На виджете **Обработано** вы можете оценить статус обработки данных, поступающих от Sensor и Endpoint Agent на Central Node, и отследить ошибки обработки данных.

Вы можете выбрать компонент (Sensor или Endpoint Agent), поступление данных с которого вы хотите оценить, в раскрывающемся списке справа от названия виджета **Обработано**.

Вы можете выбрать тип отображения данных в раскрывающемся списке справа от названия компонента (Sensor или Endpoint Agent):

- **Текущая загрузка** – 5 минут до текущего момента.
- **Выбранный период**. В этом случае вы также можете настроить период отображения данных на виджетах.

В левой части каждого виджета отображается легенда виджета по цветам, которые используются на самих виджетах.

Если выбран тип отображения данных **Текущая загрузка**, справа от легенды отображается средняя скорость обработки данных за последние 5 минут.

Пример:
На виджете **Обработано**, где выбран Sensor типа **(SPAN)** или **(ICAP)** и тип отображения данных **Текущая загрузка**, отображается скорость обработки данных SPAN- и ICAP-трафика, поступающих от Sensor на Central Node в определенное время.
Отображаются следующие данные:

- **Трафик** – скорость поступления трафика на Central Node зеленым цветом (Мбит/сек.).

  Если скорость поступления трафика менее 1 Мбит/сек. информация по нему не отображается на виджете.

- **Файлы** – скорость обработки файлов серым цветом (объектов/сек.).
- **URL-адреса** – скорость обработки URL-адресов синим цветом (объектов/сек.).
- **Не обработано** – количество необработанных объектов вертикальными линиями красного цвета.
  При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость обработки данных в определенное время.
  На виджете **Обработано**, где выбран Sensor типа **(SMTP)** и тип отображения данных **Текущая загрузка**, отображается скорость обработки данныданных SPAN- и ICAP-трафикаых почтового трафика, поступающих от почтового сенсора на Central Node в определенное время.
  Отображаются следующие данные:
- **Трафик** – скорость поступления трафика на сервер с компонентом Sensor зеленым цветом (сообщений/сек.).
- **Файлы** – скорость обработки файлов серым цветом (объектов/сек.).
- **URL-адреса** – скорость обработки URL-адресов синим цветом (объектов/сек.).
- **Не обработано** – количество необработанных объектов вертикальными линиями красного цвета.
  При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость обработки данных в определенное время.
  На виджете **Обработано**, где выбран Sensor типа **(LOAD) Endpoint Agents** и тип отображения данных **Текущая загрузка**, отображается скорость обработки событий, поступающих от компонентов Endpoint Agent на сервер с компонентом Central Node в определенное время (Событий/сек.).
  При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость обработки данных в определенное время.

Если выбран тип отображения данных **Выбранный период**, справа от легенды отображается средняя скорость поступления трафика на Central Node и количество обработанных объектов за выбранный период.

Пример:
На виджете **Обработано**, где выбран Sensor типа **(SPAN)** или **(ICAP)** и тип отображения данных **Выбранный период** с настроенным периодом отображения данных **Месяц**, отображается скорость поступления SPAN- и ICAP-трафика на Central Node, а также количество файлов и URL-адресов, извлеченных из почтового трафика за выбранный месяц.
Отображаются следующие данные:

- **Средний трафик** – скорость поступления трафика на сервер с компонентом Central Node зеленым цветом (объектов/сек.).
- **Файлы** – количество извлеченных файлов серым цветом.
- **URL-адреса** – количество извлеченных URL-адресов синим цветом.
- **Не обработано** – количество необработанных объектов вертикальными линиями красного цвета.
  При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость поступления трафика на Central Node и количество обработанных объектов в определенное время.
  На виджете **Обработано**, где выбраны Sensor типа **(SMTP)** и тип отображения данных **Выбранный период** с настроенным периодом отображения данных **Месяц**, отображается скорость обработки данных почтового трафика, поступающих от почтового сенсора на Central Node, а также количество файлов и URL-адресов, извлеченных из почтового трафика за выбранный месяц.
  Отображаются следующие данные:
- **Средний трафик** – скорость поступления трафика на Central Node зеленым цветом (объектов/сек.).
- **Файлы** – количество извлеченных файлов серым цветом.
- **URL-адреса** – количество извлеченных URL-адресов синим цветом.
- **Не обработано** – количество необработанных объектов вертикальными линиями красного цвета.
  При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость поступления трафика на Central Node и количество обработанных объектов в определенное время.

На виджете **Обработано**, где выбран Sensor типа **(LOAD) Endpoint Agents** и тип отображения данных **Выбранный период** с настроенным периодом отображения данных **Месяц**, отображается количество событий, поступивших от хостов Endpoint Agent на Central Node за выбранный месяц.

При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается количество событий, поступивших в определенное время.

Мониторинг очередей обработки данных модулями и компонентами приложения

На виджете **Очереди** вы можете оценить статус обработки данных модулями приложения YARA, AM Engine, компонентом Sandbox и отследить объем необработанных данных.

Передача данных в очереди измеряется сообщениями.

Вы можете выбрать тип отображения данных в раскрывающемся списке справа от названия виджета **Очереди**:

- **Текущая загрузка** – 5 минут до текущего момента.
- **Выбранный период**. В этом случае вы также можете настроить период отображения данных на виджетах.

В левой части виджета отображается легенда виджета по цветам, которые используются на виджете.

На виджете **Очереди** отображаются следующие данные:

- **Количество сообщений** и **Объем данных**, обработанных модулями и компонентами приложения:
  - **YARA** – синим цветом.
  - **Sandbox** – фиолетовым цветом.
  - **AM Engine** – зеленым цветом.
- **Не обработано** – объем необработанных данных вертикальными линиями красного цвета.

При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается статус обработки данных модулями приложения **YARA**, **AM Engine** и компонентом **Sandbox**, а также объем необработанных данных в определенное время.

Мониторинг обработки данных компонентом Sandbox

На виджете **Время обработки в Sandbox** отображается среднее время, прошедшее от момента отправки данных на один или несколько серверов с компонентом Sandbox (включая время ожидания отправки) до отображения результатов обработки данных компонентом Sandbox в веб-интерфейсе Kaspersky Anti Targeted Attack Platform в выбранный период.

Пример:
Если настроен период отображения данных на виджетах **Месяц**, на виджете **Время обработки в Sandbox** отображаются столбики оранжевого цвета на каждый день месяца.
При наведении курсора мыши на каждый столбик появляется всплывающее окно, в котором отображается среднее время, прошедшее от момента отправки данных на один или несколько серверов с компонентом Sandbox до отображения результатов обработки данных компонентом Sandbox в веб-интерфейсе Kaspersky Anti Targeted Attack Platform в выбранный день.

Вы можете увеличить скорость обработки данных компонентом Sandbox и пропускную способность компонента Sandbox, увеличив количество серверов с компонентом Sandbox и распределив по этим серверам данные, предназначенные для обработки.

Просмотр состояния работоспособности модулей и компонентов приложения

Если в работе модулей и компонентов приложения возникли проблемы, на которые администратору рекомендуется обратить внимание, в верхней части окна раздела **Мониторинг** веб-интерфейса приложения отображается рамка желтого цвета с предупреждениями.

Пользователю с ролью **Администратор** или **Аудитор** доступна информация о работоспособности того сервера Central Node, PCN или SCN, на котором он сейчас работает.

Пользователю с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** или **Аудитор** доступна следующая информация о работоспособности:

- Если вы используете отдельный сервер Central Node, пользователю доступна информация о работоспособности того сервера Central Node, на котором он сейчас работает.
- Если вы используете режим распределенного решения и мультитенантности и пользователь работает на сервере SCN, пользователю доступна информация о работоспособности этого сервера SCN в рамках тех тенантов, к данным которых у него есть доступ.
- Если вы используете режим распределенного решения и мультитенантности и пользователь работает на сервере PCN, пользователю доступна информация о работоспособности этого сервера PCN и всех серверов SCN, подключенных к этому серверу, в рамках тех тенантов, к данным которых у него есть доступ.

Чтобы получить более подробную информацию о работоспособности модулей и компонентов приложения,

по ссылке **Просмотреть сведения** откройте окно **Работоспособность системы**.

В окне **Работоспособность системы** в зависимости от работоспособности модулей и компонентов приложения отображается один из следующих значков:

- Значок OK, если модули и компоненты приложения работают нормально.
- Значок с количеством проблем (например, 1), если обнаружены проблемы, на которые администратору рекомендуется обратить внимание. В этом случае в правой части окна **Работоспособность системы** отображается подробная информация о проблемах.

Окно **Работоспособность системы** содержит разделы:

- **Работоспособность компонентов** – статус работы модулей и компонентов приложения, карантина, а также обновления баз на всех серверах, на которых работает приложение.

  Пример:
  Если базы одного или нескольких компонентов приложения не обновлялись в течение 24 часов, рядом с именем сервера, на котором установлены модули и компоненты приложения, отображается значок !.
  Для решения проблемы убедитесь, что серверы обновлений доступны. Если для соединения с серверами обновлений вы используете прокси-сервер, убедитесь, что на прокси-сервере нет ошибок, связанных с подключением к серверам Kaspersky Anti Targeted Attack Platform.

- **Обработано** – статус приема и обработки входящих данных. Статус формируется на основе следующих критериев:
  - Состояние получения данных с серверов с компонентом Sensor, с сервера или виртуальной машины с почтовым сенсором, с хостов с компонентом Endpoint Agent.
  - Информация о превышении максимально допустимого времени, которое объекты ожидают в очереди на проверку модулями и компонентами приложения.
- **Соединение с серверами** – состояние соединения между сервером PCN и подключенными серверами SCN (отображается, если вы используете режим распределенного решения и мультитенантности).

В случае обнаружения проблем в работоспособности модулей и компонентов приложения, которые вы не можете решить самостоятельно, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Работа с информацией о серверах с компонентами Central Node и Sensor

Информация о серверах с компонентами Central Node и Sensor отображается в разделе **Серверы Sensor** окна веб-интерфейса приложения.

В разделе отображаются карточки компонентов (слева) и карточки сетевых интерфейсов, обнаруженных на этих компонентах (справа от каждого компонента).

Над карточкой компонента Sensor отображается карточка компонента Central Node, к которому подключен Sensor. Если компонент Central Node развернут со встроенным компонентом Sensor, для этого компонента Sensor в карточке отображается имя Embedded Sensor.

Вы можете просматривать карточки компонентов и сетевых интерфейсов.

Просмотр информации о серверах с компонентами Central Node и Sensor

Чтобы просмотреть информацию о компоненте Central Node или Sensor:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.

На вкладке **Параметры** для компонентов Central Node и Sensor отображаются следующие сведения:

- **Статус** – текущий статус компонента в виде значка и текстового описания.
- **Тип узла** – компонент приложения: **Сервер** (компонент Central Node) или **Сенсор** (компонент Sensor).
- **Текущий объем данных программы** – пространство на диске, занятое файлами приложения. Включает в себя установленные файлы и файлы, созданные в процессе работы приложения.
- **Максимально возможный объем данных программы** – пространство на диске, которое могут занять файлы приложения. Включает в себя установленные файлы и сумму всех заданных ограничений по объему в правилах хранения данных. Значение не может превышать объем доступного пространства на диске.
- **Занято на диске** – пространство на диске, занятое всеми файлами. Включает в себя файлы приложения, файлы операционной системы и других приложений. Объем пространства рассчитывается на диске, который содержит директорию /var/ в файловой системе компонента.
- **Свободно на диске** – пространство на диске, не занятое файлами. Объем пространства рассчитывается на диске, который содержит директорию /var/ в файловой системе компонента.
- **Объем диска** – общий объем пространства на диске, который содержит директорию /var/ в файловой системе компонента.

- **BPF-фильтрация** – признак включенной или выключенной фильтрации с использованием технологии BPF (Berkeley Packet Filter) по адресным параметрам в сетевых пакетах.
- **Внешнее хранилище для файлов дампа трафика** – статус подключения внешнего хранилища. Могут отображаться следующие статусы: **Подключено**, **Не подключено**.
- **Правила хранения** – текущие и максимальные значения объема, количества элементов и времени хранения данных приложения.

Для компонента Sensor, кроме вкладки **Параметры**, также отображаются вкладки **Внешнее хранилище**, **Другое**, **ICAP-интеграция**, **POP3-интеграция**, **SMTP-интеграция**.

- На вкладке **Внешнее хранилище** отображается информация о параметрах внешнего хранилища для записи зеркалированного SPAN-трафика.
- На вкладке **Другое** отображается следующая информация:
  - Максимальный размер проверяемого файла – текущее ограничение на размер файлов, проверяемых компонентом.
  - Запись HTTP body – признак включенной или выключенной записи содержимого HTTP-пакета.
- На вкладке **ICAP-интеграция** отображаются параметры интеграции с прокси-сервером по протоколу ICAP.

  В поле **Хост** отображаются URL-адреса служб Response Modification (RESPMOD) и Request Modification (REQMOD) в формате icap://<IP-адрес сервера Central Node, к которому подключен Sensor>:1344/av/<respmod или reqmod>.

  Для настройки интеграции с Kaspersky Anti Targeted Attack Platform скопируйте нужный URL-адрес, замените IP-адрес сервера Central Node на IP-адрес сервера Sensor, для которого вы хотите настроить параметры интеграции по протоколу ICAP, и укажите получившийся URL-адрес в параметрах прокси-сервера, который используется в вашей организации.
- На вкладке **POP3-интеграция** отображаются параметры интеграции с почтовым сервером по протоколу POP3.
- На вкладке **SMTP-интеграция** отображаются параметры интеграции с почтовым сервером по протоколу SMTP.

Просмотр информации о сетевых интерфейсах

На карточке сетевого интерфейса в разделе **Серверы Sensor** веб-интерфейса приложения отображаются следующие сведения:

- Имя сетевого интерфейса.
- MAC-адрес сетевого интерфейса.
- IP-адрес сетевого интерфейса.
- Пропускная способность сетевого интерфейса.
- LED-тест. Эта ссылка позволяет определить Ethernet-порт, связанный с сетевым интерфейсом.

Если на сетевой интерфейс добавлена точка мониторинга, на карточке сетевого интерфейса отображаются следующие сведения о точке мониторинга:

- Имя точки мониторинга.
- **Режим технологий** – состояние функции наследования технологий. Может иметь значение **Включено** или **Выключено**.

Вы можете просмотреть подробную информацию о сетевом интерфейсе.

Чтобы просмотреть подробную информацию о сетевом интерфейсе:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного сетевого интерфейса и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о сетевом интерфейсе.

В карточке сетевого интерфейса отображаются следующие сведения:

- **Сетевой интерфейс** – имя сетевого интерфейса в операционной системе.
- **Подключение** – значок подключения сетевого кабеля к Ethernet-порту сетевого интерфейса:
  - – сетевой кабель подключен;
  - – сетевой кабель отключен.

    Значок мигает при включенном режиме индикации Ethernet-порта.
  - **MAC-адрес** – MAC-адрес сетевого интерфейса.
  - **IP-адрес** – IP-адрес сетевого интерфейса.

    Если на сетевом интерфейсе обнаружено несколько IP-адресов, то в области деталей отображаются не более 16 IP-адресов.

Если на сетевой интерфейс добавлена точка мониторинга, в карточке сетевого интерфейса отображаются следующие сведения:

- **Статус** – текущий статус точки мониторинга в виде значка и текстового описания:
  - *OK*. Точка мониторинга доступна.
  - *Переключение*. Происходит переключение режима работы точки мониторинга.
  - *Ошибка*. Обнаружена ошибка при переключении режима работы точки мониторинга.
- **Подключение** – значок подключения сетевого кабеля к Ethernet-порту сетевого интерфейса:
  - – сетевой кабель подключен;
  - – сетевой кабель отключен.

  Значок мигает при включенном режиме индикации Ethernet-порта.
- **Сетевой интерфейс** – имя сетевого интерфейса в операционной системе.

- **Режим** – текущий режим работы точки мониторинга:
  - *Включена*.
  - *Выключена*.
- На вкладке **Параметры**:
  - **Наследование технологий** – признак включенного или выключенного наследования технологий сервера.
  - **MAC-адрес** – MAC-адрес сетевого интерфейса.
  - **IP-адрес** – IP-адрес сетевого интерфейса.

Определение Ethernet-порта, связанного с сетевым интерфейсом

Сервер, на котором установлены компоненты приложения, может иметь несколько Ethernet-портов для подключения к локальной сети. С помощью приложения вы можете включить режим индикации для сетевого интерфейса и определить, какой Ethernet-порт связан с этим интерфейсом. При включенном режиме индикации рядом с Ethernet-портом в течение 15 секунд мигает LED-индикатор.

Если сетевой интерфейс не поддерживает LED-индикацию (например, рядом с Ethernet-портом отсутствует LED-индикатор или сетевой интерфейс является объединенным логическим интерфейсом), при включении режима индикации отображается ошибка.

Чтобы определить Ethernet-порт, связанный с сетевым интерфейсом:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. В карточке нужного сетевого интерфейса нажмите на кнопку **LED-тест**.

   Если сетевой интерфейс поддерживает LED-индикацию, в карточке сетевого интерфейса начнет мигать значок подключения сетевого кабеля. Одновременно на соответствующем сетевом адаптере компьютера начнет мигать LED-индикатор рядом с Ethernet-портом.

Пока включен режим индикации для одного сетевого интерфейса, вы не можете включить режим индикации для другого сетевого интерфейса на этом же сервере.

Управление серверами Central Node, PCN или SCN с помощью веб-интерфейса приложения

С помощью веб-интерфейса приложения вы можете выполнять следующие действия с сервером, на котором установлен компонент Central Node:

- менять FQDN-имя сервера;
- настраивать дату и время сервера;

- выключать и перезагружать сервер;
- управлять сертификатом сервера;
- управлять параметрами сохранения трафика;
- управлять параметрами сохранения файлов дампа трафика;
- настраивать сетевые параметры сервера.

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Настройка даты и времени сервера

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить дату и время сервера:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Дата и время**.
2. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, в котором находится сервер Central Node.
3. В блоке **NTP-серверы** установите значение параметра **Максимальное время передачи пакета**, который ограничивает максимально возможное время отправки пакета от сервера Central Node до NTP-сервера.

   Значение по умолчанию: 5 секунд.

   Включить или выключить синхронизацию с NTP-серверами можно в меню администратора Central Node.
4. В блоке **NTP-серверы в**ыполните следующие действия
   - Если вы хотите добавить новый NTP-сервер, выполните следующие действия:

     a. Нажмите на кнопку **Добавить**.

     b. В появившемся поле введите IP-адрес или доменное имя NTP-сервера.

     c. Справа от поля нажмите на кнопку ✓.

- Если вы хотите изменить IP-адрес или доменное имя NTP-сервера, в строке с этим сервером нажмите на кнопку .
- Если вы хотите удалить NTP-сервер, в строке с этим сервером нажмите на кнопку .

5. Нажмите на кнопку **Применить**.

Дата и время сервера будут настроены.

Генерация или загрузка TLS-сертификата сервера

Если вы уже используете TLS-сертификат сервера и сгенерируете или загрузите новый сертификат, сертификат, который используется в приложении, будет удален и заменен на новый сертификат.

Вам потребуется указать данные нового сертификата везде, где использовался старый.

Если вы замените TLS-сертификат на новый, вам потребуется:

- Повторно авторизовать почтовые сенсоры (KSMG, KLMS) на Central Node.
- Повторно настроить соединение Central Node, PCN и SCN с Sandbox.
- Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent.

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

Вы можете сгенерировать новый сертификат через веб-интерфейс сервера Central Node или загрузить самостоятельно созданный сертификат.

Для соответствия нормам и стандартам безопасности необходимо заменить TLS-сертификат, установленный в приложении по умолчанию, на ваш TLS-сертификат.

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы сгенерировать TLS-сертификат сервера Central Node:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сертификаты**.

3. В разделе **Сертификат сервера** нажмите на кнопку **Сгенерировать**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Kaspersky Anti Targeted Attack Platform сгенерирует новый TLS-сертификат. Страница автоматически обновится.

Связь с почтовыми сенсорами, компонентом Sandbox, компонентом Endpoint Agent будет прервана до повторной авторизации.

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Anti Targeted Attack Platform.

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.

  Приложение не работает с сертификатами другого формата.

  Если вы подготовили сертификат в другом формате, вам нужно конвертировать его в формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Выполняйте действия по загрузке TLS-сертификат в веб-интерфейсе того сервера, на который вы хотите загрузить сертификат.

Чтобы загрузить самостоятельно подготовленный TLS-сертификат через веб-интерфейс Kaspersky Anti Targeted Attack Platform:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификат сервера** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

4. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Anti Targeted Attack Platform.

Связь с почтовыми сенсорами, компонентом Sandbox, компонентом Endpoint Agent будет прервана до повторной авторизации.

Скачивание TLS-сертификата сервера на компьютер

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы скачать TLS-сертификат сервера на компьютер:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сертификаты**.
2. В разделе **Сертификат сервера** нажмите на кнопку **Скачать**.

   Файл сертификата сервера будет сохранен в папке загрузки браузера.

Назначение FQDN-имени сервера

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы назначить FQDN-имя сервера:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. В поле **Имя сервера (FQDN)** введите полное доменное имя сервера.

   Указывайте имя сервера в формате FQDN (например, `host.domain.com` или `host.domain.subdomain.com`).
3. Нажмите на кнопку **Применить**.

   Имя сервера будет назначено.

Настройка параметров DNS

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить параметры DNS:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. В блоке параметров **Параметры DNS** в поле **DNS-серверы** введите IP-адреса DNS-серверов.
3. Нажмите на кнопку **Применить**.

   Параметры DNS будут настроены.

Настройка параметров сетевого интерфейса

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить параметры сетевого интерфейса:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. Выберите сетевой интерфейс, параметры которого вы хотите настроить.

   Откроется окно **Изменить сетевой интерфейс**.
3. В блоке параметров **Состояние** выберите один из следующих вариантов:
   - **Выключено**.
   - **Включено, используется DHCP-сервер**, если вы хотите, чтобы для сетевого интерфейса использовались параметры, полученные от DHCP-сервера.
   - **Включено, настройка вручную**, если вы хотите, чтобы для сетевого интерфейса использовались параметры, заданные вручную.
4. Если вы выбрали **Включено, настройка вручную**, укажите значения для следующих параметров:
   a. В поле **IP** укажите IP-адрес сетевого интерфейса.
   b. В поле **Маска подсети** укажите маску подсети сетевого интерфейса.
   c. В поле **Шлюз** введите IP-адрес шлюза.
5. Нажмите на кнопку **Сохранить**.

Параметры сетевого интерфейса будут настроены.

Настройка сетевого маршрута для использования по умолчанию

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить сетевой маршрут для использования по умолчанию:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. В блоке параметров **Сетевой маршрут** в раскрывающемся списке **Сетевой интерфейс** выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.

3. В поле **Шлюз** введите IP-адрес шлюза.
4. Нажмите на кнопку **Применить**.

Сетевой маршрут для использования по умолчанию будет настроен.

Настройка параметров соединения с прокси-сервером

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить параметры соединения с прокси-сервером:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. В блоке параметров **Прокси-сервер** переведите переключатель в положение **Включено**.
3. В поле **Хост** укажите URL- или IP-адрес прокси-сервера.
4. В поле **Порт** укажите порт подключения к прокси-серверу.
5. В поле **Имя пользователя** укажите имя пользователя для аутентификации на прокси-сервере.
6. В поле **Пароль** укажите пароль для аутентификации на прокси-сервере.
7. Если вы не хотите использовать прокси-сервер при подключении к локальным адресам, установите флажок **Не использовать прокси-сервер для локальных адресов**.
8. Нажмите на кнопку **Применить**.

Параметры соединения с прокси-сервером будут настроены.

Если при сохранении параметров возникла ошибка, переведите переключатель **Использовать прокси-сервер** в положение **Выключено**, затем верните в положение **Включено** и нажмите на кнопку **Применить**.

Настройка параметров соединения с почтовым сервером

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Приложение может отправлять уведомления об алертах и работе системы. Для этого необходимо настроить параметры сервера для отправки уведомлений.

Чтобы настроить параметры сервера для отправки уведомлений:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на вкладку **Конфигурация почтового сервера**.

3. В поле **Хост** укажите IP-адрес почтового сервера.
4. В поле **Порт** укажите порт подключения к почтовому серверу.
5. В поле **Отправлять с адреса** укажите адрес электронной почты, с которого будут отправляться уведомления.
6. Если вы хотите включить проверку подлинности на почтовом сервере, установите флажок **Использовать SMTP-проверку подлинности получателей сообщений**.
7. В поле **Имя пользователя** укажите имя пользователя для аутентификации на сервере для отправки уведомлений.
8. В поле **Пароль** укажите пароль для аутентификации на сервере для отправки уведомлений.
9. Если вы хотите использовать TLS-шифрование при отправке уведомлений, установите флажок **Использовать TLS-шифрование**.
10. Если вы хотите проверить сертификат почтового сервера, установите флажок **Подтверждать TLS-шифрование**.

    В поле **Отпечаток сертификата** отобразится отпечаток сертификата почтового сервера.

    > Если флажок **Подтверждать TLS-шифрование** не установлен, приложение будет считать любой сертификат почтового сервера доверенным.

11. Нажмите на кнопку **Применить**.

Параметры сервера для отправки уведомлений будут настроены.

Управление параметрами сохранения трафика

Приложение может сохранять трафик, полученный на момент регистрации событий. Трафик сохраняется в базе данных сервера Central Node при регистрации событий, для которых включено сохранение трафика. Также приложение может сохранять трафик в базе данных сервера непосредственно при запросе на загрузку трафика, используя временные файлы дампа трафика.

Приложение сохраняет данные о трафике блоками. Если блок трафика относится к нескольким событиям (когда события регистрируются в коротком промежутке времени), этот блок трафика не дублируется в базе данных.

Чтобы изменить параметры сохранения трафика в базе данных сервера:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента Central Node и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.
3. Нажмите на кнопку **Изменить**.
4. Перейдите на вкладку **Общие**.

5. В блоке параметров **Трафик для событий** задайте максимальный объем сохраняемого трафика в поле **Макс. объем**.

   Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

   При изменении значения параметра вам нужно учитывать, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для сервера.

6. Нажмите на кнопку **Сохранить**.

Параметры сохранения трафика будут изменены.

Управление параметрами сохранения файлов дампа трафика

Приложение сохраняет трафик, полученный через точки мониторинга, в виде файлов дампа трафика. Эти файлы используются приложением для анализа поступающего трафика. Также с помощью этих файлов вы можете выполнять следующие действия в приложении:

- загрузка трафика при работе с картой сетевых взаимодействий;
- загрузка трафика сетевых сеансов;
- загрузка трафика для событий (файлы дампа трафика позволяют загрузить трафик для событий, даже если в соответствующих типах событий выключено сохранение трафика).

Файлы дампа трафика размещаются во внутренних хранилищах на серверах с компонентом Sensor. Если вы используете компонент Central Node со встроенным Sensor, файлы дампа трафика сохраняются во внутреннем хранилище сервера с компонентом Central Node.

Приложение хранит файлы дампа трафика временно. По мере поступления трафика приложение автоматически удаляет из хранилищ самые старые файлы дампа трафика, если общий объем файлов приближается к ограничению, заданному для хранилища. Вы можете настроить параметры сохранения трафика во внутреннем хранилище.

Чтобы настроить параметры сохранения файлов дампа трафика во внутреннем хранилище:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента Central Node и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.

3. Нажмите на кнопку **Изменить**.
4. Перейдите на вкладку **Общие**.

5. При необходимости включите фильтрацию в блоке **Фильтрация сохраняемого трафика** и введите выражение для фильтрации с использованием технологии BPF (Berkeley Packet Filter) по адресным параметрам в сетевых пакетах.

   Фильтрация позволяет сократить объем сохраняемого трафика за счет отбрасывания сетевых пакетов, не удовлетворяющих фильтру. Однако при использовании фильтрации вам нужно учитывать, что приложение может получать в отфильтрованном трафике не все данные, необходимые для качественного анализа трафика. Вам нужно настроить фильтрацию таким образом, чтобы в файлах дампа трафика сохранялись все сетевые пакеты, которые требуются для анализа трафика в соответствии с функциональностью приложения.

6. Перейдите к блоку параметров **Файлы дампа трафика** и задайте ограничение занимаемого объема для хранения файлов дампа трафика с помощью параметра **Макс. объем**.

   Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

   При изменении значения параметра вам нужно учитывать объем и скорость поступления входящего трафика, а также, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для узла.

7. Нажмите на кнопку **Сохранить**.

Параметры сохранения файлов дампа трафика во внутреннем хранилище будут настроены.

Управление компонентом Sensor

Компонент Sensor выполняет прием данных из сетевого и почтового трафика.

Для управления компонентом требуется добавить в приложение лицензионный ключ KATA или KATA+NDR. Если ключ не добавлен, управление компонентом недоступно.

Вы можете установить компоненты Sensor и Central Node на одном сервере или на отдельных серверах. Установленный на отдельном сервере компонент Sensor необходимо подключить к серверу с компонентом Central Node. Если вы используете режим распределенного решения и мультитенантности, выполняйте действия по подключению компонента Sensor на том сервере PCN или SCN, к которому вы хотите подключить компонент.

Централизованное управление компонентами Sensor с PCN в режиме распределенного решения и мультитенантности не предусмотрено. Настройка параметров компонента Sensor осуществляется только с того сервера Central Node, к которому подключен компонент.

Подключение компонента Sensor к Central Node

При добавлении компонента Sensor на Central Node формируется конфигурационный пакет, содержащий сертификат и конфигурационные данные для компонента Sensor. Подключение добавленного компонента выполняется с использованием веб-интерфейса компонента Sensor. Веб-интерфейс компонента позволяет загрузить конфигурационный пакет и подключить компонент следующими способами:

- С помощью файла свертки.

  В этом случае конфигурационный пакет сохраняется в виде файла, в котором сертификат защищен паролем. Этот файл называется *файлом свертки*. Файл свертки требуется загрузить в веб-интерфейс компонента Sensor. После загрузки файла свертки компонент Sensor автоматически подключается к тому компоненту Central Node, на котором был создан файл свертки.

- Автоматически по сети.

  В этом случае конфигурационный пакет передается по сети на указанный IP-адрес сервера с компонентом Sensor. Sensor обрабатывает конфигурационный пакет, формирует на его основе запрос на подпись сертификата (CSR) и отправляет этот запрос компоненту Central Node. После получения запроса на странице веб-интерфейса Kaspersky Anti Targeted Attack Platform отображается отпечаток полученного запроса в виде последовательности символов. Такой же отпечаток запроса в это время отображается и на странице веб-интерфейса компонента Sensor. Вам нужно убедиться в идентичности отпечатков перед завершением подключения.

Если соединение между компонентами Central Node и Sensor устанавливается вне доверенной среды, для защиты соединения от перехвата трафика вам требуется использовать внешние средства криптографической защиты информации (СКЗИ), поддерживающие отечественные алгоритмы шифрования. Если компоненты соединены доверенной средой, например, с помощью патч-корда в рамках серверной стойки без постороннего доступа, вам не требуется использовать внешние СКЗИ.

Подключение компонента Sensor с помощью файла свертки

Чтобы подключить компонент Sensor с помощью файла свертки:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

2. Нажмите на кнопку **Добавить сенсор**.

   Откроется окно **Добавление нового сенсора**.

3. В поле **Имя сенсора** введите имя для компонента Sensor, который вы хотите подключить.

   После подключения к Central Node в имени вкладки браузера со страницей веб-интерфейса компонента будет отображаться имя, заданное на этом шаге.

4. В поле **Адрес Сервера** введите IP-адрес сервера Central Node, к которому вы хотите подключить компонент Sensor.

   Если Central Node развернут в виде кластера, вам нужно ввести IP-адрес обрабатывающего сервера кластера, для которого **настроено получение зеркалированного трафика со SPAN-портов**.

   Вы можете включить получение зеркалированного трафика при установке компонента. Если вы отказались от получения трафика на этапе установки, выполните шаги инструкции ниже.

Чтобы включить получение зеркалированного трафика со SPAN-портов:

1. Если Central Node установлен на сервере, войдите в консоль управления этим сервером по протоколу SSH или через терминал.

2. Если Central Node развернут в виде кластера, войдите в консоль управления любым из обрабатывающих серверов кластера по протоколу SSH или через терминал.

3. Выполните команду:

   ```
   kata-enable-span
   ```

   Получение зеркалированного трафика со SPAN-портов будет включено.

5. В поле **IP-адрес сенсора** введите IP-адрес сервера с компонентом Sensor, который вы хотите подключить к компоненту Central Node.

6. В разделе **Шифрование сертификата в файле свертки** укажите пароль, который будет использоваться для защиты сертификата.

   Пароль должен удовлетворять следующим требованиям:

   - содержит от 8 до 256 символов ASCII;
   - содержит одну или несколько прописных букв латинского алфавита;
   - содержит одну или несколько строчных букв латинского алфавита;
   - содержит одну или несколько цифр;
   - содержит не более трех одинаковых символов подряд.

7. Нажмите на кнопку **Создать файл свертки**. Браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

8. Поместите сохраненный файл свертки на любой компьютер, на котором разрешен доступ к серверу Sensor.

9. На компьютере, на который вы поместили файл свертки, запустите интерпретатор командной строки.

10. Выполните команду:

    ```
    ssh -4 -L 9444:localhost:9444 admin@<IP-адрес сервера Sensor>
    ```

    Если после выполнения команды отобразилась ошибка *Corrupted MAC on input. ssh_dispatch_run_fatal: Connection to <IP-адрес сервера Sensor> port 22: message authentication code incorrect*, выполните следующую команду:

    ```
    ssh -4 -L 9444:localhost:9444 admin@<IP-адрес сервера Sensor> -o "MACs hmac-sha2-256"
    ```

11. В адресной строке браузера введите: https://localhost:9444.

12. На странице веб-интерфейса Sensor нажмите на кнопку **Выберите файл**.

    Откроется стандартное окно используемого браузера для выбора файла.

13. Укажите путь к файлу свертки.

14. Нажмите на кнопку открытия файла.

15. После загрузки содержимого файла введите пароль для доступа к сертификату, заданный на шаге 6 этой инструкции.

    Компонент Sensor будет подключен к компоненту Central Node, после чего на страницах веб-интерфейсов компонентов Sensor и Central Node отобразятся сведения о подключении.

Добавление и подключение компонента Sensor автоматически по сети

Чтобы подключить компонент Sensor автоматически по сети:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

2. Нажмите на кнопку **Добавить сенсор**.

   Откроется окно **Добавление нового сенсора**.

3. Перейдите на вкладку **Автоматически по сети**.

4. В поле **Имя сенсора** введите имя для компонента Sensor, который вы хотите подключить.

   После подключения к Central Node в имени вкладки браузера со страницей веб-интерфейса компонента будет отображаться имя, заданное на этом шаге.

5. В поле **Адрес Сервера** введите IP-адрес сервера Central Node, к которому вы хотите подключить компонент Sensor.

   Если Central Node развернут в виде кластера, вам нужно ввести IP-адрес обрабатывающего сервера кластера, для которого **настроено получение зеркалированного трафика со SPAN-портов**.

   Вы можете включить получение зеркалированного трафика при установке компонента. Если вы отказались от получения трафика на этапе установки, выполните шаги инструкции ниже.

   Чтобы включить получение зеркалированного трафика со SPAN-портов:

   1. Если Central Node установлен на сервере, войдите в консоль управления этим сервером по протоколу SSH или через терминал.

   2. Если Central Node развернут в виде кластера, войдите в консоль управления любым из обрабатывающих серверов кластера по протоколу SSH или через терминал.

   3. Выполните команду:

      ```
      kata-enable-span
      ```

      Получение зеркалированного трафика со SPAN-портов будет включено.

6. В поле **IP-адрес сенсора** введите IP-адрес сервера с компонентом Sensor, который вы хотите подключить к компоненту Central Node.

   Приложение установит соединение с сервером, на котором установлен компонент Sensor, на странице веб-интерфейса приложения появится запрос для подтверждения полученного отпечатка запроса на подпись сертификата.

7. На любом компьютере, на котором разрешен доступ к серверу Sensor, запустите интерпретатор командной строки.

8. Выполните команду:

   ```
   ssh -4 -L 9444:localhost:9444 admin@<IP-адрес сервера Sensor>
   ```

Если после выполнения команды отобразилась ошибка *Corrupted MAC on input. ssh_dispatch_run_fatal: Connection to <IP-адрес сервера Sensor> port 22: message authentication code incorrect*, выполните следующую команду:

```
ssh -4 -L 9444:localhost:9444 admin@<IP-адрес сервера Sensor> -o "MACs hmac-sha2-256"
```

9. В адресной строке браузера введите: https://localhost:9444.

   В окне браузера откроется страница веб-интерфейса компонента Sensor. На странице веб-интерфейса отобразится сообщение, содержащее информацию об отпечатке запроса сертификата, который был отправлен компоненту Central Node.

10. Убедитесь в идентичности последовательностей символов, представляющих отпечаток запроса сертификата на страницах веб-интерфейсов компонентов Sensor и Central Node.

11. На странице веб-интерфейса приложения нажмите на кнопку подтверждения полученного отпечатка запроса сертификата.

Компонент Sensor будет подключен к компоненту Central Node, после чего на страницах веб-интерфейсов компонентов Sensor и Central Node отобразятся сведения о подключении.

Удаление компонента Sensor

Вы можете удалить компонент из приложения. Так как при удалении компонента также удаляются параметры настроенных для него интеграций и останавливаются прием и обработка данных, мы рекомендуем предварительно выполнить следующие действия:

- Запланировать окно простоя.
- Отключить все интеграции с Sensor на стороне внешних систем.
- Сохранить параметры интеграций с внешними системами на стороне Sensor любым удобным для вас способом.
- Сохранить параметры интеграций с Sensor на стороне внешних систем любым удобным для вас способом.

При необходимости вы можете снова подключить удаленный компонент к Central Node.

Чтобы удалить компонент:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.

3. Нажмите на кнопку **Удалить**.

Компонент будет удален.

Изменение параметров Sensor, установленного отдельно от Central Node

Если вы выбрали сетевые протоколы для получения зеркалированного трафика со SPAN-портов, настроили размер файлового хранилища или пропускную способность при захвате трафика на отдельном Sensor **до** подключения его к Central Node и хотите изменить эти параметры **после** подключения, мы рекомендуем использовать следующий сценарий по изменению этих параметров:

1. Отключение Sensor от Central Node.

   Отключение Sensor производится путем удаления компонента.

2. Подготовка Sensor к изменению параметров.

3. Выполнение инструкций для их изменения.

4. Подключение Sensor к Central Node.

После изменения одного или нескольких указанных параметров без предварительной подготовки работа Sensor, установленного отдельно от Central Node, может стать нестабильной. В этом случае статус компонента в его карточке часто меняется. Вы можете устранить проблему, отключив Sensor от Central Node и затем подключив его снова.

Подготовка к изменению параметров Sensor, установленного отдельно от Central Node

Если вы выбрали сетевые протоколы для получения зеркалированного трафика со SPAN-портов, размер файлового хранилища или пропускную способность при захвате трафика на отдельном Sensor **до** подключения его к Central Node и хотите изменить эти параметры **после** подключения, вам нужно выполнить шаги инструкции, приведенной ниже.

Все описанные ниже действия выполняются на серверах в режиме Technical Support Mode после повышения привилегий пользователя с помощью команды `sudo -i`.

Чтобы подготовить Sensor к изменению параметров:

1. Войдите в консоль этого сервера Sensor и выполните команду:

   ```
   kata-sensor-tool stop-sensor
   ```

2. Войдите в консоль управления сервера Central Node,к которому подключен Sensor, и выполните команду:

   ```
   kata-sensor-tool clear-core-cookies
   ```

3. Вернитесь в консоль управления сервера Sensor и выполните команду:

   ```
   kata-sensor-tool start-sensor
   ```

   Sensor будет подготовлен к изменению параметров. Вы можете выполнить шаги инструкций для их изменения.

Управление сертификатом сервера Sensor

В этом разделе содержится информация об управлении TLS-сертификатом сервера с компонентом Sensor.

Управление сертификатом осуществляется в меню администратора приложения.

Генерация TLS-сертификата сервера Sensor в меню администратора сервера Sensor

Чтобы сгенерировать TLS-сертификат сервера с компонентом Sensor, выполните следующие действия в меню администратора сервера с компонентом Sensor:

1. В главном окне меню администратора выберите пункт **Program settings**.
2. Нажмите на клавишу **ENTER**.

   Откроется следующее окно меню администратора.
3. Выберите пункт **Manage server certificate**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Certificate management**.
5. В нижней части окна выберите пункт **Generate new**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно с информацией о новом сертификате.
7. Нажмите на кнопку **Generate**.

   Начнется создание сертификата. Дождитесь окончания этого процесса.

Сертификат будет создан. Данные сертификатов, установленных ранее, будут перезаписаны.

Загрузка самостоятельно подготовленного TLS-сертификата через меню администратора сервера Sensor

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его на сервер Sensor по протоколу SCP. Подробнее о способах загрузки файлов по протоколу SCP см. в документации к операционной системе, установленной на том компьютере, с которого вы хотите загрузить TLS-сертификат.

Файл TLS-сертификата, предназначенный для загрузки на сервер, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.

- Имя файла должно быть kata.pem.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Чтобы загрузить самостоятельно подготовленный TLS-сертификат на сервер Sensor по протоколу SCP, выполните следующие действия в интерфейсе работы по протоколу SCP вашего компьютера (на примере операционной системы Linux):

1. Выполните команду `scp kata.pem admin@<IP-адрес сервера с компонентом Sensor>:`
2. На приглашение ввести пароль введите пароль администратора для работы в меню администратора сервера Sensor, заданный при установке.

TLS-сертификат будет загружен на сервер Sensor.

Чтобы применить загруженный TLS-сертификат на сервере Sensor, выполните следующие действия в меню администратора сервера Sensor:

1. В главном окне меню администратора выберите пункт **Program settings**.
2. Нажмите на клавишу **ENTER**.

   Откроется следующее окно меню администратора.
3. Выберите пункт **Manage server certificate**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Certificate management**.
5. В нижней части окна выберите пункт **Install from file**.
6. Нажмите на клавишу **ENTER**.

Сертификат будет применен. Данные сертификатов, установленных ранее, будут перезаписаны.

Скачивание TLS-сертификата сервера Sensor на компьютер

Вы можете скачать TLS-сертификат с сервера Sensor на любой компьютер, имеющий доступ к серверу с компонентом Sensor, по протоколу SCP. Подробнее о способах загрузки файлов по протоколу SCP см. в документации к операционной системе, установленной на том компьютере, на который вы хотите скачать TLS-сертификат.

Чтобы скачать TLS-сертификат с сервера с компонентом Sensor по протоколу SCP, выполните следующие действия в интерфейсе работы по протоколу SCP вашего компьютера (на примере операционной системы Linux):

1. Выполните команду `scp admin@<IP-адрес сервера с компонентом Sensor>:ssl/kata.crt.`
2. На приглашение ввести пароль введите пароль администратора для работы в меню администратора сервера с компонентом Sensor, заданный при установке.

TLS-сертификат будет загружен с сервера с компонентом Sensor в текущую директорию.

Изменение имени сервера

Чтобы изменить имя сервера Central Node:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.
3. Нажмите на кнопку **Изменить**.
4. Перейдите на вкладку **Общие**.
5. В поле **Имя сенсора** введите новое имя.

   Имя должно быть уникальным (не совпадать с именами других компонентов) и может содержать не более 100 символов. Вы можете использовать буквы латинского алфавита, цифры, пробел, а также специальные символы _ и - (например, Server_1). Имя должно начинаться и заканчиваться любым допустимым символом, кроме пробела.
6. Нажмите на кнопку **Сохранить**.

Имя сервера будет изменено.

Управление точками мониторинга

Для получения и обработки зеркалированного SPAN-трафика в Kaspersky Anti Targeted Attack Platform используются точки мониторинга. Точки мониторинга можно добавлять и удалять для компонентов Central Node и Sensor.

Каждая точка мониторинга должна быть связана с сетевым интерфейсом, на который поступает копия трафика из определенного сегмента сети. Для добавления точек мониторинга вы можете использовать сетевые интерфейсы, которые удовлетворяют следующим условиям:

- Тип сетевого интерфейса: Ethernet.
- MAC-адрес: отличается от 00:00:00:00:00:00.
- Сетевой интерфейс предназначен для получения копии трафика и этот интерфейс не используется в других целях (например, для соединения серверов с установленными компонентами приложения).

Точки мониторинга можно включать и выключать. Вы можете выключить точку мониторинга, чтобы временно прекратить наблюдение за сегментом сети, из которого поступает копия трафика на сетевой интерфейс. Как только вам потребуется продолжить наблюдение, вы можете включить точку мониторинга.

После выключения или удаления точки мониторинга приложение в течение некоторого времени может регистрировать события, в которых указана эта точка мониторинга. Это связано с возможной задержкой обработки поступившего трафика во время высокой загруженности компонента Central Node.

Подробная информация о точке мониторинга отображается в карточке сетевого интерфейса, к которому привязана эта точка мониторинга. При необходимости вы можете переименовать точку мониторинга.

Добавление точки мониторинга

Для получения и обработки трафика, поступающего из сети на сетевой интерфейс узла, вам нужно добавить точку мониторинга на этот сетевой интерфейс.

Чтобы добавить точку мониторинга на сетевой интерфейс:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. В карточке нужного сетевого интерфейса нажмите на ссылку **Добавить точку мониторинга**.

   Откроется окно добавления точки мониторинга.
3. В поле **Имя точки мониторинга** введите имя точки мониторинга.

   Вы можете использовать прописные и строчные буквы латинского алфавита, цифры, символы _ и -.

   Имя точки мониторинга должно удовлетворять следующим требованиям:

   - является уникальным (не присвоено другой точке мониторинга);
   - содержит от 1 до 100 символов.
4. Нажмите на кнопку **Добавить точку мониторинга**.

Точка мониторинга будет добавлена.

Переименование точки мониторинга

Вы можете переименовать точку мониторинга, связанную с сетевым интерфейсом.

> Новое имя точки мониторинга появится в событиях, зарегистрированных после ее переименования. В ранее зарегистрированных событиях отображается старое имя точки мониторинга.

Чтобы переименовать точку мониторинга:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного сетевого интерфейса и нажмите на нее левой кнопкой мыши.
3. Откроется окно с информацией о сетевом интерфейсе.
4. Нажмите на кнопку **Изменить**.
5. В поле **Имя точки мониторинга** введите новое имя.

   Вы можете использовать прописные и строчные буквы латинского алфавита, цифры, символы _ и -.

Имя точки мониторинга должно удовлетворять следующим требованиям:

- является уникальным (не присвоено другой точке мониторинга);
- содержит от 1 до 100 символов.

6. Нажмите на кнопку **Сохранить**.

Точка мониторинга будет переименована.

Включение точек мониторинга

Приложение не получает и не обрабатывает трафик, поступающий на сетевой интерфейс выключенной точки мониторинга. Вам нужно включить точку мониторинга, если вы хотите возобновить получение и обработку трафика.

Вы можете включать точки мониторинга как по отдельности, так и одновременно для одного компонента или всех компонентов.

Включать точки мониторинга могут только пользователи с ролью Администратор.

Чтобы включить точки мониторинга:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Выполните одно из следующих действий:
   - Если вы хотите включить одну точку мониторинга, в карточке нужного компонента нажмите на кнопку **Включить**. Кнопка доступна, если точка мониторинга выключена.
   - Если вы хотите включить все точки мониторинга для компонента, в карточке нужного компонента нажмите на кнопку **Включить все**. Кнопка доступна, если для компонента есть сетевые интерфейсы с выключенными точками мониторинга.
   - Если вы хотите включить все точки мониторинга для всех компонентов, воспользуйтесь ссылкой **Включить на всех узлах** в панели инструментов.
3. Дождитесь применения изменений.

Выбранные точки мониторинга будут включены.

Выключение точек мониторинга

Вы можете выключить точку мониторинга, если требуется временно приостановить получение и обработку трафика на сетевом интерфейсе этой точки мониторинга.

Вы можете выключать точки мониторинга как по отдельности, так и одновременно для всех компонентов.

Чтобы выключить точки мониторинга:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Выполните одно из следующих действий:
   - Если вы хотите выключить одну точку мониторинга, в карточке нужного компонента нажмите на кнопку **Выключить**. Кнопка доступна, если точка мониторинга включена.
   - Если вы хотите выключить все точки мониторинга для компонента, в карточке нужного компонента нажмите на кнопку **Выключить все**. Кнопка доступна, если для компонента есть сетевые интерфейсы с включенными точками мониторинга.
   - Если вы хотите выключить все точки мониторинга для всех компонентов, воспользуйтесь ссылкой **Выключить на всех узлах** в панели инструментов.
3. Дождитесь применения изменений.

Выбранные точки мониторинга будут выключены.

Удаление точки мониторинга

Вы можете удалить точку мониторинга, связанную с сетевым интерфейсом. Удаление точки мониторинга может потребоваться, если этот сетевой интерфейс больше не будет использоваться для получения трафика.

В случае, если требуется временно приостановить получение трафика на сетевом интерфейсе точки мониторинга (например, на время проведения профилактических и пусконаладочных работ), вы можете выключить точку мониторинга, не удаляя ее.

> В базе данных не удаляется трафик, полученный с точки мониторинга до ее удаления. Также информация об этой точке мониторинга сохраняется в таблице зарегистрированных событий.

Чтобы удалить точку мониторинга:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного сетевого интерфейса и нажмите на нее левой кнопкой мыши.
3. Откроется окно с информацией о сетевом интерфейсе.
4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения. Если точка мониторинга включена, приложение предложит выключить точку мониторинга.
5. В окне запроса подтвердите удаление точки мониторинга.

Точка мониторинга будет удалена.

Настройка максимального размера проверяемого файла

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить максимальный размер проверяемого файла:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.
3. Нажмите на кнопку **Изменить**.
4. Перейдите на вкладку **Другое**.
5. Переведите переключатель **Задать ограничение по размеру** в положение **Включено**.
6. В поле **Ед. изм.** выберите единицу измерения.
7. В поле **Объем** введите максимально допустимый размер файла.
8. Нажмите на кнопку **Сохранить**.

   Максимальный размер проверяемого файла будет настроен.

Если вы хотите задать максимальный размер для проверяемого файла более 100 МБ, выполните следующие действия:

1. Войдите в консоль управления сервером Sensor по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке компонента.
3. Отобразится меню администратора компонента приложения.
4. Выберите режим Technical Support Mode.
5. Нажмите на клавишу ENTER.
6. Отобразится окно подтверждения входа в режим Technical Support Mode.
7. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите Yes и нажмите на клавишу ENTER.
8. Для просмотра текущего ограничения на размер проверяемого файла выполните следующую команду:

```
docker exec $(docker ps -q -f name=nta_core) grep body-limit
/var/opt/kaspersky/kics4net/ids/client/templates/suricata.yaml.templ | grep -v '#'
```

9. Текущее ограничение отображается в полях request-body-limit и response-body-limit. Значение текущего ограничения отображается в байтах.

10. Чтобы изменить текущий лимит, выполните следующую команду:

    ```
    exec $(docker ps -q -f name=nta_core) sed -i 's/<предыдущее значение в байтах>/<новое значение в байтах>/'
    /var/opt/kaspersky/kics4net/ids/client/templates/suricata.yaml.templ
    ```

11. Выполните шаги 1 - 8 приведенной выше инструкции.

Вы можете задать максимальный размер для проверяемого файла более 100 МБ.

Настройка максимального размера проверяемого файла на сервере с компонентом Sensor, установленным отдельно от Central Node

Если вы выбрали сетевые протоколы для получения зеркалированного трафика со SPAN-портов на отдельном Sensor до подключения его к Central Node и хотите изменить эти параметры после подключения, вам нужно выполнить шаги по подготовке к изменению параметров и затем инструкции, приведенные выше.

Настройка записи содержимого HTTP-пакета

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить запись содержимого HTTP-пакета:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

2. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.

3. Нажмите на кнопку **Изменить**.

4. Перейдите на вкладку **Другое**.

5. В разделе **Запись HTTP body** выполните следующие действия:

   - Если вы хотите включить запись содержимого HTTP-пакета, переведите переключатель **Включить параметр http-body** в положение **Включено**.

     По умолчанию переключатель находится в положении **Выключено**.

   - Если вы хотите отключить запись содержимого HTTP-пакета, переведите переключатель **Включить параметр http-body** в положение **Выключено**.

6. Нажмите на кнопку **Сохранить**.

Запись содержимого HTTP-пакета будет включена или выключена.

Настройка интеграции с почтовым сервером по протоколу SMTP

SMTP-трафик может поступать в Kaspersky Anti Targeted Attack Platform двумя способами: в составе зеркалированного SPAN-трафика или при интеграции с почтовым сервером по протоколу SMTP. Если SMTP-трафик поступает в составе SPAN-трафика, приложение извлекает и проверяет только вложенные файлы. Содержимое письма, включая тело сообщения и URL-адреса, в этом случае недоступно для анализа.

Для проверки всех элементов письма вам нужно настроить интеграцию с почтовым сервером по протоколу SMTP.

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить интеграцию с почтовым сервером по протоколу SMTP:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.
3. Нажмите на кнопку **Изменить**.
4. Перейдите на вкладку **SMTP-интеграция**.
5. Если вы хотите включить интеграцию с почтовым сервером по протоколу SMTP, переведите переключатель **Включить SMTP-интеграцию** в положение **Включено**.
6. В поле **Домены назначения** укажите имя почтового домена или поддомена. Приложение будет проверять сообщения электронной почты, отправленные на почтовые ящики указанных доменов.

   Чтобы отключить домен или поддомен, заключите его в форму `!domain.tld`.

   Если вы оставите имя почтового домена пустым, приложение будет принимать сообщения, отправленные на любые адреса электронной почты.
7. В поле **Клиенты** укажите IP-адреса хостов и/или маски подсетей в нотации CIDR, с которыми приложению разрешено взаимодействовать по протоколу SMTP.

   Чтобы отключить хост или подсеть, заключайте адрес в форму `!host`.

   Если вы оставите это поле пустым, приложение будет принимать следующие сообщения:

   - с любых адресов электронной почты, если вы указали почтовые домены в поле **Домены назначения**;
   - от любого хоста, если в поле **Домены назначения** не указан ни один домен.

   Если вы хотите оставить поля **Домены назначения** и **Клиенты** пустыми, вам требуется ограничить список хостов, которым будет доступна отправка сообщений приложению, любым доступным способом.

8. Если вы хотите установить максимально допустимый размер входящих сообщений, переведите переключатель **Задать размер сообщения** в положение **Включено**.

9. В поле **Ед. изм.** выберите единицу измерения.

10. В поле **Объем** введите максимально допустимый размер файла.

11. Если вы хотите настроить TLS-шифрование соединений с почтовым сервером по протоколу SMTP, в блоке **Режим TLS-безопасности клиента** выберите один из следующих вариантов:

    - **Не использовать TLS-шифрование**.

      Приложение не будет устанавливать TLS-шифрование соединений с почтовым сервером.

    - **Проверять возможность TLS-шифрования входящих сообщений**.

      Приложение будет поддерживать TLS-шифрование соединений, но шифрование не будет являться обязательным.

    - **Требовать TLS-шифрование входящих сообщений**.

      Приложение будет принимать сообщения только по зашифрованным каналам.

12. Нажмите на кнопку **Скачать TLS-сертификат**, чтобы сохранить TLS-сертификат сервера с компонентом Sensor на компьютере в папке загрузки браузера.

    Этот сертификат необходим для проверки подлинности на почтовом сервере.

13. В блоке **Запрос клиентского TLS-сертификата** выберите один из следующих вариантов:

    - **Не запрашивать**.

      Приложение не будет проверять TLS-сертификат почтового сервера.

    - **Запрашивать**.

      Приложение будет запрашивать у почтового сервера TLS-сертификат при его наличии.

    - **Требовать**.

      Приложение будет принимать сообщения только от тех почтовых серверов, у которых есть TLS-сертификат.

14. Нажмите на кнопку **Сохранить**.

Интеграция с почтовым сервером по протоколу SMTP будет настроена. Приложение будет проверять сообщения электронной почты, полученные по протоколу SMTP, согласно заданным параметрам.

Если вы развернули компоненты Central Node и Sensor в виде кластера, вы можете настроить отказоустойчивую интеграцию с почтовым сервером.

Чтобы настроить отказоустойчивую интеграцию с почтовым сервером:

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.

2. В параметрах почтового сервера укажите это доменное имя.

   Интеграция с почтовым сервером будет настроена по доменному имени. Почтовый сервер обратится к случайному серверу кластера. При отказе этого сервера почтовый сервер будет обращаться к другому работоспособному серверу кластера.

Для кластерной конфигурации версии 7.0 при интеграции с почтовым сервером может возникать ошибка отправки сообщений электронной почты "451 4.3.0 Error: queue file write error".

Чтобы устранить ошибку:

1. Войдите в консоль управления любого сервера кластера по протоколу SSH или через терминал.

2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке компонента.

   Отобразится меню администратора компонента приложения.

3. В меню администратора приложения выберите режим Technical Support Mode.

4. Нажмите на клавишу ENTER.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите Yes и нажмите на клавишу ENTER.

6. Выполните команду:

   ```
   for addr in <IP-адреса серверов кластера (указываются через пробел)>; do nc -zv $addr 10025; done
   ```

   В консоли отобразится список серверов.

7. Войдите в веб-интерфейс приложения и на шаге 7 приведенной выше инструкции укажите IP-адрес сервера, для которого в консоли отобразилась запись `localhost [127.0.0.1] 10025 (?) open`.

   Ошибка будет устранена.

Если запись `localhost [127.0.0.1] 10025 (?) open` не отобразилась ни для одного сервера кластера, обратитесь в Службу технической поддержки.

При установке компонента Central Node версии 7.0.3 на сервере Kaspersky Anti Targeted Attack Platform может не принимать на обработку сообщения электронной почты, поступившие по протоколу SMTP. Для отправляющей стороны при этом может отображаться ошибка "Connection refused".

Чтобы устранить ограничение:

1. Войдите в консоль управления нужного сервера Central Node по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке компонента.

   Отобразится меню администратора компонента приложения.
3. В меню администратора приложения выберите режим Technical Support Mode.
4. Нажмите на клавишу ENTER.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите Yes и нажмите на клавишу ENTER.
6. Выполните команду:

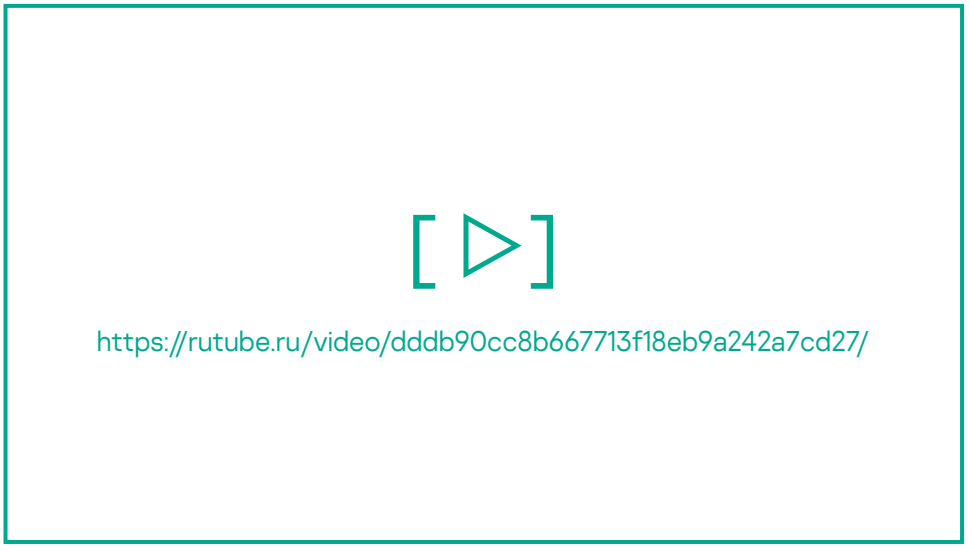
   ```
   sudo -i
   ```
7. Выполните следующие команды:

   a. `docker exec $(docker ps -q -f name=preprocessor_span) supervisorctl restart preprocessor`

   b. `docker exec $(docker ps -q -f name=preprocessor_smtp) supervisorctl restart preprocessor`

Ограничение будет устранено.

Посмотрите обучающее видео о настройке Central Node для работы с почтовым трафиком и интеграции с Kaspersky Secure Mail Gateway. Для воспроизведения видео вы можете запустить его на странице справки (см. ниже) или перейти по ссылке https://rutube.ru/video/dddb90cc8b667713f18eb9a242a7cd27/?playlist=891497.



Настройка Central Node для работы с почтовым трафиком, интеграция с Kaspersky Secure Mail Gateway

Настройка интеграции с прокси-сервером по протоколу ICAP

Интеграция с прокси-сервером по протоколу ICAP с обратной связью позволяет вам предотвратить попадание вредоносных объектов в локальную сеть организации и ограничить переход на вредоносные или фишинговые веб-сайты пользователям хоста. Kaspersky Anti Targeted Attack Platform выступает в роли ICAP-сервера, а ваш прокси-сервер – в роли ICAP-клиента. В процессе работы прокси-сервер передает запросы по протоколу ICAP на ICAP-сервер. ICAP-сервер выполняет проверку и возвращает результат на прокси-сервер. В случае обнаружения угроз пользователю хоста отобразится HTML-страница оповещения.

При интеграции с прокси-сервером по протоколу ICAP действует ряд ограничений.

В случае возникновения проблем с отсутствием свободного дискового пространства при интеграции по протоколу ICAP, обратитесь в Службу технической поддержки.

Включение и отключение интеграции с прокси-сервером по протоколу ICAP

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

При использовании отдельного прокси-сервера Kaspersky Anti Targeted Attack Platform не обеспечивает шифрование ICAP-трафика и аутентификацию ICAP-клиентов по умолчанию. Администратору приложения необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером и Kaspersky Anti Targeted Attack Platform с помощью туннелирования трафика или средствами iptables.

Чтобы включить или отключить интеграцию с прокси-сервером по протоколу ICAP:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.
3. Нажмите на кнопку **Изменить**.
4. Перейдите на вкладку **ICAP-интеграция**.
5. Выполните следующие действия:

   - Если вы хотите включить интеграцию с прокси-сервером по протоколу ICAP, переведите переключатель **Включить ICAP-интеграцию** в положение **Включено**.
   - Если вы хотите отключить интеграцию с прокси-сервером по протоколу ICAP, переведите переключатель **Включить ICAP-интеграцию** в положение **Выключено**.

Интеграция с прокси-сервером по протоколу ICAP будет настроена.

Если вы развернули компоненты Central Node и Sensor в виде кластера, вы можете настроить отказоустойчивую интеграцию с прокси-сервером.

Чтобы настроить отказоустойчивую интеграцию с прокси-сервером:

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.
2. В параметрах прокси-сервера укажите это доменное имя.

   Интеграция с прокси-сервером будет настроена по доменному имени. Прокси-сервер обратится к случайному серверу кластера. При отказе этого сервера прокси-сервер будет обращаться к другому работоспособному серверу кластера.

Включение и отключение проверки ICAP-трафика в режиме реального времени

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Включение и отключение проверки ICAP-трафика в режиме реального времени доступно, если включена интеграция с прокси-сервером по протоколу ICAP.

Если проверка ICAP-трафика в режиме реального времени включена, Kaspersky Anti Targeted Attack Platform передает информацию о проверенных объектах ICAP-клиенту в режиме реального времени. Это позволяет предотвратить скачивание вредоносных объектов и переход по недоверенным ссылкам.

Чтобы включить или отключить проверку ICAP-трафика в режиме реального времени:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.
3. Нажмите на кнопку **Изменить**.
4. Перейдите на вкладку **ICAP-интеграция**.
5. В блоке параметров **Проверка в режиме реального времени** выберите один из следующих вариантов:

   - **Выключено**.

     При выборе этого варианта проверка ICAP-трафика в режиме реального времени будет отключена. По умолчанию выбран этот вариант.

   - **Включено, стандартная проверка трафика ICAP**.

     При включении этого типа проверки репутация файлов и URL-адресов проверяется в базе знаний Kaspersky Security Network, файлы проверяются компонентом Sandbox и модулями Anti-Malware Engine и YARA. Во время проверки компонентом Sandbox файлы будут доступны.

- **Включено, усиленная проверка трафика ICAP**.

  При включении этого типа проверки репутация файлов и URL-адресов проверяется в базе знаний Kaspersky Security Network, файлы проверяются компонентом Sandbox и модулями Anti-Malware Engine и YARA. Во время проверки компонентом Sandbox файлы не будут доступны.

6. В разделе **Извлечение имени пользователя** выполните следующие действия:

   Если вы хотите извлекать имя пользователя с ICAP-сервера, переведите переключатель **Извлекать имя** в положение **Включено**. Если вам необходимо использовать декодирование Base64, установите флажок **Использовать декодирование Base64**.

7. Нажмите на кнопку **Сохранить**.

Проверка ICAP-трафика в режиме реального времени будет включена или отключена.

При отключении интеграции с прокси-сервером проверка ICAP-трафика также отключается, даже если ранее она была включена. При этом параметры проверки сохраняются, и при следующем включении интеграции с прокси-сервером проверка ICAP-трафика будет включена.

Для оптимизации нагрузки приложение может временно переключиться из режима усиленной проверки ICAP-трафика в режим стандартной проверки. В этом случае файлы, полученные из ICAP-трафика и отправленные на проверку в Sandbox, остаются доступными для скачивания. При обнаружении угрозы в проверенных файлах приложение создает алерт. Проверка файлов модулями Anti-Malware Engine и YARA продолжает работать в штатном режиме.

Настройка параметров проверки ICAP-трафика в режиме реального времени

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Настройку параметров проверки ICAP-трафика в режиме реального времени на отдельных серверах с установленным компонентом Sensor можно выполнить только в режиме Technical Support Mode. Для выполнения действий в режиме Technical Support Mode вам рекомендуется обратиться в Службу технической поддержки.

Вы можете настроить параметры проверки ICAP-трафика на сервере с установленными компонентами Central Node и Sensor в режиме реального времени для антивирусной проверки данных. Результаты проверки будут отображаться пользователю хоста на HTML-странице уведомления.

Чтобы настроить параметры проверки ICAP-трафика в режиме реального времени:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Проверка трафика ICAP**.

   Отобразится страница с параметрами проверки ICAP-трафика.

По умолчанию в блоке параметров **Уведомления** загружены страницы, соответствующие следующим событиям:

- В поле **Блокировка ссылки** загружена страница, которая будет отображаться в случае обнаружения угрозы по запрашиваемому пользователем адресу.
- В поле **Блокировка файла** загружена страница, которая будет отображаться в случае обнаружения угрозы в проверяемом файле.

По умолчанию в Kaspersky Anti Targeted Attack Platform загружены HTML-страницы из комплекта поставки. Вы можете загрузить свои страницы уведомлений и настроить их отображение. Максимальный размер страницы уведомления не должен превышать 1,5 МБ. В случае загрузки страницы уведомления размером более 1,5 МБ отобразится ошибка.

2. В блоке параметров **Порог блокировки файлов** в поле **Важность алерта Sandbox** выберите значение из раскрывающегося списка. Значения соответствуют возможному влиянию обнаружения на безопасность компьютера или локальной сети вашей организации по опыту "Лаборатории Касперского".

   Параметр может принимать одно из следующих значений:

   - **Высокая** – алерт высокой степени важности. По умолчанию выбран этот вариант.
   - **Средняя** – алерт средней степени важности.
   - **Низкая** – алерт низкой степени важности.

3. В блоке параметров **Время ожидания проверки** в поле **Время ожидания** укажите время проверки файла. Во время проверки файла скорость его загрузки снижается. Если по истечении указанного времени файл не удастся проверить, загрузка продолжится с обычной скоростью.

   Значение по умолчанию: 10 минут. Вы можете установить любое значение, которое больше 1 минуты.

4. Нажмите на кнопку **Применить.**

Проверка будет выполняться в соответствии с настроенными параметрами.

Настройка отображения страниц уведомлений

> Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Во время проверки ICAP-трафика в режиме реального времени Kaspersky Anti Targeted Attack Platform может блокировать переход по URL-адресу и скачивание файла. Во время выполнения этих операций для пользователя хоста, с которого был отправлен запрос на переход по URL-адресу или скачивание файла, отображается HTML-страница с уведомлением. Если вы хотите, чтобы при операциях с объектами вместо страниц по умолчанию отображались ваши страницы, вы можете загрузить HTML-страницы, настроенные вами.

Чтобы загрузить страницу уведомления:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Проверка трафика ICAP**.
2. В разделе **Уведомления** нажмите на кнопку **Обзор** напротив одного из нужных полей.
3. В открывшемся окне выберите свою HTML-страницу.

4. Нажмите на кнопку **Открыть.**

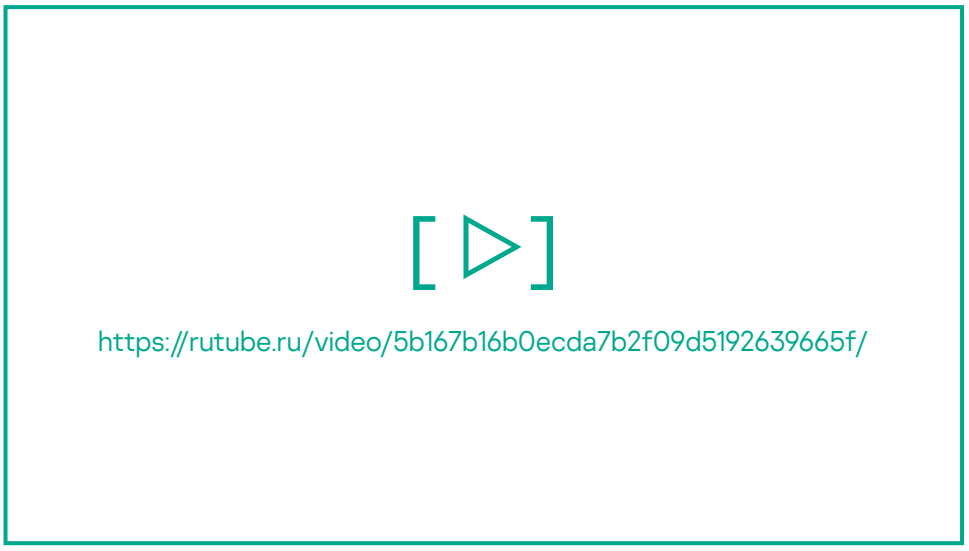
   Ваша страница будет загружена.

Настройка записи зеркалированного трафика со SPAN-портов

Kaspersky Anti Targeted Attack Platform позволяет сохранять зеркалированный трафик со SPAN-портов для проведения расследования и расширяет возможности по выявлению злонамеренной активности внутри периметра локальной сети организации. Благодаря записи зеркалированного трафика вы можете проводить ретроспективный анализ сетевых событий и расследовать действия злоумышленников. Трафик сохраняется в виде дампов в формате PCAP.

Для того чтобы сохранять зеркалированный трафик со SPAN-портов, вам необходимо включить запись этого трафика и настроить параметры записи. Вы также можете выбрать сетевые протоколы, из которых Kaspersky Anti Targeted Attack Platform будет извлекать объекты и метаинформацию при обработке зеркалированного трафика.

Посмотрите обучающее видео о настройке Central Node для работы со SPAN-трафиком через компонент Sensor. Для воспроизведения видео вы можете запустить его на странице справки (см. ниже) или перейти по ссылке https://rutube.ru/video/5b167b16b0ecda7b2f09d5192639665f/?playlist=891497.



Настройка Central Node для работы со SPAN-трафиком через Sensor

Выбор сетевых протоколов для получения зеркалированного трафика со SPAN-портов

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия по настройке в веб-интерфейсе того сервера PCN или SCN, к которому подключен компонент Sensor.

Чтобы выбрать сетевые протоколы для получения зеркалированного трафика со SPAN-портов:

1. Если вы хотите выбрать сетевые протоколы для получения зеркалированного трафика со SPAN-портов на встроенном Sensor (Embedded Sensor), войдите в консоль управления сервера Central Node с этим Sensor по протоколу SSH или через терминал.

2. Если вы хотите выбрать сетевые протоколы для получения зеркалированного трафика со SPAN-портов на Sensor, установленном отдельно от Central Node, войдите в консоль управления сервера Sensor по протоколу SSH или через терминал.

3. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке приложения.

   Откроется меню параметров компонента Sensor. Если меню не открылось, введите команду `kata-admin-menu` и нажмите на клавишу **ENTER**.

4. Перейдите в раздел **Program settings** → **Configure traffic capture** → **Setup capture protocols**, используя клавиши ↑, ↓ и **ENTER**. Выбранная строка подсвечивается красным.

   Откроется окно, где вы можете включить или отключить получение зеркалированного трафика со SPAN-портов по следующим сетевым протоколам:

   - **DNS**.
   - **FTP**.
   - **HTTP**.
   - **HTTP2**.
   - **SMTP**.
   - **SMB**.
   - **NFS**.

   Для того чтобы анализировать трафик NFS, необходимо смонтировать NFS-раздел с указанием версии протокола.

   Пример:

   для NFS v.4:

   ```
   mount -t nfs -o vers=4 -O uid=1000,iocharset=utf-8 <address>:/from/dir /to/dir
   ```

   для NFS v.3:

   ```
   mount -t nfs -o vers=3 -O uid=1000,iocharset=utf-8 <address>:/from/dir /to/dir
   ```

   Если получение зеркалированного трафика со SPAN-порта по сетевому протоколу включено, справа от названия сетевого протокола отображается **[x]**. Если получение трафика зеркалированного трафика со SPAN-порта по какому-либо сетевому протоколу отключено, справа от названия сетевого протокола отображается **[ ]**.

   По умолчанию получение зеркалированного трафика со SPAN-портов включено по всем сетевым протоколам, кроме **HTTP2**.

   Отключение HTTP- и/или DNS-протокола может привести к ошибке при обновлении баз приложения.

5. Если вы хотите включить или отключить получение зеркалированного трафика со SPAN-портов по какому-либо сетевому протоколу, выберите сетевой протокол, используя клавиши ↑, ↓, и нажмите на клавишу **ENTER**.

6. Выберите **Apply and finish** и нажмите на клавишу **ENTER**.

Сетевые протоколы для получения зеркалированного трафика со SPAN-портов будут выбраны.

Выбор сетевых протоколов на сервере с компонентом Sensor, установленным отдельно от Central Node

Если вы выбрали сетевые протоколы для получения зеркалированного трафика со SPAN-портов на отдельном Sensor до подключения его к Central Node и хотите изменить эти параметры после подключения, вам нужно выполнить шаги по подготовке к изменению параметров и затем инструкцию, приведенную выше.

Настройка параметров записи зеркалированного трафика со SPAN-портов

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия по настройке в веб-интерфейсе того сервера PCN или SCN, к которому подключен компонент Sensor.

Чтобы включить запись зеркалированного трафика со SPAN-портов:

1. Подключите и настройте внешнее хранилище.

2. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

3. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.

4. Нажмите на кнопку **Изменить**.

5. Перейдите на вкладку **Внешнее хранилище**.

   В разделе **Внешнее хранилище** в поле **Самый старый пакет** отображается дата и время первого сохраненного дампа во внешнем хранилище. В поле **Последний пакет** отображается дата и время последнего сохраненного дампа во внешнем хранилище.

6. Если вы хотите использовать внешнее хранилище, переведите переключатель **Подключить внешнее хранилище для файлов дампа трафика** в положение **Включено**.

   По умолчанию переключатель находится в положении **Выключено**.

7. Выполните следующие действия:

   a. В блоке параметров **Максимальный объем** укажите максимальный размер дампов трафика, которые будут храниться в хранилище.

      Если размер дампов, которые хранятся в хранилище, превысит указанное значение, то будут удалены ранние дампы, суммарный размер которых равен размеру новых дампов.

Если вы уменьшите максимальный размер хранилища, то будут удалены ранние дампы, суммарный размер которых равен изменению параметра.

b. Если вы хотите ограничить захват данных в трафике, в блоке параметров **Фильтрация с использованием BPF** переведите переключатель **Включить фильтрацию** в положение **Включено**. Фильтрация трафика может уменьшить размер дампов, сохраняющихся в хранилище и упростить процесс анализа трафика.

   В поле **Выражение для фильтрации** введите правило фильтрации. Для написания правила фильтрации BPF используется формат libpcap. Подробнее об описании синтаксиса см. в Руководстве pcap-filter.

   Пример выражения для фильтрации:

   ```
   tcp port 102 or tcp port 502
   ```

c. Если вы хотите назначить срок хранения дампов трафика, в блоке параметров **Ограничение времени хранения** переведите переключатель **Задать время хранения** в положение **Включено**. В поле **Время хранения (дней)** введите количество дней хранения дампов трафика. По истечении указанного срока дампы будут удалены из хранилища.

d. Нажмите на кнопку **Сохранить**.

Запись зеркалированного трафика со SPAN-портов будет настроена.

Настройка интеграции с почтовым сервером по протоколу POP3

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить интеграцию с почтовым сервером по протоколу POP3:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.
3. Нажмите на кнопку **Изменить**.
4. Перейдите на вкладку **POP3-интеграция**.
5. Переведите переключатель **Включить POP3-интеграцию** в положение **Включено**.
6. В поле **Почтовый сервер** укажите IP-адрес почтового сервера, с которым вы хотите настроить интеграцию.
7. В поле **Порт** укажите порт подключения к почтовому серверу.
8. В поле **Принимать каждые** укажите частоту соединения с почтовым сервером в секундах.
9. Если вы хотите использовать TLS-шифрование соединений с почтовым сервером по протоколу POP3, установите флажок **Использовать TLS-шифрование**.

10. В поле **Имя пользователя** укажите имя учетной записи для доступа к почтовому серверу.

11. В поле **Пароль** укажите пароль доступа к почтовому серверу.

    Почтовый сервер должен поддерживать базовую аутентификацию (Basic Authentication).

12. В раскрывающемся списке **TLS-сертификат** выберите один из следующих вариантов:

    - **Принимать любой**.
    - **Принимать недоверенный самоподписанный**.
    - **Принимать только доверенный**.

    При установке соединения с внешним почтовым сервером рекомендуется настроить прием только доверенных TLS-сертификатов. Прием недоверенных TLS-сертификатов не гарантирует защиту соединения от MITM-атак. Прием доверенных TLS-сертификатов также не полностью гарантирует защиту соединения от MITM-атак, но является самым безопасным из поддерживаемых способов интеграции с почтовым сервером по протоколу POP3.

13. При необходимости в поле **Набор шифров** измените параметры OpenSSL, используемые при установке соединения с почтовым сервером по протоколу POP3.

    Вы можете ознакомиться со справочной информацией OpenSSL по ссылке **Справка**.

14. Нажмите на кнопку **Сохранить**.

    Интеграция с почтовым сервером по протоколу POP3 будет настроена.

Если вы развернули компоненты Central Node и Sensor в виде кластера, вы можете настроить отказоустойчивую интеграцию с почтовым сервером.

Чтобы настроить отказоустойчивую интеграцию с почтовым сервером:

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.

2. В параметрах почтового сервера укажите это доменное имя.

   Интеграция с почтовым сервером будет настроена по доменному имени. Почтовый сервер обратится к случайному серверу кластера. При отказе этого сервера почтовый сервер будет обращаться к другому работоспособному серверу кластера.

Политики аутентификации

Вы можете настроить политики аутентификации для пользователей Kaspersky Anti Targeted Attack Platform. Действие политик распространяется на всех пользователей Kaspersky Anti Targeted Attack Platform с типом учетной записи **Учетная запись KATA** независимо от назначенной роли.

Обязательная смена пароля после первой успешной аутентификации

Если функция включена, смена пароля происходит по следующему сценарию:

1. Администратор создает учетную запись пользователя.
2. Пользователь выполняет аутентификацию в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.
3. Если пользователь не менял пароль до включения этой функции, при следующем входе в веб-интерфейс приложение предлагает ему изменить пароль учетной записи. Старый пароль становится недействительным.

Первой аутентификацией пользователя считается успешный вход в основной веб-интерфейс приложения. Смена пароля не запрашивается при повторном входе в веб-интерфейс по управлению масштабированием и в меню администратора приложения. Также смена пароля не запрашивается, если учетная запись используется для подключения SCN к PCN.

Регулярная смена пароля

Если регулярная смена пароля включена, приложение предлагает сменить пароль по истечении периода, заданного администратором. Отсчет периода начинается с момента смены пароля учетной записи и рассчитывается для каждого пользователя индивидуально.

Завершение неактивных сессий

Если пользователь не выполняет никаких действий (сессия неактивна), рекомендуется завершать такую сессию. Это снижает риск несанкционированного доступа к Kaspersky Anti Targeted Attack Platform, когда пользователь фактически закончил работу с приложением, но его сессия осталась незавершенной.

Информирование о неуспешных попытках аутентификации

Частые неудачные попытки входа в веб-интерфейс или консоль управления могут быть признаком того, что к Kaspersky Anti Targeted Attack Platform пытается получить доступ злоумышленник путем подбора паролей. Для предотвращения несанкционированного доступа в таких случаях рекомендуется включить информирование о превышении заданного ограничения на неуспешные попытки аутентификации.

Режим распределенного решения и мультитенантности

В режиме распределенного решения и мультитенантности параметры политик аутентификации, заданные на PCN, применяются к SCN.

Обязательная смена пароля после первой успешной аутентификации

Подробную информацию об этой функции см. в разделе *Политики аутентификации*.

Чтобы включить обязательную смену пароля после первой успешной аутентификации:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**.
2. Перейдите на вкладку **Политики аутентификации**.
3. В разделе **Смена пароля после первой аутентификации** переместите переключатель **Запрашивать смену пароля** в положение **Включено**.
4. Нажмите на кнопку **Применить**.

Обязательная смена пароля после первой аутентификации будет включена.

Обязательная смена пароля по истечении заданного периода

Подробную информацию об этой функции см. в разделе *Политики аутентификации*.

Чтобы включить и настроить обязательную смену пароля по истечении заданного периода:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**.
2. Перейдите на вкладку **Политики аутентификации**.
3. В разделе **Регулярная смена пароля** переместите переключатель **Запрашивать смену пароля** в положение **Включено**.
4. В поле **Менять пароль через** введите количество дней, по истечении которых требуется сменить пароль.
5. Нажмите на кнопку **Применить**.

Обязательная смена пароля по истечении заданного периода будет включена и настроена.

Завершение неактивных сессий

Если пользователь не выполняет никаких действий (сессия неактивна), рекомендуется завершать такую сессию. Это снижает риск несанкционированного доступа к Kaspersky Anti Targeted Attack Platform, когда пользователь фактически закончил работу с приложением, но его сессия осталась незавершенной.

Чтобы включить и настроить завершение неактивных сессий:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**.
2. Перейдите на вкладку **Политики аутентификации**.
3. В разделе **Завершение неактивных сессий** укажите время, по истечении которого нужно завершать пользовательскую сессию, если пользователь не выполняет никаких действий. Время в минутах введите в поле **Завершать неактивные сессии через**.
4. Если вы хотите, чтобы при отсутствии действий со стороны пользователя становился недоступен раздел **Мониторинг**, установите флажок **Блокировать раздел Мониторинг, когда сессия неактивна**. Если флажок снят, раздел **Мониторинг** доступен для просмотра пользователем даже в том случае, если сессия неактивна.
5. Нажмите на кнопку **Применить**.

Неактивные пользовательские сессии будут завершаться по истечении указанного интервала времени.

Информирование о неуспешных попытках аутентификации

Частые неудачные попытки входа в веб-интерфейс или консоль управления могут быть признаком того, что к Kaspersky Anti Targeted Attack Platform пытается получить доступ злоумышленник путем подбора паролей. Для предотвращения несанкционированного доступа в таких случаях рекомендуется включить информирование о превышении заданного ограничения на неуспешные попытки аутентификации.

Чтобы включить и настроить информирование о неуспешных попытках аутентификации:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**.
2. Перейдите на вкладку **Политики аутентификации**.
3. В разделе **Подсчет попыток аутентификации** переместите переключатель **Считать попытки** в положение **Включено**.

4. В поле **Период подсчета** введите время, в течение которого должны подсчитываться неуспешные попытки аутентификации. Время указывается в минутах. Если в течение этого времени пользователь неуспешно пытается войти в веб-интерфейс или консоль управления более двух раз подряд, происходит следующее:

   - В журнал активности пользователей вносится запись о неуспешных попытках аутентификации пользователя.
   - Если создано правило отправки уведомлений о превышении количества неудачных попыток аутентификации (см. ниже инструкцию о создании правила), отправляется сообщение электронной почты на адреса, указанные в правиле уведомления. В сообщении содержится информация о неуспешных попытках аутентификации пользователя.

   В поле **Период подсчета** допускается указать `0`, в этом случае подсчитываются все неуспешные попытки аутентификации, вне зависимости от временного интервала между ними.

5. Нажмите на кнопку **Применить**.

   Неуспешные попытки аутентификации будут подсчитываться, при превышении заданного порога (две неуспешные попытки аутентификации подряд) информация об этом будет сохранена и доступна для ознакомления.

Чтобы включить и настроить отправку уведомлений о превышении количества неудачных попыток аутентификации,

Следуйте инструкции по созданию правила для отправки уведомлений о работе компонентов приложения. В процессе создания правила в блоке параметров **Компоненты** установите флажок **Попытки авторизации**.

На адреса электронной почты, указанные в правиле уведомления, будет отправляться сообщение с информацией о неуспешных попытках аутентификации пользователя, если таких попыток более двух подряд за заданный интервал времени (см. выше параметр **Период подсчета**).

Управление кластером

Вы можете просматривать таблицу серверов кластера, добавлять серверы в кластер, перезагружать серверы, выводить серверы из эксплуатации, включать и выключать кластер. При необходимости вы можете увеличить дисковое пространство сервера хранения.

Просмотр таблицы серверов кластера

Таблица серверов кластера отображается в разделе **Кластер** окна веб-интерфейса приложения.

В таблице содержится следующая информация:

- **Тип сервера** – тип сервера в зависимости от его роли в кластере.

  Могут отображаться следующие значения:

  - **Хранение**.
  - **Обработка**.

- **Состояние** – состояние сервера.

  Могут отображаться следующие значения:

  - **Подключен**.
  - **Не подключен**.

- **Имя хоста** – имя сервера.
- **IP** – IP-адрес сервера.
- **ОЗУ** – уровень загрузки оперативной памяти сервера.
- **ЦП** – уровень загрузки процессора сервера.
- **Действие** – действия, которые вы можете выполнить с сервером.

  Доступно следующее действие: **Удалить**.

Добавление сервера в кластер

Для добавления сервера в кластер вам нужно запустить установку Kaspersky Anti Targeted Attack Platform на этом сервере и выполнить шаги по установке компонентов. Добавленный сервер отобразится в списке серверов кластера.

Увеличение дискового пространства сервера хранения

Вы можете увеличить дисковое пространство функционирующего сервера хранения, установив дополнительный диск.

> Для увеличения дискового пространства сервера хранения с помощью дополнительного диска вам требуется обратиться в Службу технической поддержки.

Настройка сервера производится в режиме Technical Support Mode.

Перезагрузка серверов кластера

Перед перезагрузкой сервера любого типа вам нужно убедиться, что другой сервер соответствующего типа остается активным. Мы настоятельно рекомендуем перезагружать серверы поочередно и переходить к перезагрузке следующего сервера кластера только после того, как вы выполните все шаги одной из инструкций, приведенных ниже.

Перезагрузка обрабатывающего сервера кластера

Чтобы перезагрузить обрабатывающий сервер:

1. Определите, каким из серверов кластера присвоена роль manager в Docker Swarm. Для этого на любом из серверов кластера выполните команду:

   ```
   docker node ls
   ```

   После выполнения команды отобразится список серверов кластера. Роль manager присвоена тем из них, у которых в столбце MANAGER STATUS указано Leader или Reachable.

2. Сохраните полученный список серверов любым удобным для себя способом.

   Через эти серверы вы можете отследить статус переноса сервисов, необходимых для работы приложения, между обрабатывающими серверами кластера после перезагрузки.

3. Перезагрузите требуемый обрабатывающий сервер в меню администратора компонента.

4. Подождите не менее 5 минут.

5. На сервере с ролью manager проверьте статус переноса сервисов на другой обрабатывающий сервер:

   ```
   docker service ls | grep -v configurator | grep ' 0/'
   ```

   Вывод должен быть пустым. Это означает, что все сервисы успешно запустились на другом обрабатывающем сервере.

6. При необходимости повторяйте шаг 5, пока вывод не станет пустым.

Обрабатывающий сервер будет перезагружен. Вы можете приступить к перезагрузке следующего обрабатывающего сервера.

Перезагрузка серверов хранения

Чтобы перезагрузить серверы хранения:

1. Перезагрузите требуемый сервер хранения в меню администратора компонента.

2. Подождите не менее 5 минут.

3. На любом сервере кластера проверьте статус работоспособности кластера:

   ```
   $ceph -s
   ```

   После выполнения команды должен отобразиться статус `HEALTH_OK`.

4. При необходимости повторяйте шаг 3, пока не отобразится статус `HEALTH_OK`.

Сервер хранения будет перезагружен. Вы можете приступить к перезагрузке следующего сервера хранения.

Вывод серверов из эксплуатации

Для вывода из эксплуатации функционирующего сервера вам требуется обратиться в Службу технической поддержки.

При отказе сервера вы можете вывести его из эксплуатации самостоятельно.

Чтобы вывести из эксплуатации неработоспособный обрабатывающий сервер:

1. Добавьте новый обрабатывающий сервер в кластер.
2. Удалите сервер из кластера.
3. Настройте параметры масштабирования приложения для новой конфигурации.

   Обрабатывающий сервер будет выведен из эксплуатации.

Чтобы вывести из эксплуатации неработоспособный сервер хранения:

1. Добавьте новый сервер хранения в кластер.
2. Обратитесь в Службу технической поддержки, чтобы удалить сервер из кластера.

   Сервер хранения будет выведен из эксплуатации.

Удаление сервера из кластера

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Удаленный сервер нельзя восстановить. Убедитесь, что выбранный сервер не функционирует.

Чтобы удалить сервер из кластера:

1. В окне веб-интерфейса приложения выберите раздел **Кластер**.
2. В столбце **Действие** нажмите на ссылку **Удалить** напротив того сервера, который вы хотите удалить.
3. Нажмите на кнопку **Продолжить**.

   Процесс удаления будет запущен. Удаление может занять около суток. Информация об удаленном сервере не будет отображаться в таблице серверов.

После удаления сервера вы можете изменить конфигурацию серверов кластера или добавить сервер с аналогичной ролью, чтобы сохранить производительность приложения на прежнем уровне.

Включение и выключение кластера

Для выключения и включения кластера вам рекомендуется обратиться в Службу технической поддержки. Не выполняйте выключение и включение кластера при возникновении проблем с работоспособностью приложения.

Если вы хотите отключить питание работоспособных серверов кластера, вам нужно предварительно выключить кластер, чтобы избежать потери данных.

Чтобы выключить кластер:

1. В окне веб-интерфейса приложения перейдите в раздел **Кластер**.
2. Нажмите на кнопку **Выключить**.

   Работа основных компонентов приложения будет остановлена. Вы можете отключить питание серверов кластера.

Чтобы запустить серверы кластера:

1. Отключите питание серверов, если оно не было отключено ранее.
2. Включите питание сервера хранения.
3. Включите питание остальных серверов.

   Серверы кластера будут запущены.

Запуск всех серверов кластера занимает около 90 минут. Веб-интерфейс приложения становится доступным до того, как запустятся все серверы кластера. При этом для пользователей с ролями **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Аудитор** в веб-интерфейсе приложения не отображается меню приложения, а для пользователей с ролью **Администратор** доступен только раздел **Конфигурация серверов**.

Настоятельно не рекомендуется менять параметры масштабирования приложения, пока все серверы кластера не будут запущены.

После запуска всех серверов кластера меню веб-интерфейса приложения отображается в штатном режиме.

Уведомления о максимальной загрузке центрального процессора и оперативной памяти серверов Central Node и Sensor

Высокая загрузка центрального процессора и оперативной памяти серверов Central Node и Sensor может привести к неработоспособности компонентов приложения.

Вы можете настроить максимальные допустимые значения загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor, при превышении которых в верхней части окна раздела **Мониторинг** веб-интерфейса приложения для пользователей с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** и **Администратор** отобразится рамка желтого цвета с предупреждением. Также вы можете настроить отправку уведомлений на адрес или адреса электронной почты и соединение с протоколом SNMP для отправки данных об уровне загрузки центрального процессора и оперативной памяти во внешние системы, поддерживающие этот протокол.

Если вы развернули компоненты Central Node и Sensor в виде кластера, предупреждения отображаются отдельно для каждого сервера кластера.

Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** также могут создавать правила для отправки уведомлений. В этом случае для корректной отправки уведомлений вам требуется предварительно настроить максимальные допустимые значения загрузки центрального процессора и оперативной памяти серверов, а также параметры сервера для отправки уведомлений.

В существующих правилах для отправки уведомлений о работе компонентов приложения функция уведомления о загрузке центрального процессора и оперативной памяти серверов будет включена автоматически, если при создании правила в блоке параметров **Компоненты** был установлен флажок **Все**.

Настройка максимального допустимого значения загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor

В режиме распределенного решения и мультитенантности вам нужно задать максимальные допустимые значения загрузки центрального процессора и оперативной памяти на каждом сервере Central Node, с которого вы хотите получать уведомления. Если вы используете кластер Central Node, вы можете настроить эти параметры на любом сервере кластера.

Чтобы настроить максимальное допустимое значение загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Мониторинг** выполните следующие действия:
   - В поле **Уведомление о загрузке ЦП более чем на N % в течение M минут** укажите максимальное допустимое значение загрузки центрального процессора и время, в течение которого указанная загрузка считается допустимой.

     По умолчанию максимальное допустимое значение загрузки центрального процессора составляет 95% в течение 5 минут.

- В поле **Уведомление о загрузке ОЗУ более чем на N % в течение M минут** укажите максимальное допустимое значение загрузки оперативной памяти и время, в течение которого указанная загрузка считается допустимой.

  По умолчанию максимальное допустимое значение загрузки оперативной памяти составляет 95% в течение 5 минут.

3. Нажмите на кнопку **Применить**.

Максимальное значение загрузки центрального процессора и оперативной памяти серверов будет настроено. При превышении одного из заданных показателей на сервере Central Node и/или Sensor, в верхней части окна раздела **Мониторинг** веб-интерфейса приложения для пользователей с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** и **Администратор** отобразится рамка желтого цвета с предупреждением.

Настройка соединения по протоколу SNMP

Вы можете отправлять данные о загрузке центрального процессора и оперативной памяти серверов Central Node и Sensor во внешние системы, поддерживающие протокол SNMP. Для этого вам требуется настроить параметры соединения по протоколу.

Если компонент Central Node развернут в виде кластера, во внешние системы отправляются данные о загрузке центрального процессора и оперативной памяти каждого сервера кластера.

Чтобы настроить параметры соединения по протоколу SNMP на сервере Central Node:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **SNMP** установите флажок **Использовать SNMP**.
3. В поле **Версия протокола** выберите одну из следующих версий протокола:
   - **v2c**.
   - **v3**.
4. Если вы выбрали версию протокола **v2c**, в поле **Строка сообщества** укажите пароль, который будет использоваться для подключения к Kaspersky Anti Targeted Attack Platform.
5. Если вы выбрали **v3**, выполните следующие действия:
   a. В поле **Протокол аутентификации** выберите один из следующих вариантов проверки достоверности и целостности данных, переданных во внешнюю систему:
      - **MD5**.
      - **SHA256**.
   b. В поле **Имя пользователя** укажите имя пользователя.

c. В поле **Пароль** укажите пароль для аутентификации.

Имя пользователя и пароль, заданные в полях **Имя пользователя** и **Пароль** должны совпадать с именем пользователя и паролем, заданными при создании учетной записи во внешней системе. Если данные не совпадают, соединение не будет установлено.

d. В поле **Протокол шифрования** выберите один из следующих типов шифрования:

- **DES**.
- **AES**.

e. В поле **Пароль** укажите пароль для шифрования.

Пароль, заданный в этом поле, должен совпадать с паролем, заданным во внешней системе.

Параметры соединения по протоколу SNMP на сервере Central Node будут настроены. При успешной обработке запроса на получение данных на сервере внешней системы отобразится информация о загрузке центрального процессора и оперативной памяти сервера Central Node.

Чтобы настроить параметры соединения по протоколу SNMP на сервере Sensor:

1. Войдите в консоль управления сервера Sensor по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке приложения.

   Отобразится меню администратора компонента приложения.
3. Выполните шаги 2 – 5 инструкции, приведенной выше.

Параметры соединения по протоколу SNMP на сервере Sensor будут настроены. При успешной обработке запроса на сервере внешней системы отобразится информация о загрузке центрального процессора и оперативной памяти сервера Sensor.

В режим распределенного решения и мультитенантности параметры соединения по протоколу SNMP для каждого сервера PCN, SCN и Sensor настраиваются отдельно.

Описание объектов MIB Kaspersky Anti Targeted Attack Platform

В таблице ниже приведена информация об объектах MIB Kaspersky Anti Targeted Attack Platform.

Данные о загрузке жесткого диска, центрального процессора и оперативной памяти серверов Central Node и Sensor

Данные о загрузке жесткого диска, центрального процессора и оперативной памяти серверов Central Node и Sensor

Символьное имя	Описание	Идентификатор (OID)
dskTotal	Размер диска или тома, КБ.	1.3.6.1.4.1.2021.9.1.6
dskAvail	Свободное пространство на диске, КБ.	1.3.6.1.4.1.2021.9.1.7
dskUsed	Используемое пространство на диске, КБ.	1.3.6.1.4.1.2021.9.1.8
dskPercent	Процент используемого пространства на диске, %.	1.3.6.1.4.1.2021.9.1.9
laLoad	Среднее значение загрузки системы (load average) в течение 1, 5 и 15 минут.	1.3.6.1.4.1.2021.10.1.3
memTotalReal	Размер оперативной памяти, КБ.	1.3.6.1.4.1.2021.4.5
memAvailReal	Количество используемой оперативной памяти, КБ.	1.3.6.1.4.1.2021.4.6
memTotalFree	Количество свободной оперативной памяти, КБ.	1.3.6.1.4.1.2021.4.11

Работа с информацией о хостах с компонентом Endpoint Agent

Приложение, выступающее в роли компонента Endpoint Agent, устанавливается на отдельные компьютеры (далее также "хосты"), входящие в IT-инфраструктуру организации. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих хостах, открытыми сетевыми соединениями и изменяемыми файлами.

Пользователи с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Аудитор** и **Администратор** могут оценить регулярность получения данных с хостов с компонентом Endpoint Agent, на закладке **Endpoint Agents** окна веб-интерфейса сервера Central Node в рамках тех тенантов, к данным которых у них есть доступ. Если вы используете режим распределенного решения и мультитенантности, то в веб-интерфейсе сервера PCN отображается список хостов с компонентом Endpoint Agent для PCN и всех подключенных SCN.

Пользователи с ролью **Администратор** могут настроить отображение регулярности получения данных с хостов с компонентом Endpoint Agent в рамках тех тенантов, к данным которых у них есть доступ.

В случае возникновения подозрительной сетевой активности пользователь с ролью **Старший сотрудник службы безопасности** может изолировать от сети любой из хостов с компонентом Endpoint Agent в рамках тех тенантов, к данным которых у него есть доступ. При этом соединение между сервером с компонентом Central Node и хостом с компонентом Endpoint Agent не будет прервано.

Для оказания поддержки при неполадках в работе компонента Endpoint Agent специалисты Службы технической поддержки могут попросить вас в отладочных целях выполнить следующие действия (в том числе в режиме Technical Support Mode):

- Активировать функциональность получения расширенной диагностической информации.
- Изменить параметры отдельных компонентов приложения.

- Изменить параметры хранения и отправки получаемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Специалисты Службы технической поддержки сообщат вам необходимую для выполнения перечисленных действий информацию (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав получаемых в отладочных целях данных. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка полученных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы приложения способами, не описанными в настоящем руководстве, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

Выбор тенанта для работы в разделе Endpoint Agents

Если вы используете режим распределенного решения и мультитенантности, перед началом работы в разделе **Активы** → **Endpoint Agents** вам нужно выбрать тенанты, данные по которым вас интересуют.

*Чтобы выбрать тенант для работы в разделе **Активы** → **Endpoint Agents**:*

1. В верхней части меню веб-интерфейса приложения нажмите на стрелку рядом с названием тенанта.
2. В раскрывшемся списке выберите тенант.

   Отобразятся данные по выбранному вами тенанту. Если вы хотите изменить тенант, вам нужно повторить действия по выбору тенанта.

Просмотр таблицы хостов с компонентом Endpoint Agent на отдельном сервере Central Node

Таблица хостов с компонентом Endpoint Agent находится в разделе **Активы** → **Endpoint Agents** окна веб-интерфейса приложения.

В таблице могут отображаться следующие данные:

- Количество хостов и показатели активности компонента Endpoint Agent:
  - **Критическое бездействие** – количество хостов, от которых последние данные были получены очень давно.
  - **Предупреждение** – количество хостов, от которых последние данные были получены давно.
  - **Нормальная активность** – количество хостов, от которых последние данные были получены недавно.
- **Хост** – имя хоста с компонентом Endpoint Agent.

- **Серверы** – имена серверов, к которым подключен хост с компонентом Endpoint Agent.

  Поле отображается, если вы используете режим распределенного решения и мультитенантности.

- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Agent.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Agent.
- **Лицензия** – статус лицензионного ключа приложения, которое используется в роли компонента Endpoint Agent.
- **Версия** – версия приложения, которое используется в роли компонента Endpoint Agent.
- **Активность** – показатель активности компонента Endpoint Agent. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.
- **Последнее подключение** – дата и время последнего подключения компонента Endpoint Agent к серверу Central Node.

По ссылке в столбцах таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

Просмотр информации о хосте

Чтобы просмотреть информацию о хосте с компонентом Endpoint Agent:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.
3. Выберите хост, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о хосте.

Окно содержит следующую информацию:

- В разделе **Хост**:
  - **Имя** – имя хоста с компонентом Endpoint Agent.
  - **IP** – IP-адрес хоста, на который установлен компонент Endpoint Agent.
  - **ОС** – версия операционной системы на хосте, на который установлен компонент Endpoint Agent.

- **Сервер** – имя сервера SCN или PCN. Отображается только в режиме распределенного решения и мультитенантности.

- В разделе **Endpoint Agent**:
  - **Версия** – версия приложения, которое используется в роли компонента Endpoint Agent.
  - **Активность** – показатель активности компонента Endpoint Agent. Может иметь следующие значения:
    - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
    - **Предупреждение** – хосты, от которых последние данные были получены давно.
    - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.
  - **Подключен к серверу** – имя сервера, Central Node, SCN или PCN, к которому подключен хост.
  - **Последнее подключение** – время последнего соединения с сервером Central Node, SCN или PCN.
  - **Лицензия** – состояние лицензионного ключа приложения, которое используется в роли компонента Endpoint Agent.

По ссылкам с именем хоста и его IP-адресом доступно следующее действие: **Скопировать значение в буфер**.

Фильтрация и поиск хостов с компонентом Endpoint Agent по имени хоста

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по имени хоста:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.
3. По ссылке **Хост** откройте окно настройки фильтрации.
4. Если вы хотите, чтобы отобразились только изолированные хосты, установите флажок **Показывать только изолированные Endpoint Agents**.
5. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
6. В поле ввода укажите один или несколько символов имени хоста.
7. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

8. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.

9. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent, изолированных от сети

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent, изолированные от сети:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.

2. Перейдите на вкладку **Endpoint Agents**.
   Откроется таблица хостов.

3. По ссылке **Хост** откройте окно настройки фильтрации.

4. Установите флажок **Показывать только изолированные Endpoint Agents**.

5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по именам серверов PCN и SCN

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать или найти хосты с компонентом Endpoint Agent по именам серверов PCN и SCN, к которым подключены эти хосты.

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по именам серверов PCN и SCN:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.
3. По ссылке **Серверы** откройте окно настройки фильтрации.
4. Установите флажки рядом с теми именами серверов, по которым вы хотите отфильтровать или найти хосты с компонентом Endpoint Agent.
5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по IP-адресу компьютера

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по IP-адресу компьютера, на котором установлено приложение:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.
3. По ссылке **IP** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов IP-адреса компьютера. Вы можете ввести IP-адрес компьютера или маску подсети в формате IPv4 (например, `192.0.0.1` или `192.0.0.0/16`).
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

7. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.

8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по версии операционной системы на компьютере

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по версии операционной системы, установленной на компьютере:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.

2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.

3. По ссылке **ОС** откройте окно настройки фильтрации.

4. В раскрывающемся списке выберите один из следующих операторов фильтрации:

   - **Содержит**.
   - **Не содержит**.

5. В поле ввода укажите один или несколько символов версии операционной системы.

6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

7. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.

8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по версии компонента

Вы можете отфильтровать хосты по версии приложения, которое используется в роли компонента Endpoint Agent.

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по версии компонента:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.
3. По ссылке **Версия** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов версии приложение, которое используется в роли компонента Endpoint Agent.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по их активности

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по их активности:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.

3. По ссылке **Активность** откройте окно настройки фильтрации.

   Установите флажки рядом с одним или несколькими показателями активности:

   - **Нормальная активность**, если вы хотите найти хосты, от которых последние данные были получены недавно.
   - **Предупреждение**, если вы хотите найти хосты, от которых последние данные были получены давно.
   - **Критическое бездействие**, если вы хотите найти хосты, от которых последние данные были получены очень давно.

4. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

   В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Быстрое создание фильтра хостов с компонентом Endpoint Agent

Чтобы быстро создать фильтр хостов с компонентом Endpoint Agent:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.

3. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:

   a. Наведите курсор мыши на ссылку с тем значением столбца таблицы, которое вы хотите добавить в качестве условия фильтрации.

   b. Нажмите на левую клавишу мыши.

      Откроется список действий над значением.

   c. В открывшемся списке выберите одно из следующих действий:

      - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
      - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.

4. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

   В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Сброс фильтра хостов с компонентом Endpoint Agent

Чтобы сбросить фильтр хостов с компонентом Endpoint Agent по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.
3. Нажмите на кнопку справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Настройка показателей активности компонента Endpoint Agent

Пользователи с ролью **Администратор** могут определить, какой период бездействия приложения, которое используется в роли компонента Endpoint Agent, считать нормальной, низкой и очень низкой активностью, а также настроить показатели активности приложения. Пользователи с ролью **Аудитор** могут просматривать параметры показателей активности компонента. Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут просмотреть показатели активности приложения в столбце **Активность** таблицы компонентов Endpoint Agent в разделе **Endpoint Agents** окна веб-интерфейса приложения.

Чтобы настроить показатели активности компонента Endpoint Agent:

1. В окне веб интерфейса приложения выберите раздел **Параметры**, подраздел **Endpoint Agents**.
2. В полях под названием раздела введите количество дней бездействия хостов с компонентом Endpoint Agent, которое вы хотите отображать как **Предупреждение** и **Критическое бездействие**.

   По умолчанию используются значения 1 и 7.
3. Нажмите на кнопку **Применить**.

Показатели активности компонента Endpoint Agent будут настроены.

Удаление хостов с компонентом Endpoint Agent

Чтобы удалить один или несколько хостов из таблицы **Endpoint Agents**:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.
3. Установите флажки рядом с одним или несколькими хостами, которые вы хотите удалить. Вы можете выбрать все хосты, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.
4. Нажмите на кнопку **Удалить**.
5. В открывшемся окне подтверждения действия нажмите на кнопку **Да**.

Выбранные хосты будут удалены из таблицы **Endpoint Agents**.

При удалении хостов в веб-интерфейсе Kaspersky Anti Targeted Attack Platform происходят следующие изменения:

- Для удаленного хоста нельзя создать задачу, правило запрета и правило сетевой изоляции.
- Если для хоста ранее было создано правило запрета, при удалении этого хоста его имя в окне просмотра правила (поле **Запрет для**) будет скрыто. Правило продолжит действовать.

  При повторном подключении этого хоста к серверу Central Node имя хоста будет восстановлено в поле **Запрет для** и правило запрета снова будет на него распространяться.
- Если для хоста ранее было создано правило сетевой изоляции, оно продолжит действовать до истечения времени, указанного в правиле.

  При повторном подключении этого хоста к серверу Central Node правило снова будет распространяться на этот хост.
- Метаданные объектов, помещенных на карантин на удаленном хосте, удаляются из карантина Kaspersky Anti Targeted Attack Platform.

  При повторном подключении этого хоста к серверу Central Node метаданные объектов в карантине Kaspersky Anti Targeted Attack Platform **не** восстанавливаются. Вы можете избежать переполнения карантина на хосте, очистив его с помощью командной строки или через Kaspersky Security Center. Подробнее см. в справке приложения, которое используется в роли компонента Endpoint Agent.
- Если объект был помещен на карантин по задаче **Поместить файл на карантин** только на одном хосте и этот хост был удален, в окне просмотра задачи кнопка **Восстановить все** будет неактивна, так как восстановить файл на удаленном хосте нельзя.

Поиск событий по имени удаленного хоста остается доступным.

Автоматическое удаление неактивных хостов

Вы можете включать и отключать автоматическое удаление неактивных хостов из таблицы **Endpoint Agents**. Неактивными считаются хосты, которые не подключались к серверу Central Node в течение указанного вами времени.

*Чтобы включить или отключить автоматическое удаление хостов из таблицы **Endpoint Agents**:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Endpoint Agents**.
2. В блоке параметров **Автоматическое удаление неактивных хостов** выполните следующие действия:
   - Если вы хотите включить функцию, переведите переключатель **Удалять хосты** в положение **Включено**.
   - Если вы хотите отключить функцию, переведите переключатель **Удалять хосты** в положение **Выключено**.
3. Если вы включили функцию, в поле **Удалять после** укажите количество дней, по истечении которых хосты, не подключавшиеся за это время к компоненту Central Node, будут считаться неактивными.

   Значение не может быть меньше 1 и больше 365.

Автоматическое удаление неактивных хостов будет включено или отключено.

Если значение, указанное в поле **Удалять после**, меньше значений, указанных в полях **Предупреждение** и / или **Критическое бездействие** блока параметров **Индикаторы активности**, хосты будут удалены раньше, чем в разделе **Мониторинг** отобразится предупреждение об их неактивности.

При удалении хостов в веб-интерфейсе Kaspersky Anti Targeted Attack Platform происходят следующие изменения:

- Для удаленного хоста нельзя создать задачу, правило запрета и правило сетевой изоляции.
- Если для хоста ранее было создано правило запрета, при удалении этого хоста его имя в окне просмотра правила (поле **Запрет для**) будет скрыто. Правило продолжит действовать.

  При повторном подключении этого хоста к серверу Central Node имя хоста будет восстановлено в поле **Запрет для** и правило запрета снова будет на него распространяться.
- Если для хоста ранее было создано правило сетевой изоляции, оно продолжит действовать до истечения времени, указанного в правиле.

  При повторном подключении этого хоста к серверу Central Node правило снова будет распространяться на этот хост.

- Метаданные объектов, помещенных на карантин на удаленном хосте, удаляются из карантина Kaspersky Anti Targeted Attack Platform.

  При повторном подключении этого хоста к серверу Central Node метаданные объектов в карантине Kaspersky Anti Targeted Attack Platform **не** восстанавливаются. Вы можете избежать переполнения карантина на хосте, очистив его с помощью командной строки или через Kaspersky Security Center. Подробнее см. в справке приложения, которое используется в роли компонента Endpoint Agent.

- Если объект был помещен на карантин по задаче **Поместить файл на карантин** только на одном хосте и этот хост был удален, в окне просмотра задачи кнопка **Восстановить все** будет неактивна, так как восстановить файл на удаленном хосте нельзя.

Поиск событий по имени удаленного хоста остается доступным.

Настройка интеграции с компонентом Sandbox

Вы можете подключить один компонент Sandbox к нескольким компонентам Central Node.

Предусмотрен следующий порядок настройки соединения компонента Sandbox с компонентом Central Node:

1. **Создание запроса на подключение к компоненту Sandbox**

   Вы можете создать запрос в веб-интерфейсе приложения под учетной записью администратора. Если у вас есть несколько компонентов Central Node, установленных на сервере, вам нужно создать запрос для каждого сервера с компонентом Central Node, который вы хотите подключить к компоненту Sandbox. Если компонент Central Node развернут в виде кластера, вы можете создать запрос на подключение с любого сервера кластера.

2. **Обработка запроса на подключение в веб-интерфейсе Sandbox**

   Вы можете принять или отклонить каждый запрос.

Если вы хотите подключить несколько компонентов Sandbox к одному компоненту Central Node, убедитесь, что на подключаемых компонентах Sandbox совпадают наборы операционных систем для проверки объектов и максимальное количество одновременно запускаемых виртуальных машин.

После настройки соединения серверу Sandbox требуется 5–10 минут для подготовки к работе. В течение этого времени в окне **Работоспособность системы** веб-интерфейса приложения отображается предупреждение *Возникла проблема со стандартной конфигурацией*. Когда сервер будет готов к работе, предупреждение исчезнет.

Просмотр таблицы серверов с компонентом Sandbox

Пользователи с ролью **Аудитор** могут просматривать таблицу серверов с компонентом Sandbox.

Таблица серверов с компонентом Sandbox находится в разделе **Серверы Sandbox**, на закладке **Серверы** окна веб-интерфейса приложения.

В поле **Отпечаток сертификата** отображается отпечаток TLS-сертификата сервера Central Node.

Таблица **Список серверов** содержит следующую информацию:

- **IP и имя** – IP-адрес или полное доменное имя сервера с компонентом Sandbox.
- **Отпечаток сертификата** – отпечаток сертификата сервера с компонентом Sandbox.
- **Авторизация** – статус запроса на подключение к компоненту Sandbox.
- **Состояние** – состояние подключения к компоненту Sandbox.

Для пользователей с ролью **Сотрудник службы безопасности** просмотр таблицы серверов с компонентом Sandbox недоступен.

Создание запроса на подключение к серверу с компонентом Sandbox

Чтобы создать запрос на подключение к серверу с компонентом Sandbox через веб-интерфейс приложения:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sandbox**.
2. В правом верхнем углу окна нажмите на кнопку **Добавить**.

   Откроется окно **Подключение сервера Sandbox**.
3. В поле **IP** введите IP-адрес сервера с компонентом Sandbox, к которому вы хотите подключиться.
4. Нажмите на кнопку **Получить отпечаток сертификата**.

   В рабочей области отобразится отпечаток сертификата сервера с компонентом Sandbox.
5. Сравните полученный отпечаток сертификата с отпечатком, указанным в веб-интерфейсе Sandbox в разделе **Авторизация KATA** в поле **Отпечаток сертификата**.

   Если отпечатки сертификата совпадают, выполните дальнейшие шаги инструкции.

   Не рекомендуется подтверждать подключение при несовпадении отпечатков сертификата. Убедитесь, что в поле **IP** введен верный IP-адрес.
6. В поле **Имя** укажите имя для компонента Sandbox, которое будет отображаться в веб-интерфейсе компонента Central Node.

   Это имя не связано с именем хоста, на котором установлен Sandbox, и может быть любым.
7. Если вы хотите сделать соединение с Sandbox активным сразу после подключения, установите флажок **Включить**.
8. Нажмите на кнопку **Добавить**.

Запрос на подключение отобразится в веб-интерфейсе компонента Sandbox, где его можно принять, отклонить или отозвать.

Включение и отключение соединения с компонентом Sandbox

Чтобы сделать соединение с компонентом Sandbox активным или отключить его:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sandbox**.

   Отобразится таблица серверов с компонентами Sandbox.

2. В строке с нужным сервером в столбце **Состояние** выполните одно из следующих действий:

   - Если вы хотите сделать соединение с компонентом Sandbox активным, переведите переключатель в положение **Включено**.
   - Если вы хотите отключить соединение с компонентом Sandbox, переведите переключатель в положение **Выключено**.

3. Нажмите на кнопку **Применить**.

Соединение с компонентом Sandbox станет активным или будет отключено.

Удаление соединения с компонентом Sandbox

Чтобы удалить соединение с компонентом Sandbox:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sandbox**.

   Отобразится таблица компьютеров, на которых установлен компонент Sandbox.

2. Установите флажок в строке с компонентом Sandbox, соединение с которым вы хотите удалить.
3. В правом верхнем углу окна нажмите на кнопку **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**.

Соединение с компонентом Sandbox будет удалено.

Выбор операционных систем для проверки объектов в Sandbox

Вы можете выбрать набор операционных систем, на основе которого будут формироваться задачи на проверку объектов для компонента Sandbox. Вам потребуется установить виртуальные машины с операционными системами, которые соответствуют выбранному набору, на сервере Sandbox.

Чтобы выбрать набор операционных систем:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sandbox**.
2. Выберите закладку **Параметры**.

3. В блоке параметров **Набор ОС** выберите один из вариантов:

   - **Windows 7, Windows 10**.
   - **CentOS 7.8, Windows 7, Windows 10**.
   - **Astra Linux 1.7, Windows 7, Windows 10**.
   - **Пользовательские**.

4. Если вы выбрали **Пользовательские**, в блоке параметров **Состав набора** установите флажки напротив операционных систем, которые вы хотите использовать в наборе.

   Пользовательские операционные системы отображаются в списке, если виртуальные машины с этими операционными системами были установлены на сервере Sandbox. Преднастроенные операционные системы всегда отображаются в списке, но если виртуальные машины с этими операционными системами не развернуты, рядом с названием операционной системы отображается статус **Неизвестно**.

Kaspersky Anti Targeted Attack Platform будет создавать задачи на проверку объектов в Sandbox в соответствии с выбранным набором.

Если набор операционных систем, установленных на сервере Sandbox, не совпадает с набором, выбранным на сервере Central Node, объекты не отправляются на проверку этому серверу Sandbox. При подключении к серверу Central Node нескольких серверов Sandbox приложение отправляет объекты на проверку тем серверам Sandbox, на которых установлены операционные системы, соответствующие выбранному на Central Node набору.

Вы можете изменить набор операционных систем в ходе эксплуатации приложения. В этом случае вам нужно убедиться, что конфигурация сервера Sandbox соответствует аппаратным требованиям.

В режиме распределенного решения и мультитенантности настройки набора операционных систем, заданные на сервере PCN, не распространяются на подключенные к нему серверы SCN. Вы можете выбрать набор операционных систем для каждого сервера PCN и SCN отдельно.

Ручная отправка файлов с хостов с компонентом Endpoint Agent на проверку в Sandbox

Вы можете включить ручную отправку файлов с хостов с компонентом Endpoint Agent на проверку компоненту Sandbox. Если функция включена, пользователь хоста с компонентом Endpoint Agent может проверить в Sandbox любой файл, который считает небезопасным.

Функция доступна, если компонент Endpoint Agent представлен приложениями Kaspersky Endpoint Security для Windows и/или Kaspersky Endpoint Security для Linux и для этих компонентов настроена интеграция с Kaspersky Anti Targeted Attack Platform.

Сценарий отправки файлов на проверку включает следующие этапы:

1. Включение ручной отправки файлов с хостов с компонентом Endpoint Agent на проверку компоненту Sandbox в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.
2. Отправка файлов на проверку через Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Security для Linux.
1.
2.
3.
4.

По результатам проверки Kaspersky Anti Targeted Attack Platform может записать алерт в базу алертов. Данные об этих алертах отображаются на виджете **Алерты по вектору атаки**.

В режиме распределенного решения и мультитенантности вам нужно включить ручную отправку файлов на проверку компоненту Sandbox на каждом сервере Central Node, на котором вы хотите использовать эту функцию. Если компонент Central Node развернут в виде кластера, вы можете включить функцию на любом сервере кластера.

Если вы используете только функциональность KATA (лицензионный ключ KATA), в веб-интерфейсе Kaspersky Anti Targeted Attack Platform в разделе **Endpoint Agents** отображается список хостов, с которых отправлялись файлы на проверку компоненту Sandbox. Вы можете просмотреть этот список и информацию о выбранном хосте.

Включение и отключение ручной отправки файлов с хостов Endpoint Agent на проверку в Sandbox

Чтобы включить или отключить ручную отправку файлов на проверку компоненту Sandbox:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Endpoint Agents**.
2. В блоке параметров **Отправка файлов с хостов на анализ в Sandbox вручную** выполните следующие действия:
   - Переместите переключатель **Отправлять файлы** в положение **Включено**, если хотите включить ручную отправку файлов на проверку компоненту Sandbox.

     По умолчанию функция включена.
   - Переместите переключатель **Отправлять файлы** в положение **Выключено**, если хотите отключить ручную отправку файлов на проверку компоненту Sandbox.
3. Нажмите на кнопку **Применить**.

Ручная отправка файлов с хостов Endpoint Agent на проверку компоненту Sandbox будет включена или отключена.

Настройка интеграции с внешними системами

Вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с внешними системами для проверки хранящихся в них файлов. Результаты их проверки будут отображаться в таблице алертов. В роли внешней системы также может выступать почтовый сенсор.

Если вы используете режим распределенного решения и мультитенантности, вам нужно настроить интеграцию внешней системы с тем сервером PCN или SCN, на котором вы хотите проверять данные из этой системы.

Предусмотрен следующий порядок интеграции Kaspersky Anti Targeted Attack Platform с внешними системами:

1. **Ввод параметров интеграции и создание запроса на интеграцию на стороне внешней системы**

   Подробнее о вводе параметров интеграции на стороне почтового сенсора см. Справку Kaspersky Secure Mail Gateway или Справку Kaspersky Security для Linux Mail Server.

   Для интеграции других внешних систем необходимо использовать REST API.

2. **Подтверждение интеграции на стороне Kaspersky Anti Targeted Attack Platform**

   Внешние системы должны использовать уникальные сертификаты для авторизации на сервере с компонентом Central Node. В этом случае в интерфейсе Kaspersky Anti Targeted Attack Platform будет отображаться один запрос на интеграцию. Для подключения нескольких внешних систем, имеющих один IP-адрес, вам необходимо использовать уникальный сертификат для каждой внешней системы.

   > При использовании одного сертификата вы сможете настроить интеграцию только с одной внешней системой.

3. **Проверка соединения внешней системы с Kaspersky Anti Targeted Attack Platform**

Просмотр таблицы внешних систем

Таблица внешних систем находится в разделе **Внешние системы** окна веб-интерфейса приложения. В таблице содержится следующая информация:

- **Sensor** – IP-адрес или доменное имя сервера внешней системы.
- **Тип** – тип внешней системы (почтовый сенсор или другая система).
- **Имя** – название интегрированной внешней системы, не являющейся почтовым сенсором.

  Для почтового сенсора в этом столбце отображается прочерк.
- **ID** – идентификатор внешней системы.

- **Отпечаток сертификата** – отпечаток TLS-сертификата сервера с внешней системой, с помощью которого устанавливается шифрованное соединение с сервером с компонентом Central Node.

  Отпечаток сертификата сервера с компонентом Central Node отображается в верхней части окна в поле **Отпечаток сертификата**.

- **Состояние** – состояние запроса на интеграцию.

В режиме распределенного решения и мультитенантности в таблице отображается информация только о внешних системах, подключенных к тому серверу Central Node, в веб-интерфейсе которого вы находитесь.

Обработка запроса от внешней системы

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы обработать запрос на интеграцию от внешней системы:

1. В окне веб-интерфейса приложения выберите раздел **Внешние системы**.

   В таблице **Список серверов** отобразятся уже подключенные внешние системы, а также запросы на интеграцию с Kaspersky Anti Targeted Attack Platform от внешних систем.

2. В строке с запросом на интеграцию выполните одно из следующих действий:

   - Если вы хотите настроить интеграцию с внешней системой, нажмите на кнопку **Принять**.
   - Если вы не хотите настраивать интеграцию с внешней системой, нажмите на кнопку **Отклонить**.

3. В окне подтверждения нажмите на кнопку **Да**.

Запрос на интеграцию от внешней системы будет обработан.

Удаление внешней системы из списка разрешенных к интеграции

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

После того как вы приняли запрос на интеграцию от внешней системы, вы можете удалить ее из списка разрешенных к интеграции. В этом случае соединение между Kaspersky Anti Targeted Attack Platform и внешней системой будет прервано.

Чтобы удалить внешнюю систему из списка разрешенных к интеграции:

1. В окне веб-интерфейса приложения выберите раздел **Внешние системы**.

   В списке **Список серверов** отобразятся уже добавленные внешние системы, а также запросы на интеграцию с Kaspersky Anti Targeted Attack Platform от внешних систем.

2. Нажмите на кнопку **Удалить** в строке с запросом на интеграцию от той внешней системы, которую вы хотите удалить.

3. В окне подтверждения нажмите на кнопку **Да**.

Внешняя система будет удалена из списка разрешенных к интеграции.

Настройка приоритета обработки трафика от почтовых сенсоров

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Вы можете включить или отключить максимальный приоритет обработки трафика от почтовых сенсоров.

Чтобы включить или отключить максимальный приоритет обработки трафика от почтовых сенсоров:

1. В окне веб-интерфейса приложения выберите раздел **Внешние системы**.

2. Выполните одно из следующих действий:

   - Включите переключатель рядом с названием параметра **Максимальный приоритет проверки**, если вы хотите включить максимальный приоритет обработки трафика от почтовых сенсоров.

   - Выключите переключатель рядом с названием параметра **Максимальный приоритет проверки**, если вы хотите отключить максимальный приоритет обработки трафика от почтовых сенсоров.

Приоритет обработки трафика от почтовых сенсоров будет настроен.

Настройка интеграции с Kaspersky Managed Detection and Response

Приложение Kaspersky Managed Detection and Response (далее также "MDR") предназначено для обнаружения и предотвращения мошеннических действий в инфраструктуре клиента. MDR обеспечивает непрерывную управляемую защиту и позволяет организациям автоматически выявлять труднообнаружимые угрозы и освобождать сотрудников группы IT-безопасности для решения задач, требующих их участия.

Kaspersky Anti Targeted Attack Platform получает данные и отправляет их в Kaspersky Managed Detection and Response с помощью потока Kaspersky Security Network. Поэтому для настройки интеграции с MDR обязательно участие в KSN.

Интеграция с MDR доступна только при наличии хотя бы одной действующей лицензий KATA или EDR. Если в приложении добавлен один лицензионный ключ (только KATA или только EDR), то статистика отправляется в рамках функциональности, предусмотренной этой лицензией. Если в приложении добавлено оба лицензионных ключа, то статистика отправляется в полном объеме.

Перед настройкой интеграции Kaspersky Anti Targeted Attack Platform с приложением MDR требуется получить архив с конфигурационным файлом на портале MDR.

Включение интеграции с MDR

Убедитесь, что в приложении добавлен активный лицензионный ключ и настроено участие в KSN. В противном случае интеграция с MDR будет недоступна.

Чтобы включить интеграцию с MDR:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. В блоке параметров **Интеграция MDR** нажмите на кнопку **Загрузить**, чтобы загрузить конфигурационный файл.

   Откроется окно выбора файлов.
4. Выберите архив, полученный при регистрации на портале MDR, и нажмите кнопку **Open**.

   В окне отобразится следующая информация о лицензии MDR:

   - **Серийный номер**.
   - **Дата окончания срока действия**.
   - **Осталось дней**.

Интеграция с MDR будет включена. Параметры интеграции, указанные в конфигурационном файле, будут распространены на все подключенные компоненты Sensor. Приложение MDR начнет использовать статистику о выявленных обнаружениях, отправляемую через поток KSN.

Отключение интеграции с MDR

Чтобы отключить интеграцию с MDR:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.

3. В блоке параметров **Интеграция MDR** нажмите на кнопку **Удалить файл**.

4. В окне подтверждения нажмите на кнопку **Да**.

Конфигурационный файл будет удален, а интеграция с MDR будет отключена. Приложение продолжит отправлять статистику на серверы KSN, однако эта информация не будет использоваться приложением MDR.

Замена конфигурационного файла MDR

Чтобы заменить конфигурационный файл MDR:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.

3. В блоке параметров **Интеграция MDR** нажмите на кнопку **Заменить файл**.

   Откроется окно выбора файла.

4. Выберите новый архив с конфигурационным файлом и нажмите на кнопку **Open**.

   В веб-интерфейсе приложения обновится информация о лицензии MDR.

Конфигурационный файл будет заменен. Новые параметры интеграции будут распространены на все подключенные компоненты Sensor.

Настройка интеграции с SIEM-системой

Kaspersky Anti Targeted Attack Platform может публиковать информацию о действиях пользователей в веб-интерфейсе приложения и алертах в *SIEM-систему*, которая уже используется в вашей организации, по протоколу Syslog.

Для передачи данных вы можете использовать TLS-шифрование.

Если вы развернули компоненты Central Node и Sensor в виде кластера, вы можете настроить отказоустойчивую интеграцию с внешней системой одним из следующих способов:

- Использовать функцию Round Robin.
- Настроить параметры внешней системы, чтобы при возникновении сетевой ошибки внешняя система переключалась между IP-адресами серверов кластера.

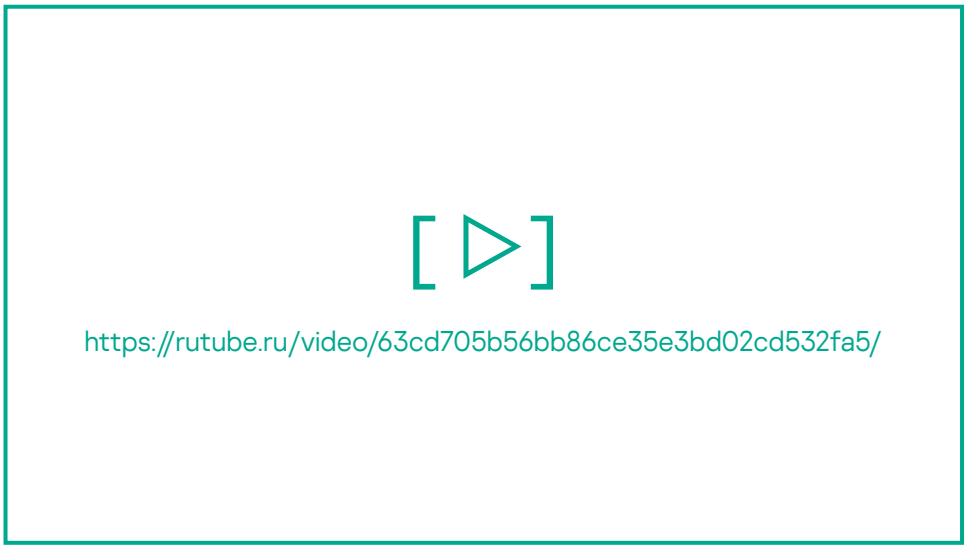
Чтобы настроить отказоустойчивую интеграцию с внешней системой с помощью функции Round Robin:

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.

2. В параметрах почтового сервера укажите это доменное имя.

Интеграция с внешней системой будет настроена по доменному имени. Внешняя система обратится к случайному серверу кластера. При отказе этого сервера внешняя система будет обращаться к другому работоспособному серверу кластера.

Посмотрите обучающее видео о настройке интеграции с SIEM-системой. Для воспроизведения видео вы можете запустить его на странице справки (см. ниже) или перейти по ссылке https://rutube.ru/video/63cd705b56bb86ce35e3bd02cd532fa5/?playlist=891497.



Настройка Central Node для интеграции KATA и KEDR Expert с KUMA

Включение и отключение записи информации в удаленный журнал

Вы можете настроить запись информации о действиях пользователей в веб-интерфейсе и обнаружениях в удаленный журнал. Файл журнала хранится на сервере, на котором установлена SIEM-система. Для записи в удаленный журнал необходимо настроить параметры интеграции с SIEM-системой.

Чтобы включить или отключить запись информации о действиях пользователей в веб-интерфейсе и обнаружениях в удаленный журнал:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Если вы хотите включить / отключить запись информации о действиях пользователей в веб-интерфейсе в удаленный журнал, выполните одно из следующих действий:
   - Если вы хотите включить запись информации о действиях пользователей в веб-интерфейсе, установите флажок **Активность пользователей**.
   - Если вы хотите отключить запись информации о действиях пользователей в веб-интерфейсе, снимите флажок **Активность пользователей**.
3. Если вы хотите включить / отключить запись информации об обнаружениях в удаленный журнал, выполните одно из следующих действий:
   - Если вы хотите включить запись информации об обнаружениях, установите флажок **Обнаружения**.
   - Если вы хотите отключить запись информации об обнаружениях, снимите флажок **Обнаружения**.

Вы можете установить оба флажка одновременно.

4. Нажмите на кнопку **Применить** в нижней части окна.

Запись информации в удаленный журнал будет включена или отключена.

Пользователи с ролью **Аудитор** могут только просматривать информацию о настройках записи в удаленный журнал.

Настройка основных параметров интеграции с SIEM-системой

Чтобы настроить основные параметры интеграции с SIEM-системой:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Установите флажки **Активность пользователей** и / или **Обнаружения**.

   Вы можете установить один из флажков или оба флажка одновременно.
3. В поле **Хост/IP** введите IP-адрес или имя хоста сервера вашей SIEM-системы.
4. В поле **Порт** введите номер порта подключения к вашей SIEM-системе.
5. В поле **Протокол** выберите **TCP** или **UDP**.
6. В поле **ID хоста** укажите идентификатор хоста. Хост с этим идентификатором в журнале SIEM-системы будет указан как источник обнаружения.
7. В поле **Периодичность сигнала** введите интервал отправки сообщений в SIEM-систему.
8. Нажмите на кнопку **Применить** в нижней части окна.

Основные параметры интеграции с SIEM-системой будут настроены.

Пользователи с ролью **Аудитор** могут только просматривать информацию о настройках интеграции с SIEM-системой.

Загрузка TLS-сертификата

Чтобы загрузить TLS-сертификат для шифрования соединения с SIEM-системой:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **SIEM-система**.
2. В разделе **TLS-шифрование** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

3. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

   TLS-сертификат будет добавлен в приложение.

4. Нажмите на кнопку **Применить** в нижней части окна.

Загруженный TLS-сертификат будет использоваться для шифрования соединения с SIEM-системой.

Включение и отключение TLS-шифрования соединения с SIEM-системой

Чтобы включить или отключить TLS-шифрование соединения с SIEM-системой:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Установите флажки **Активность пользователей** и / или **Алерты**.

   Вы можете установить один из флажков или оба флажка одновременно.
3. В разделе **TLS-шифрование** выполните одно из следующих действий:

   - Включите переключатель рядом с названием параметра **TLS-шифрование**, если вы хотите включить TLS-шифрование соединения с SIEM-системой.
   - Выключите переключатель рядом с названием параметра **TLS-шифрование**, если вы хотите отключить TLS-шифрование соединения с SIEM-системой.

   Переключатель рядом с названием параметра **TLS-шифрование** доступен, только если загружен TLS-сертификат.
4. Нажмите на кнопку **Применить** в нижней части окна.

TLS-шифрование соединения с SIEM-системой будет включено или отключено.

Содержание и свойства syslog-сообщений об обнаружениях

Информация о каждом обнаружении передается в отдельной syslog-категории (syslog facility), которая не используется системой для передачи сообщений от других источников. Информация о каждом обнаружении передается как отдельное syslog-сообщение формата CEF. Если обнаружение выполнено модулем Targeted Attack Analyzer, то информация о нем передается в виде нескольких отдельных syslog-сообщений формата CEF.

Максимальный размер syslog-сообщения об обнаружении по умолчанию составляет 32 Кб. Сообщения, превышающие максимальный размер, обрываются в конце.

В заголовке каждого syslog-сообщения об обнаружении содержится следующая информация:

- Версия формата.

  Номер текущей версии: `0`. Текущее значение поля: `CEF:0`.

- Производитель.

  Текущее значение поля: `AO Kaspersky Lab`.

- Название приложения.

  Текущее значение поля: `Kaspersky Anti Targeted Attack Platform`.

- Версия приложения.

  Текущее значение поля: 7.1.1.531.

- Тип обнаружения.

  См. таблицу ниже.

- Наименование события.

  См. таблицу ниже.

- Важность обнаружения.

  Допустимые значения поля: `Low`, `Medium`, `High` или `0` (для сообщений типа `heartbeat`).

- Дополнительная информация.

  Пример:
  ```
  CEF:0|AO Kaspersky Lab| Kaspersky Anti Targeted Attack Platform |7.1.1.531|url_web| URL from web detected|Low|
  ```

Тело syslog-сообщения об обнаружении соответствует информации об этом обнаружении, отображающейся в веб-интерфейсе приложения. Все поля представлены в формате `"<ключ>=<значение>"`. В зависимости от того, в сетевом или почтовом трафике произошло обнаружение, а также от технологии, при проверке которой был создан , в теле syslog-сообщения могут передаваться разные ключи. Если значение пустое, то ключ не передается.

Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
`file_web`	`File from web detected` В сетевом трафике обнаружен файл.	• `dvchost` = <имя сервера с компонентом Central Node>. • `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения по UTC>. • `dst` = <IP-адрес назначения>. • `dpt` = <порт назначения>. • `src` = <IP-адрес источника>. • `spt` = <порт источника>. • `shost` = <имя хоста, на котором обнаружен файл>. • `suser` = <имя пользователя>. • `fName` = <имя файла внутри составного объекта>. • `fsize` = <размер файла внутри составного объекта (в байтах)>. • `fileType` = <формат файла внутри составного объекта>. • `fileHash` = <MD5-хеш файла внутри составного объекта >. • `KasperskyLabKATAcompositeFilePath` = <имя составного объекта>. • `KasperskyLabKATAcompositeFileSize` = <общий размер составного объекта (в байтах)>. • `KasperskyLabKATAcompositeFileHash` = <MD5-хеш составного объекта>. • `KasperskyLabKATAfileSHA256` = <SHA256-хеш составного объекта>. • `cs2` = <технология, с помощью которой обнаружен файл>. • `cs3Label` = <имя виртуальной машины, на которой обнаружен файл> (только для компонента Sandbox). • `cs1` = <список типов обнаруженных объектов по классификации "Лаборатории Касперского">. • `cs3` = <версия баз, с помощью которых проверен файл>. • `app` = <название протокола прикладного уровня> (HTTP(S) или FTP). • `requestMethod` = <метод HTTP-запроса> (только для протокола HTTP(S)). • `requestClientApplication` = <User Agent клиентского компьютера> (только для протокола HTTP(S)). • `request` = <URL обнаруженного объекта> (только для протокола HTTP(S)). • `requestContext` = <HTTP-заголовок Referer> (только для протокола HTTP(S)).
`file_mail`	`File from mail detected` В почтовом трафике обнаружен файл.	• `dvchost` = <имя сервера с компонентом Central Node>. • `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения по UTC>. • `fName` = <имя файла внутри составного объекта>. • `fsize` = <размер файла внутри составного объекта (в байтах)>. • `fileType` = <формат файла внутри составного объекта >. • `fileHash` = <MD5-хеш файла внутри составного объекта >. • `KasperskyLabKATAcompositeFilePath` = <имя составного объекта>. • `KasperskyLabKATAcompositeFileSize` = <общий размер составного объекта (в байтах)>. • `KasperskyLabKATAcompositeFileHash` = <MD5-хеш составного объекта>. • `KasperskyLabKATAfileSHA256` = <SHA256-хеш составного объекта>. • `KasperskyLabKATAmailEnvelopeFrom` = <адрес электронной почты отправителя> (из заголовка Received). • `KasperskyLabKATAmailFor` = <адрес электронной почты получателя> (из заголовка Received). • `KasperskyLabKATAmailRecievedFromIp` = <IP-адрес первого в цепочке отправки сообщения сервера> (из заголовка Received). • `cs2` = <технология, с помощью которой обнаружен файл>. • `cs3Label` = <имя виртуальной машины, на которой обнаружен файл> (только для компонента Sandbox). • `cs1` = <список типов обнаруженных объектов по классификации "Лаборатории Касперского">. • `cs3` = <версия баз, с помощью которых проверен файл>. • `externalId` = <ID сообщения электронной почты>. • `suser` = <адрес электронной почты отправителя>. • `duser` = <адреса электронной почты получателей>. • `msg` = <тема сообщения>.
`ids`	`IDS event detected` Обнаружение выполнено модулем Intrusion Detection System.	• `dvchost` = <имя сервера с компонентом Central Node>. • `eventId` = <ID обнаружения>. • `requestMethod` = <метод HTTP-запроса> (только для протокола HTTP(S)). • `requestClientApplication` = <User Agent клиентского компьютера> (только для протокола HTTP(S)). • `rt` = <дата и время обнаружения по UTC>.

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
		• `dst` = <IP-адрес назначения>. • `dpt` = <порт назначения>. • `src` = <IP-адрес источника>. • `spt` = <порт источника>. • `proto` = <название протокола транспортного уровня> (TCP или UDP). • `cs1` = <тип обнаруженного объекта по классификации "Лаборатории Касперского">. • `cs2Label` = <название правила IDS>. • `cs2` = <номер правила IDS>. • `cs3` = <версия баз модуля Intrusion Detection System>. • `requestMethod` = <метод HTTP-запроса> (только для протокола HTTP). • `requestClientApplication` = <User Agent клиентского компьютера> (только для протокола HTTP). • `request` = <URL обнаруженного объекта>.
`url_web`	`URL from web detected` Обнаружение выполнено технологией URL Reputation или Sandbox в сетевом трафике.	• `dvchost` = <имя сервера с компонентом Central Node>. • `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения по UTC>. • `dst` = <IP-адрес назначения>. • `dpt` = <порт назначения>. • `src` = <IP-адрес источника>. • `spt` = <порт источника>. • `shost` = <имя хоста, на котором обнаружен файл>. • `suser` = <имя пользователя>. • `cs1` = <список категорий, к которым принадлежит URL-адрес обнаруженного объекта>. • `requestMethod` = <метод HTTP-запроса>. • `requestClientApplication` = <User Agent клиентского компьютера>. • `request` = <URL-адрес обнаруженного объекта>. • `requestContext` = <HTTP-заголовок Referer>. • `reason` = <код HTTP-ответа>.
`url_mail`	`URL from mail detected` Обнаружение выполнено технологией URL Reputation или Sandbox в почтовом трафике.	• `dvchost` = <имя сервера с компонентом Central Node>. • `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения по UTC>. • `externalId` = <ID сообщения электронной почты>. • `suser` = <адрес электронной почты отправителя>. • `duser` = <адреса электронной почты получателей>. • `KasperskyLabKATAmailEnvelopeFrom` = <адрес электронной почты отправителя> (из заголовка Received). • `KasperskyLabKATAmailFor` = <адрес получателя> (из заголовка Received). • `KasperskyLabKATAmailRecievedFromIp` = <IP-адрес первого в цепочке отправки сообщения сервера> (из заголовка Received). • `msg` = <тема сообщения>. • `request` = <URL-адрес обнаруженного объекта>. • `cs2` = <технология, с помощью которой Обнаружение выполнено> (Sandbox или URL Reputation). • `cs3Label` = <имя виртуальной машины, на которой обнаружен файл> (только для Sandbox). • `cs1` = <список типов обнаруженных объектов по классификации "Лаборатории Касперского"> (для Sandbox) или <список категорий> (для URL Reputation). • `cs3` = <версия баз, с помощью которых проверен файл> (только для Sandbox).
`dns`	`DNS request detected` Обнаружение выполнено технологией URL Reputation в DNS-трафике.	• `dvchost` = <имя сервера с компонентом Central Node>. • `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения по UTC>. • `dst` = <IP-адрес назначения>. • `dpt` = <порт назначения>. • `src` = <IP-адрес источника>. • `spt` = <порт источника>. • `shost` = <имя хоста, на котором обнаружен файл>. • `suser` = <имя пользователя>. • `cs2` = <список URL-категорий, к которым принадлежат доменные имена>. • `requestMethod` = <тип DNS-сообщения> (request или response). • `flexString1` = <тип записи из DNS-запроса>. • `dhost` = <имя хоста из DNS-запроса>. • `cs1` = <список доменных имен из DNS-ответа>.
`file_endpoint`	`File from endpoint detected`	• `dvchost` = <имя сервера с компонентом Central Node>.

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
	Обнаружение выполнено компонентом Endpoint Agent на хосте пользователя и содержит файл.	• `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения по UTC>. • `src` = <IP-адрес источника>. • `shost` = <имя хоста, на котором обнаружен файл>. • `fName` = <имя файла внутри составного объекта>. • `fsize` = <размер файла внутри составного объекта (в байтах)>. • `fileType` = <формат файла внутри составного объекта >. • `fileHash` = <MD5-хеш файла внутри составного объекта >. • `KasperskyLabKATAcompositeFilePath` = <имя составного объекта>. • `KasperskyLabKATAcompositeFileSize` = <общий размер составного объекта (в байтах)>. • `KasperskyLabKATAcompositeFileHash` = <MD5-хеш составного объекта>. • `KasperskyLabKATAfileSHA256` = <SHA256-хеш составного объекта>. • `cs2` = <технология, с помощью которой обнаружен файл>. • `cs3Label` = <имя виртуальной машины, на которой обнаружен файл> (только для компонента Sandbox). • `cs1` = <список типов обнаруженных объектов по классификации "Лаборатории Касперского">. • `cs3` = <версия баз, с помощью которых проверен файл>. • `app` = <название протокола прикладного уровня> (HTTP(S) или FTP). • `FilePath` = <путь к файлу на компьютере с компонентом Endpoint Agent>.
`iocScanning`	`IOC has tripped on endpoint` Обнаружение выполнено в результате IOC-проверки хостов с компонентом Endpoint Agent для Windows. Этот тип алертов доступен, если вы используете функциональность KEDR.	• `dvchost` = <имя сервера с компонентом Central Node>. • `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения по UTC>. • `src` = <IP-адрес источника>. • `shost` = <имя хоста, на котором обнаружен файл>. • `cs1` = <имя IOC-файла, по которому создан алерт>.
`taaScanning`	`TAA has tripped on events database` Обнаружение выполнено в результате IOA-анализа событий. Этот тип обнаружений доступен, если вы используете функциональность KEDR.	• `dvchost` = <имя сервера с компонентом Central Node>. • `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения по UTC>. • `shost` = <имя хоста, на котором Обнаружение выполнено>. • `cs1` = <имя IOA-правила, по которому создан алерт>.
`yaraScanningEP`	`YARA has tripped on endpoint` Обнаружение выполнено в результате YARA-проверки хостов с компонентом Endpoint Agent для Windows. Этот тип обнаружений доступен, если вы используете функциональность KEDR.	• `dvchost` = <имя сервера с компонентом Central Node>. • `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения по UTC>. • `src` = <IP-адрес источника>. • `shost` = <имя хоста, на котором Обнаружение выполнено>. • `cs1` = <имя YARA-правила, по которому создан алерт>.
`heartbeat`	Периодическое сообщение, содержащее статус компонентов.	• `dvchost` = <имя сервера с компонентом Central Node>. • `rt` = <дата и время события по UTC>. • `KasperskyLabKATAcomponentName` = <название компонента>. • `KasperskyLabKATAcomponentState` = <статус компонента> (`0` – OK, `>0` – Ошибка).

Управление коннекторами

Этот раздел содержит информацию об управлении коннекторами в Kaspersky Anti Targeted Attack Platform. *Коннекторы* – это специальные программные модули, которые обеспечивают обмен данными с Kaspersky Anti Targeted Attack Platform и могут предоставлять возможности выполнения управляющих действий в самом приложении или с помощью приложения.

Коннекторы расширяют функциональность приложения для взаимодействия со сторонними системами. В зависимости от своего функционального назначения, коннекторы могут передавать данные в сторонние системы (например, передавать события, сообщения приложения и записи аудита в SIEM-систему) или обеспечивать получение данных от сторонних систем. Также в приложении могут использоваться коннекторы для проведения активных опросов устройств.

Компьютеры, на которых работают программные модули коннекторов, называется *узлами размещения коннекторов*. В качестве узла размещения коннектора вы можете использовать любой компьютер, имеющий сетевой доступ к компьютеру сервера Central Node (в том числе узлы с установленными компонентами приложения, включая и компьютер самого сервера Central Node).

Таблицы коннекторов и типов коннекторов отображаются в разделе **Параметры**, подразделе **Коннекторы** веб-интерфейса приложения. Управлять коннекторами и типами коннекторов могут только пользователи с ролью Администратор. Пользователи с ролями **Аудитор**, **Сотрудник службы безопасности** и **Старший сотрудник службы безопасности** могут просматривать коннекторы и типы коннекторов.

Функциональные возможности коннектора зависят от выбранного *типа коннектора*. Вы можете выбрать нужный тип коннектора при добавлении коннектора в приложение. По умолчанию в приложение встроены следующие типы коннекторов:

- **Syslog**

  Этот тип коннектора предоставляет возможности отправки данных на сервер Syslog.

  При добавлении коннектора типа **Syslog** или при изменении параметров вам нужно настраивать не только общие параметры коннектора, но и дополнительные параметры, сгруппированные в блоке **Детали**:

  - Адрес сервера Syslog.
  - Порт сервера Syslog.
  - Протокол передачи данных.

- **SIEM**

  Этот тип коннектора предоставляет возможности отправки данных на сервер SIEM-системы.

  При добавлении коннектора типа **SIEM** или при изменении параметров вам нужно настраивать не только общие параметры коннектора, но и дополнительные параметры, сгруппированные в блоке **Детали**:

  - Адрес сервера SIEM-системы.
  - Порт сервера SIEM-системы.
  - Протокол передачи данных.

- **Generic**

  Этот тип коннектора предоставляет возможности подключения приложений, использующих NDR API.

- **Email**

  Этот тип коннектора предоставляет возможности отправки данных в сообщениях электронной почты.

  При добавлении коннектора типа **Email** или при изменении параметров вам нужно настраивать не только общие параметры коннектора, но также и дополнительные параметры, сгруппированные в блоке **Детали**:

  - Адрес, указываемый в качестве отправителя сообщений электронной почты.
  - Адреса получателей сообщений электронной почты.
  - Темы сообщений электронной почты для событий, сообщений приложения и записей аудита.
  - Шаблоны текстовых описаний для событий, сообщений приложения, записей аудита, описаний сетевых взаимодействий и для всего письма с уведомлениями. Шаблоны составляются с использованием переменных.

- Тема и текст письма для сообщения электронной почты о достижении максимального количества отправленных уведомлений.
- Максимальное количество отправляемых сообщений электронной почты в сутки.
- Максимальное количество уведомлений в каждом сообщении. Определяет максимальное количество зарегистрированных уведомлений одного типа (событий, сообщений приложения или записей аудита), которые можно поместить в одно сообщение электронной почты. Если зарегистрированных уведомлений больше, то формируется дополнительное сообщение электронной почты (в пределах суточного ограничения).

Для работы коннектора типа **Email** следует предварительно настроить соединение с почтовым сервером.

- **Active poll**

  Этот тип коннектора предоставляет возможности активного опроса устройств в рамках заданий контроля конфигураций и заданий активных опросов.

  При добавлении коннектора типа **Active poll** или при изменении параметров вам нужно настраивать не только общие параметры коннектора, но также и дополнительные параметры, сгруппированные в блоке **Детали**:

  - Методы проведения активных опросов, которые будут доступны пользователю приложения при использовании коннектора.
  - Диапазоны разрешенных и запрещенных IP-адресов устройств, по которым будет разрешено и запрещено проведение активных опросов. Адрес `0.0.0.0` соответствует всем возможным IP-адресам.

    Если адрес входит в диапазон как разрешенных, так и запрещенных IP-адресов, то Kaspersky Anti Targeted Attack Platform отнесет его к запрещенным IP-адресам.
  - Имена адресных пространств, для устройств которых будет разрешено проведение активных опросов. Если требуется, вы можете выбрать адресные пространства для IP-адресов в поле **Адресное пространство L3** и для MAC-адресов в поле **Адресное пространство L2**.

    При выборе адресного пространства, отличающегося от адресного пространства **Default**, вам нужно добавить новое правило для этого адресного пространства или изменить имеющееся правило. В правиле должен быть указан коннектор, для которого выбрано это адресное пространство. Настройка параметров правил выполняется при изменении адресного пространства.

- **KUMA**

  Этот тип коннектора предоставляет возможности интеграции с программным решением Kaspersky Unified Monitoring and Analysis Platform (далее также KUMA). Программные модули для коннекторов данного типа поставляются отдельно от Kaspersky Anti Targeted Attack Platform. С помощью коннектора данного типа вы можете отправлять в KUMA сведения об устройствах и рисках, а также применять в KUMA команды на изменение статусов устройств. После добавления коннектора требуется настроить интеграцию в KUMA (создать подключение к Kaspersky Anti Targeted Attack Platform). Взаимодействие коннектора KUMA с сервером Central Node выполняется с использованием Kaspersky Anti Targeted Attack Platform API.

  Коннектор KUMA обеспечивает интеграцию в части отправки сведений об устройствах и рисках и применения команд на изменение статусов устройств. Для отправки событий в KUMA вы можете добавить в Kaspersky Anti Targeted Attack Platform коннектор типа **Syslog** или **SIEM** и указать для этого коннектора данные для подключения к серверу KUMA. После добавления коннектора требуется настроить коллектор на стороне KUMA.

- **Cisco Switch**

  Этот тип коннектора предоставляет возможности автоматического управления сетевым доступом устройств с использованием сетевых коммутаторов Cisco.

  При добавлении коннектора типа **Cisco Switch** или при изменении параметров вам нужно настраивать не только общие параметры коннектора, но также и дополнительные параметры, сгруппированные в блоке **Детали**:

  - Имя коммутатора, которое будет указываться в событиях выполненных действий приложения с помощью коннектора.
  - Адресная информация для подключения коннектора к сетевому коммутатору: IP-адрес и SSH-порт.
  - Учетные данные для установки SSH-соединения с сетевым коммутатором.
  - Открытый ключ, используемый для проверки совпадения с полученным открытым ключом сетевого коммутатора перед установкой SSH-соединения с целью защиты от подмены этого устройства в сети. Если значение пустое, то проверка не выполняется.
  - Используемый метод для ограничения сетевого доступа устройств. Предусмотрены методы создания правил блокировки в списках контроля доступа коммутатора по MAC-адресам (MAC ACL), по IP-адресам (IP ACL), а также с отключением Ethernet-портов, к которым подключены устройства.

    Для использования метода отключения Ethernet-портов вам нужно настроить конфигурацию подключений к сетевому коммутатору таким образом, чтобы исключить соединение нескольких устройств через один порт. Иначе при отключении Ethernet-порта для блокировки одного устройства сетевой доступ будет также заблокирован для всех устройств, которые соединены с сетью через этот порт.

  - Параметр сброса правил блокировки при изменении метода ограничения сетевого доступа. Если параметр включен, при изменении метода сбрасываются правила, которые ранее были заданы для блокировки устройств.
  - Параметр исключения сетевых устройств для применения метода ограничения сетевого доступа. Если параметр включен, метод не применяется к устройствам категорий **Сетевое устройство**, **Брандмауэр**, **Коммутатор**, **Виртуальный коммутатор**, **Маршрутизатор**, **Виртуальный маршрутизатор**, **Wi-Fi**.
  - Параметр применения правил блокировки только к новым устройствам. Если параметр включен, метод применяется только к тем неразрешенным устройствам, для которых зарегистрировано событие обнаружения нового устройства с кодом типа события 4000005003.
  - Длительность интервала времени между запросами данных о наличии устройств со статусами *Разрешенное* и *Неразрешенное* в таблице устройств.
  - Параметр отправки уведомлений о заблокированных устройствах при перезапуске коннектора. Если параметр включен, после включения или перезапуска коннектора на сервер Central Node отправляется список устройств, для которых ранее были применены ограничения сетевого доступа.

При необходимости в приложение можно добавлять другие типы коннекторов, которые будут обеспечивать обмен данными или предоставлять возможности выполнения управляющих действий при взаимодействии приложения с другими сторонними системами.

Для соединений коннекторов с сервером Central Node используются определенные порты и протоколы.

Подключение сторонней системы через коннектор выполняется от имени одного из пользователей приложения. Для каждого коннектора рекомендуется использовать отдельную учетную запись пользователя. За счет этого вам будет удобнее анализировать действия, которые выполнялись через коннекторы, по записям аудита.

Максимальное количество коннекторов в приложении – 20. Максимальное количество типов коннекторов – 100.

Об управляемых и неуправляемых коннекторах

В приложении могут использоваться управляемые и неуправляемые коннекторы.

Коннектор является *управляемым*, если для его программных модулей доступны функции автоматической регистрации и запуска после добавления коннектора, а также функции управления этими модулями при включении и выключении коннектора и при его удалении. Узлами размещения управляемых коннекторов могут быть только узлы с установленными компонентами приложения.

Неуправляемый коннектор не предоставляет функции управляемого коннектора. Регистрацию такого коннектора, а также запуск, остановку и удаление его программных модулей требуется выполнять вручную на узле размещения коннектора. При включении и выключении неуправляемого коннектора приложение соответственно разрешает и запрещает взаимодействие с коннектором на стороне сервера Central Node.

Безопасность соединений коннекторов с сервером Central Node приложения обеспечивается с использованием сертификатов. Сертификаты для коннекторов создаются при добавлении коннекторов в приложение. Для программных модулей управляемых коннекторов приложение автоматически передает созданные сертификаты. При добавлении неуправляемого коннектора (или при добавлении управляемого коннектора с включенным режимом игнорирования функций управляемого коннектора) сертификат для программных модулей этого коннектора требуется загрузить вручную с помощью файла свертки. При необходимости заменить (выпустить новый) сертификат для такого коннектора вам нужно создать новый файл свертки и использовать этот файл для загрузки нового сертификата. Замена сертификатов управляемых коннекторов возможна только путем удаления и повторного добавления этих коннекторов.

Об отправке событий, сообщений приложения и записей аудита в сторонние системы

Вы можете настроить отправку событий, сообщений приложения или записей аудита (далее также "зарегистрированные уведомления") в стороннюю систему с помощью коннекторов. Для типов коннекторов **Syslog**, **SIEM**, **Email** возможность отправки зарегистрированных уведомлений включена по умолчанию. Для типа коннектора **KUMA** возможность отправки зарегистрированных уведомлений доступна при наличии установленных программных модулей. При использовании других типов коннекторов, добавленных в приложение, эта возможность доступна в зависимости от заданных параметров для этих типов коннекторов.

Параметры отправки зарегистрированных уведомлений настраиваются для каждого коннектора. При настройке типов событий вы можете выбрать нужные типы событий для передачи через коннекторы. При создании коннектора или при изменении его параметров вы можете включить или выключить отправку всех сообщений приложения и всех записей аудита через этот коннектор.

Коннектор типа **Email** предоставляет возможность ограничения объема передаваемых данных. Для этого типа коннектора можно задать максимальное количество сообщений электронной почты о новых зарегистрированных уведомлениях и максимальное количество зарегистрированных уведомлений в каждом сообщении. Если отправлено максимальное количество сообщений электронной почты, получателям отправляется ещё одно сообщение о превышении максимального количества. После этого новые сообщения не будут отправляться до конца текущих суток в часовом поясе сервера Central Node.

Сообщения электронной почты, отправляемые через коннектор **Email**, формируются раздельно для каждого типа зарегистрированных уведомлений. То есть для отправки событий, сообщений приложения и записей аудита формируются разные сообщения электронной почты.

Содержание и порядок сведений о зарегистрированных уведомлениях, которые передаются через коннекторы типов **Syslog** и **SIEM**, могут отличаться в этих системах от содержания и порядка сведений, отображаемых на страницах веб-интерфейса Kaspersky Anti Targeted Attack Platform.

Об автоматическом управлении сетевым доступом устройств с помощью коннекторов типа Cisco Switch

Вы можете настроить автоматическое управление сетевым доступом устройств с помощью коннекторов типа **Cisco Switch**. Коннекторы этого типа соединяются с сетевыми коммутаторами и отправляют на эти коммутаторы команды, добавляющие или удаляющие правила блокировки (ограничения) сетевого доступа для устройств, которые подключены к коммутаторам.

Управление сетевым доступом устройств осуществляется в зависимости от их статусов. Коннектор создает на сетевом коммутаторе правила блокировки для устройств со статусом *Неразрешенное* и удаляет такие правила после присвоения устройствам статуса *Разрешенное*.

Каждый коннектор может устанавливать соединение только с одним сетевым коммутатором.

Ограничение сетевого доступа с помощью коннектора типа **Cisco Switch** выполняется для тех устройств, в сведениях о которых указаны их MAC-адреса. Также эти MAC-адреса должны храниться в ARP-таблице сетевого коммутатора. То есть устройства с этими MAC-адресами должны быть подключены к сетевому коммутатору, с которым соединяется коннектор.

Коннектор может использовать различные методы для ограничения сетевого доступа устройств. Предусмотрены методы создания правил блокировки в списках контроля доступа коммутатора по MAC-адресам (MAC ACL), по IP-адресам (IP ACL), а также с отключением Ethernet-портов, к которым подключены устройства.

Для использования метода отключения Ethernet-портов вам нужно настроить конфигурацию подключений к сетевому коммутатору таким образом, чтобы исключить соединение нескольких устройств через один порт. Иначе при отключении Ethernet-порта для блокировки одного устройства сетевой доступ будет также заблокирован для всех устройств, которые соединены с сетью через этот порт.

Для минимизации рисков влияния коннектора на сетевую доступность устройств вы можете включить следующие параметры при настройке коннектора:

- Параметр исключения сетевых устройств для применения метода ограничения сетевого доступа. Если параметр включен, метод не применяется к устройствам категорий **Сетевое устройство**, **Брандмауэр**, **Коммутатор**, **Виртуальный коммутатор**, **Маршрутизатор**, **Виртуальный маршрутизатор**, **Wi-Fi**.

- Параметр применения правил блокировки только к новым устройствам. Если параметр включен, метод применяется только к тем неразрешенным устройствам, для которых зарегистрировано событие обнаружения нового устройства с кодом типа события 4000005003.

Коннектор соединяется с сетевым коммутатором путем установки SSH-соединения. Учетные данные для установки SSH-соединения указываются при настройке параметров коннектора и сохраняются в нем. Эти учетные данные, представляющие идентификационную и аутентификационную информацию, требуется защищать от компрометации. Для защиты от компрометации, которая возможна в случае подмены сетевого коммутатора, в коннекторе предусмотрена функция проверки сохраненного открытого ключа коммутатора и полученного открытого ключа. Передача идентификационной и аутентификационной информации на сетевой коммутатор происходит после проверки идентичности полученного открытого ключа и открытого ключа, сохраненного в коннекторе.

В процессе работы коннектор регистрирует в приложении события по результатам выполненных действий. События регистрируются по технологии Внешние системы. Предусмотрены события со следующими заголовками:

- `Для коммутатора <имя коммутатора> сброшены правила блокировки устройств`

  Это событие регистрируется, если при изменении метода ограничения сетевого доступа в коннекторе сброшены правила, которые ранее были заданы для блокировки устройств.

- `Обновлены сведения об устройстве <имя устройства> с адресом <MAC-адрес устройства> по данным от коммутатора <имя коммутатора>`

  Это событие регистрируется, если от сетевого коммутатора получена информация о подключении устройства к определенному порту.

- `Добавлено правило блокировки устройства <имя устройства> на коммутаторе <имя коммутатора>`

  Это событие регистрируется, если ограничен сетевой доступ неразрешенного устройства.

- `Удалено правило блокировки устройства <имя устройства> на коммутаторе <имя коммутатора>`

  Это событие регистрируется, если снято ограничение сетевого доступа устройства.

- `На коммутаторе <имя коммутатора> есть правила блокировки устройств, добавленные ранее`

  Это событие регистрируется, если после включения или перезапуска коннектора найдены устройства, для которых ранее были применены ограничения сетевого доступа.

- `Установлено SSH-соединение с коммутатором <имя коммутатора> без проверки открытого ключа`

  Это событие регистрируется, если коннектор установил SSH-соединение с сетевым коммутатором, однако проверка полученного открытого ключа коммутатора не выполнена. В этом случае вам нужно убедиться в отсутствии подменного устройства в сети и после этого сохранить в параметрах коннектора полученный открытый ключ.

- `Обнаружено несовпадение открытого ключа коммутатора <имя коммутатора>`

  Это событие регистрируется, если при проверке полученного открытого ключа сетевого коммутатора обнаружено несовпадение со значением, сохраненным в параметрах коннектора. Из-за этого SSH-соединение с коммутатором не установлено. В этом случае вам нужно убедиться как в отсутствии подменного устройства в сети, так и в действительном изменении открытого ключа коммутатора и после этого сохранить в параметрах коннектора полученный открытый ключ.

- `Отказ в установке SSH-соединения с коммутатором <имя коммутатора>: неверные учетные данные`

  Это событие регистрируется, если коннектору не удалось установить SSH-соединение с коммутатором из-за неверно указанных учетных данных в параметрах коннектора (имя пользователя или пароль).

- `На коммутаторе <имя коммутатора> не выполнено действие для привилегированного режима: неверный пароль`

  Это событие регистрируется, если коннектору недоступны функции привилегированного режима для выполнения действий по добавлению и удалению правил блокировки устройств на коммутаторе. В этом случае вам нужно ввести правильный пароль привилегированного режима в параметрах коннектора.

Добавление коннектора

Вы можете добавить коннектор на основе одного из типов коннекторов, доступных в приложении. Неуправляемый коннектор следует создавать только на основе пользовательских типов коннекторов.

Перед добавлением коннектора рекомендуется создать отдельную учетную запись пользователя, под которым сторонняя система будет подключаться к приложению. Для работы коннектора типа **Email** следует предварительно настроить соединение с почтовым сервером.

Чтобы добавить коннектор:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Параметры**, подраздел **Коннекторы**.
3. На вкладке **Коннекторы** откройте область деталей по кнопке **Добавить коннектор**.
4. Настройте общие параметры коннектора:
   a. Выберите нужный тип коннектора и введите имя коннектора.
   b. Если вы хотите добавить неуправляемый коннектор (или коннектор с включенным режимом игнорирования функций управляемого коннектора), введите пароль для доступа к сертификату коннектора.

      С использованием заданного пароля будет зашифрован сертификат в файле свертки коннектора.
   c. Укажите адрес сервера Central Node.

      По указанному адресу коннектор будет подключаться к Central Node.

d. Укажите узел размещения коннектора:

- Если вы хотите добавить управляемый коннектор, в качестве узла размещения коннектора вы можете указать один из узлов с установленными компонентами приложения.
- Если вы хотите добавить неуправляемый коннектор, вам нужно ввести IP-адрес компьютера, на котором будут работать программные модули коннектора.

e. Выберите пользователя, под которым сторонняя система будет подключаться к приложению через коннектор. Требуется указать имя одного из пользователей приложения.

5. В блоке **Детали** укажите дополнительные параметры в зависимости от типа коннектора. Блок **Детали** отсутствует в области деталей, если тип коннектора не предусматривает настройку дополнительных параметров.

6. Если тип коннектора предусматривает возможность передачи записей аудита и сообщений приложения, включите или выключите отправку этих данных с помощью соответствующих флажков.

7. При необходимости введите описание коннектора.

8. Нажмите на кнопку **Сохранить**.

Новый коннектор появится в таблице коннекторов.

Если добавлен неуправляемый коннектор, Central Node сформирует файл свертки для нового коннектора, после чего браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла. Содержимое полученного файла свертки вам нужно загрузить в приложение, которое будет использовать коннектор.

Просмотр таблицы коннекторов

Таблица коннекторов отображается в разделе **Параметры**, подразделе **Коннекторы** на вкладке **Коннекторы**.

Параметры коннекторов отображаются в следующих столбцах таблицы:

- **Имя**.

  Заданное имя коннектора.

- **ID коннектора**.

  Идентификатор, присвоенный коннектору при его создании.

- **Включен**.

  Признак готовности Central Node к взаимодействию с программными модулями коннектора. Если параметр имеет значение **Нет**, сервер Central Node не принимает запросы от программных модулей коннектора.

- **Статус**.

Статус работы программных модулей коннектора. Предусмотрены следующие статусы:

- **Ожидает регистрации** – после добавления неуправляемого коннектора или после создания нового файла свертки для неуправляемого коннектора подключение через этот коннектор еще не выполнялось.
- **Переключение** – происходит переключение режима работы программных модулей коннектора из статуса **Не работает** в статус **Работает** или обратно.
- **Не работает** – сервер Central Node не принимает запросы от программных модулей коннектора. Если коннектор управляемый, для его программных модулей отправлена команда остановки работы.
- **Работает** – выполнено успешное подключение через коннектор с использованием сертификата, созданного для этого коннектора.
- **Ошибка** – возникла ошибка при попытке выполнения действий с программными модулями коннектора.

- **Тип**.

  Значок и название типа коннектора.

- **Последнее подключение**.

  Дата и время последнего подключения через коннектор.

- **Управляемый**.

  Признак управляемого коннектора. Если параметр имеет значение **Нет**, коннектор является неуправляемым или для коннектора включен режим игнорирования функций управляемого коннектора.

- **Изменен**.

  Дата и время последнего изменения параметров коннектора.

- **Описание**.

  Заданное описание коннектора.

При просмотре таблицы коннекторов вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Включение и выключение коннектора

Если вы хотите временно запретить подключение программных модулей коннектора к серверу Central Node, вы можете выключить этот коннектор. Для возобновления подключения вам потребуется включить коннектор.

Чтобы включить или выключить коннектор:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Параметры**, подраздел **Коннекторы**.
3. На вкладке **Коннекторы** выберите коннектор, который вы хотите включить или выключить.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на нужную кнопку: **Включить** или **Выключить**.

   Откроется окно с запросом подтверждения.

5. В окне запроса нажмите на кнопку **OK**.

Изменение параметров коннектора

Чтобы изменить параметры коннектора:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Параметры**, подраздел **Коннекторы**.
3. На вкладке **Коннекторы** выберите нужный коннектор.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Изменить**.
5. Измените параметры аналогично процедуре добавления коннектора.

   Для изменения доступны не все параметры. Например, невозможно изменить выбранный тип коннектора.

6. Нажмите на кнопку **Сохранить**.

   Изменения отобразятся в соответствующих столбцах таблицы коннекторов. Если вы изменили имя коннектора, новое имя отобразится в заголовке столбца в таблице типов событий.

При изменении некоторых параметров неуправляемого коннектора сервер Central Node сформирует новый файл свертки для коннектора (например, если вы изменили адрес сервера для коннектора **Syslog**, у которого включен режим игнорирования функций управляемого коннектора). В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла свертки. Содержимое нового файла свертки вам нужно загрузить в приложение, которое использует коннектор. Иначе новое подключение через коннектор для этого приложения будет невозможно.

Создание нового файла свертки для коннектора

При добавлении неуправляемого коннектора автоматически создается файл свертки для этого коннектора. При необходимости вы можете создать для коннектора новый файл свертки (например, если сертификат из предыдущего файла свертки был скомпрометирован).

После создания нового файла свертки сертификат из старого файла свертки становится недействительным. Поэтому для следующего подключения сторонней системы через этот коннектор вам потребуется использовать новый файл свертки.

Чтобы создать новый файл свертки для неуправляемого коннектора:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Параметры**, подраздел **Коннекторы**.

3. На вкладке **Коннекторы** выберите неуправляемый коннектор, для которого вы хотите создать новый файл свертки.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Получить новый файл свертки**.

   Откроется окно **Генерация нового файла свертки**.

5. Укажите параметры для создания файла свертки:

   - Имя пользователя, под которым сторонняя система будет подключаться к приложению через коннектор. Требуется указать имя одного из пользователей приложения.

     Рекомендуется указать имя пользователя, которое было указано при добавлении коннектора. Если требуется указать имя другого пользователя, рекомендуется выбрать из учетных записей пользователей приложения того пользователя, имя которого не указано для других коннекторов и не используется для подключения к Central Node через веб-интерфейс.

   - Адрес узла, на котором работают программные модули коннектора.

   - Пароль для доступа к сертификату коннектора. С использованием заданного пароля будет зашифрован сертификат в файле свертки коннектора.

6. Нажмите на кнопку **Создать файл свертки**.

Сервер сформирует новый файл свертки для выбранного коннектора, после чего браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла. Содержимое полученного файла свертки вам нужно загрузить в приложение, которое использует коннектор. Иначе новое подключение через коннектор для этого приложения будет невозможно.

Удаление коннектора

При удалении управляемого коннектора его программные модули автоматически останавливаются и удаляются на узле размещения коннектора.

Если вы удаляете неуправляемый коннектор или коннектор, для которого включен режим игнорирования функций управляемого коннектора, перед удалением коннектора вам нужно вручную остановить и удалить его программные модули.

Чтобы удалить коннектор:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.

2. Выберите раздел **Параметры**, подраздел **Коннекторы**.

3. На вкладке **Коннекторы** выберите коннектор, который вы хотите удалить.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.

5. В окне запроса подтвердите удаление выбранного коннектора.

Добавление и удаление типов коннекторов

Типы коннекторов задают для коннекторов доступные функциональные возможности и реализуемую функциональность в рамках этих возможностей. Вы можете использовать как встроенные в приложение типы коннекторов, поставщиком которых является "Лаборатория Касперского", так и дополнительные типы коннекторов от любых других поставщиков.

Для добавления типа коннектора в приложение поставщик должен предоставить вам следующие файлы:

- файлы для установки программных модулей коннекторов;
- файл описания типа коннектора.

Если тип коннектора от стороннего поставщика позволяет сохранять в коннекторах учетные данные пользователей для доступа к сторонней системе, рекомендуется принять меры для защиты этих учетных данных от компрометации. Для минимизации рисков в случае компрометации учетных данных рекомендуется предоставлять минимально необходимые права для этих учетных записей (достаточные только для подключений через коннекторы).

Таблица типов коннекторов отображается в разделе **Параметры**, подразделе **Коннекторы** на вкладке **Типы коннекторов**.

Просмотр таблицы типов коннекторов

Таблица типов коннекторов отображается в разделе **Параметры**, подразделе **Коннекторы** на вкладке **Типы коннекторов**.

Параметры коннекторов отображаются в следующих столбцах таблицы:

- **Название**.

  Название типа коннектора, заданное поставщиком.

- **Поставщик**.

  Название поставщика типа коннектора.

- **Версия**.

  Номер версии типа коннектора.

- **Код**.

  Уникальный номер типа коннектора.

- **Возможности**.

  Список функциональных возможностей, которые будут доступны для коннекторов данного типа.

При просмотре таблицы типов коннекторов вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Добавление типа коннектора

Вы можете добавить в приложение тип коннектора с помощью файла описания, предоставленного поставщиком типа коннектора. Файл описания типа коннектора должен быть упакован в ZIP-архив.

Установку программных модулей коннекторов для добавляемого типа коннектора требуется выполнить вручную с помощью файлов, предоставленных поставщиком типа коннектора. Программные модули нужно установить на тех компьютерах, которые будут указаны в качестве узлов размещения коннекторов при добавлении коннекторов.

Чтобы добавить тип коннектора:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Параметры**, подраздел **Коннекторы**.
3. На вкладке **Типы коннекторов** откройте область деталей по ссылке **Добавить тип коннектора**.
4. Укажите файл описания типа коннектора с помощью кнопки **Обзор**.
5. Нажмите на кнопку **Сохранить**.

   Новый тип коннектора появится в таблице коннекторов.

Удаление типа коннектора

При удалении типа коннектора в приложении удаляются сведения об этом типе коннектора, а также все коннекторы, которые были добавлены с использованием этого типа.

Чтобы удалить тип коннектора:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Параметры**, подраздел **Коннекторы**.
3. На вкладке **Типы коннекторов** выберите тип коннектора, который вы хотите удалить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление выбранного типа коннектора.
6. Если в приложении есть коннекторы данного типа, подтвердите также и удаление этих коннекторов.

Управление секретами с учетными данными для удаленных подключений

В Kaspersky Anti Targeted Attack Platform реализовано хранилище секретов. *Секреты* позволяют безопасно хранить и использовать идентификационную и аутентификационную информацию, которая необходима приложению для автоматических удаленных подключений к устройствам. Секреты применяются в заданиях активного опроса.

В приложении предусмотрены различные типы секретов. В зависимости от назначения секрета вы можете выбирать нужный тип и вводить соответствующие данные при добавлении или изменении параметров секрета.

Вам нужно сохранять в секретах такие учетные данные, которые необходимы для удаленных подключений к устройствам по протоколам удаленных подключений. Задания активного опроса могут использовать для удаленных подключений различные протоколы, в зависимости от выбранных методов опроса.

Для безопасного использования идентификационной и аутентификационной информации, хранящейся в секретах, в приложении реализована защита от компрометации секретов при удаленных подключениях к устройствам. После сохранения в приложении открытых ключей, полученных от устройств, приложение контролирует все последующие удаленные подключения к этим устройствам и не отправляет информацию из секретов в случае подмены устройств в сети.

Критически важная информация секрета (пароль или закрытый ключ сертификата) доступна вам в открытом виде только один раз – при вводе этой информации во время создания секрета. После сохранения секрета его критически важную информацию невозможно просмотреть. Вы можете только заменить критически важную информацию секрета на новую при изменении секрета (например, ввести другой пароль).

Вы можете управлять секретами в разделе **Параметры**, подразделе **Секреты**. В приложение можно добавить не более 500 секретов.

Управлять секретами могут только пользователи с ролью Администратор.

Добавление секрета

Вы можете добавлять секреты в хранилище секретов приложения.

Чтобы добавить секрет:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Параметры**, подраздел **Секреты**.
3. Нажмите на кнопку **Добавить секрет**.

   Откроется область деталей.

4. Введите имя секрета.

   Имя секрета должно быть уникальным (не совпадать с именами других секретов) и может содержать до 256 символов. Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. Имя секрета должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

5. Выберите тип секрета и настройте его параметры.

   Для выбора доступны следующие типы секретов:

   - **Только пароль** – этот тип секрета применяется, если для доступа к конфигурационным данным устройства требуется только пароль пользователя, обладающего необходимыми правами.

   - **Имя и пароль пользователя** – этот тип секрета применяется, если для получения данных от устройства требуется указать имя пользователя и его пароль.

   - **Имя и пароль пользователя, пароль для root** – этот тип секрета применяется, если для получения данных от устройства требуется указать имя пользователя и его пароль, а для подключения с привилегиями администратора (с root-правами) дополнительно требуется пароль учетной записи root или учетной записи для обработки запросов с привилегиями администратора.

   - **Имя и пароль пользователя, пароль шифрования** – этот тип секрета применяется, если для получения данных от устройства требуется указать имя пользователя и его пароль, а для установки зашифрованных соединений дополнительно требуется пароль шифрования.

   - **Смешанный** – этот тип секрета применяется для способа опроса устройств **Удаленное подключение**. Для секрета этого типа вы можете задать следующие параметры:

     - Имя пользователя, которое будет использоваться для удаленных подключений к устройствам.

       Имя пользователя может содержать буквы латинского алфавита, цифры, точки, а также специальные символы `_` и `-`. Имя должно начинаться с буквы и заканчиваться любым поддерживаемым символом, кроме точки.

     - **Пароль пользователя** – если для аутентификации будет использоваться пароль пользователя.

       Пароль должен содержать до 256 символов ASCII.

     - **Закрытый ключ** – если для аутентификации будет использоваться закрытый ключ сертификата.

       Вы можете ввести последовательность символов ключа вручную или загрузить ключ из файла сертификата по ссылке **Копировать из файла**. Для загрузки закрытых ключей поддерживаются файлы форматов CRT, PEM, CER. Если файл с закрытым ключом защищен парольной фразой, перед загрузкой ключа введите парольную фразу в поле **Парольная фраза**.

       > Для использования закрытого ключа сертификата вам нужно скопировать открытый ключ этого сертификата на все устройства, к которым будут выполняться удаленные подключения с помощью секрета. Действия для копирования открытого ключа на устройства выполняются без участия Kaspersky Anti Targeted Attack Platform.

     - **Пароль для пользователя root** – если требуется дополнительный пароль для подключений к сетевому оборудованию с привилегиями администратора (с root-правами). Запрос доступа в таких случаях выполняется от имени учетной записи root или от имени той учетной записи, которая задана на сетевом оборудовании для обработки запросов с привилегиями администратора.

6. Нажмите на кнопку **Сохранить**.

Просмотр таблицы секретов

Таблица секретов для удаленных подключений отображается в разделе **Параметры**, подразделе **Секреты** веб-интерфейса приложения.

Сведения о секретах отображаются в следующих столбцах таблицы:

- **Имя секрета**.

  Имя, под которым секрет представлен в приложении.

- **Создан**.

  Дата и время добавления секрета в приложение.

- **Изменен**.

  Дата и время последнего изменения секрета в приложении.

При просмотре таблицы секретов вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Защита от компрометации секретов при удаленных подключениях к устройствам

Идентификационная и аутентификационная информация из секретов должна использоваться при удаленных подключениях только к тем устройствам, которые выбраны для заданий активного опроса. Для защиты этой информации от компрометации, которая возможна в случае подмены устройства, перед ее отправкой приложение проверяет открытый ключ, полученный от этого устройства. Открытый ключ используется на устройстве для установки SSH-соединений. Открытый ключ позволяет приложению удостовериться в том, что SSH-соединение устанавливается с правильным устройством. Передача идентификационной и аутентификационной информации на устройство происходит после проверки идентичности полученного открытого ключа и открытого ключа, сохраненного в приложении.

Сохраненный открытый ключ устройства отображается в области деталей выбранного устройства на вкладке **Общие**.

Получение и сохранение открытых ключей устройств в приложении

В Kaspersky Anti Targeted Attack Platform по умолчанию не заданы открытые ключи устройств. Получение и сохранение открытого ключа устройства происходит при первой установке SSH-соединения с этим устройством для сканирования в рамках задания активного опроса с использованием коннектора типа **Active poll**. При этом идентификационная и аутентификационная информация из выбранного секрета передается на устройство без проверки полученного открытого ключа. Поэтому перед первым запуском задания активного опроса, для которого выбрано это устройство и будет устанавливаться SSH-соединение, вам нужно убедиться в отсутствии подменного устройства в сети. Для этого, например, вы можете проверить совпадение IP-адресов устройства, заданных в приложении, и IP-адресов на сетевых интерфейсах самого устройства с помощью команды `ifconfig`.

Сброс сохраненных открытых ключей устройств

С течением времени на устройствах могут изменяться ключи, используемые для установки SSH-соединений. Например, пользователи устройств могут выполнять процедуры генерации новых ключей при угрозе компрометации текущих закрытых ключей.

При смене закрытого ключа на устройстве происходит смена открытого ключа. После изменения открытого ключа приложение не передает на это устройство информацию из секретов из-за несовпадения нового открытого ключа и открытого ключа, сохраненного в приложении. Как следствие, следующие сканирования устройства в рамках заданий активного опроса завершаются с ошибкой.

После изменения открытого ключа на устройстве вам нужно сбросить текущий сохраненный открытый ключ этого устройства в приложении. Это позволит снова использовать секреты при удаленных подключениях к устройству.

После сброса сохраненного открытого ключа приложение сохранит новый полученный открытый ключ при следующей установке SSH-соединения с этим устройством. При этом вам нужно убедиться в отсутствии подменного устройства в сети аналогично, как при первичном получении и сохранении открытого ключа.

Сбросить сохраненные открытые ключи устройств могут только пользователи с ролью **Старший сотрудник службы безопасности**.

Чтобы сбросить сохраненные открытые ключи устройств:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью **Старший сотрудник службы безопасности**.
2. Выберите раздел **Активы**.
3. На вкладке **Устройства** выберите устройства, для которых вы хотите сбросить сохраненные открытые ключи.
4. По правой кнопке мыши откройте контекстное меню одного из выбранных устройств.
5. В контекстном меню выберите пункт **Сбросить открытый ключ**.

   Откроется окно с запросом подтверждения.
6. В окне запроса нажмите на кнопку **ОК**.

Изменение параметров секрета

При изменении параметров секрета вы можете изменить его тип или задать другие значения для учетных данных.

После изменения параметров секрета, в том числе после изменения имени секрета, новые параметры применяются в заданиях активного опроса, в которых этот секрет был указан ранее. Если вы изменяете тип секрета, при следующих запусках этих заданий могут возникать ошибки в тех случаях, когда новый тип секрета не соответствует параметрам коннектора.

Чтобы изменить параметры секрета:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Параметры**, подраздел **Секреты**.
3. Выберите секрет, который вы хотите изменить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. Измените нужные параметры. Для изменения параметров вам доступны те же действия, что и при добавлении секрета.

   Критически важная информация секрета (пароли и закрытый ключ сертификата) не отображается в открытом виде. Вы можете только заменить критически важную информацию секрета на новую с помощью ссылок, расположенных над полями с учетными данными.

Удаление секретов

Вы можете удалять секреты из хранилища секретов Kaspersky Anti Targeted Attack Platform.

Перед удалением секрета рекомендуется указать другой секрет или другой способ опроса в заданиях активного опроса, в которых указан этот секрет. Если удаленный секрет остался указанным в задании для активного опроса, при следующих запусках этого задания будут возникать ошибки.

Чтобы удалить секреты:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Параметры**, подраздел **Секреты**.
3. Выберите секреты, которые вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление секретов.

Обновление баз приложения

Базы приложения (далее также "базы") представляют собой файлы с записями, на основании которых компоненты и модули приложения обнаруживают события, происходящие в IT-инфраструктуре вашей организации.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, в том числе угроз "нулевого дня", создают для них идентифицирующие записи и включают их в пакеты обновлений баз (далее также "пакеты обновлений"). *Пакет обновлений* представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, прошедшее с момента выпуска предыдущего пакета обновлений. Рекомендуется регулярно получать пакеты обновлений. При установке приложения дата выпуска баз соответствует дате выпуска приложения, поэтому базы нужно обновить сразу после установки приложения.

Приложение автоматически проверяет наличие новых пакетов обновлений на серверах обновлений "Лаборатории Касперского" один раз в 30 минут. По умолчанию, если базы компонентов приложения по каким-либо причинам не обновляются в течение 24 часов, Kaspersky Anti Targeted Attack Platform отображает эту информацию в разделе **Мониторинг** окна веб-интерфейса приложения.

Если версия Kaspersky Anti Targeted Attack Platform не поддерживается, базы приложения не будут обновляться и в разделе **Мониторинг** в окне **Работоспособность системы** веб-интерфейса приложения будет отображаться предупреждение *Эта версия Kaspersky Anti Targeted Attack Platform больше не поддерживается. Обновите версию приложения до поддерживаемой.*

Вы можете посмотреть, какие версии приложения находятся на поддержке, на странице жизненного цикла приложений.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

В режиме распределенного решения и мультитенантности базы приложения обновляются отдельно на каждом сервере PCN и SCN.

Если вы развернули Kaspersky Anti Targeted Attack Platform в изолированной сети или в сети с ограниченной пропускной способностью канала выхода в интернет, вы можете настроить обновление баз приложения с помощью утилиты Kaspersky Update Utility.

Выбор источника обновления баз

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Вы можете выбрать источник, из которого приложение будет загружать обновления баз. Источником обновлений может быть сервер "Лаборатории Касперского", а также сетевая или локальная папка одного из компьютеров вашей организации.

Чтобы выбрать источник обновления баз приложения:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке **Обновление баз** в раскрывающемся списке **Источник обновлений** выберите одно из следующих значений:

   - **Сервер обновлений "Лаборатории Касперского"**.

     Приложение будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTP и загружать актуальные базы.

- **Сервер обновлений "Лаборатории Касперского" (безопасное подключение)**.

  Приложение будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTPS и загружать актуальные базы. Рекомендуется выполнять обновления баз по протоколу HTTPS.

- **Другой сервер**.

  Приложение будет подключаться к вашему FTP- или HTTP-серверу или к папке с базами приложения на вашем компьютере и загружать актуальные базы.

  Обмен данными между вашим HTTP-сервером и Central Node должен осуществляться по протоколу HTTP. HTTPS в этом случае не поддерживается.

3. Если вы выбрали **Другой сервер**, в поле под названием этого параметра укажите URL-адрес пакета обновлений на вашем HTTP-сервере или полный путь к папке с пакетом обновлений баз приложения на вашем компьютере.

4. Нажмите на кнопку **Применить**.

Источник обновления баз приложения будет выбран.

Запуск обновления баз вручную

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы запустить обновление баз приложения вручную:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Общие параметры**.

2. В блоке **Обновление баз** нажмите на кнопку **Запустить**.

3. Нажмите на кнопку **Применить**.

Обновление баз приложения будет запущено. Справа от кнопки отобразится сообщение о результате выполнения обновления.

Обновление баз приложения с помощью Kaspersky Update Utility

Если вы развернули Kaspersky Anti Targeted Attack Platform в изолированной сети или в сети с ограниченной пропускной способностью канала выхода в интернет, вы можете настроить обновление баз приложения с помощью утилиты Kaspersky Update Utility. В этом случае пакеты обновлений с помощью утилиты скачиваются на компьютер, который находится вне локальной сети организации, и копируются на ваш FTP- или HTTP-сервер. Kaspersky Anti Targeted Attack Platform получает пакеты обновлений с этого сервера.

Настройка обновления баз приложения с помощью утилиты состоит из следующих этапов:

1. Скачивание пакетов обновлений с помощью Kaspersky Update Utility

   Предварительно вам потребуется запросить в Службе технической поддержки "Лаборатории Касперского" дистрибутив утилиты и список серверов для загрузки обновлений.

2. Загрузка пакетов обновлений, полученных с помощью утилиты Kaspersky Update Utility, на ваш FTP- или HTTP-сервер.

3. Выбор вашего FTP- или HTTP-сервера в качестве источника обновления баз.

Скачивание пакетов обновлений с помощью Kaspersky Update Utility

Для выполнения шагов инструкции вам нужно запросить в Службе технической поддержки "Лаборатории Касперского" дистрибутив утилиты и список серверов для загрузки обновлений.

Чтобы установить утилиту Kaspersky Update Utility:

1. Загрузите на компьютер папку с дистрибутивом утилиты.

2. Запустите файл UpdateUtility-Gui.exe.

3. В открывшемся окне нажмите на кнопку **Applications** и установите флажок слева от версии **7.0-7.1**.

4. Нажмите на кнопки **OK** и **Apply**.

Утилита будет установлена. Вы можете скачать пакеты обновлений, выполнив шаги инструкции ниже.

Чтобы скачать пакеты обновлений с помощью Kaspersky Update Utility:

1. В главном окне утилиты нажмите на кнопку **Settings** и выберите **Download**.

2. В блоке параметров **Updates source** выберите **Other** и введите адрес сервера для загрузки обновлений.

3. Нажмите на кнопки **OK** и **Apply**.

4. Нажмите на кнопку **Start**.

Пакеты обновлений будут скачаны на компьютер, где располагается утилита. Файлы будут готовы к загрузке на ваш FTP- или HTTP-сервер.

Обновление сертификата для подключения к Central Node через API

Для обновления сертификата для подключения к серверу Central Node через Kaspersky Anti Targeted Attack Platform API вам нужно заменить сертификат, используемый сервером REST API. Вы можете указать новый сертификат сервера REST API в разделе **Параметры**, подразделе **Серверы подключений** на вкладке **Сервер REST API**.

Интеграция со средствами для раскрытия зашифрованного SSL/TLS-трафика

Kaspersky Anti Targeted Attack Platform принимает расшифрованный SSL/TLS-трафик от сторонних средств расшифровки на стандартные сетевые интерфейсы, обеспечивая его обработку и анализ. Настройка получения и обработки расшифрованного трафика в Kaspersky Anti Targeted Attack Platform аналогична настройке получения и обработки зеркалированного SPAN-трафика: вам необходимо включить поддержку SPAN-интеграции при установке приложения и создать и включить точку мониторинга для сетевого интерфейса, на который подается трафик (если она не была создана и включена ранее).

Поступление расшифрованного трафика в приложение увеличивает нагрузку по обработке трафика в 5 раз по сравнению с нешифруемым трафиком. Вы можете посмотреть подробную информацию об аппаратных требованиях к серверам для установки Central Node в разделе Калькулятор масштабирования.

При получении расшифрованного трафика Kaspersky Anti Targeted Attack Platform может обрабатывать и сохранять чувствительную информацию, которая передается по зашифрованным протоколам. Например, имена и пароли учетных записей, номера банковских карт.

Сотруднику службы безопасности: работа в веб-интерфейсе приложения

Этот раздел адресован специалистам, в обязанности которых входит обеспечение безопасности данных организации. Он содержит информацию и инструкции по настройке средств для защиты IT-инфраструктуры организации и своевременного обнаружения угроз.

Приложение допускает совместную работу нескольких специалистов по информационной безопасности.

Интерфейс Kaspersky Anti Targeted Attack Platform

Работа с приложением осуществляется через веб-интерфейс. Разделы веб-интерфейса приложения различаются в зависимости от роли пользователя – администратор или сотрудник службы безопасности (**Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Аудитор**).

Окно веб-интерфейса приложения содержит следующие элементы:

- разделы в левой части и в нижней части окна веб-интерфейса приложения;
- закладки в верхней части окна веб-интерфейса приложения для некоторых разделов приложения;
- рабочую область в нижней части окна веб-интерфейса приложения.

Разделы окна веб-интерфейса приложения

Веб-интерфейс приложения для пользователей с ролями **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** и **Аудитор** содержит следующие разделы:

- **Мониторинг**. Содержит данные мониторинга Kaspersky Anti Targeted Attack Platform.

  Для пользователей с ролью **Аудитор** окно **Мониторинг** содержит следующие разделы: **Алерты**, **Работоспособность системы**.

- **Алерты**. Содержит информацию об алертах в сети тенанта, к которому у вас есть доступ.
- **События в трафике сети**. Информация о событиях и агрегирующих событиях в трафике сети.
- **Поиск угроз**. Содержит информацию о событиях, найденных на хостах тенанта, к которому у вас есть доступ.
- **Задачи**. Содержит информацию о задачах, с помощью которых вы можете работать с файлами и приложениями на хостах.
- **Политики**. Содержит информацию о политиках, с помощью которых вы можете управлять запретами запуска файлов на выбранных хостах.

- **Пользовательские правила**: **TAA**, **Обнаружение вторжений**, **IOC**, **YARA**, **Sandbox** Содержит информацию для работы с пользовательскими правилами.
- **Хранилище**: **Файлы** и **Карантин**. Содержит информацию для работы с объектами на карантине и в Хранилище.
- **Активы**. Содержит информацию о компьютерах с компонентом Endpoint Agent и их параметрах.
- **Карта сети**: **Карта сетевых взаимодействий**, **Топологическая карта**, **Сетевые сессии**. Содержит информацию о взаимодействии устройств в различные периоды времени, схемах физических подключений устройств в сети и информацию о сетевых сеансах.
- **Риски и аномалии**. Содержит информацию о рисках, которым подвержены ресурсы информационной системы.
- **Отчеты**: **Созданные отчеты** и **Шаблоны**. Содержит конструктор отчетов и список созданных отчетов об алертах.
- **Журналы**: **Сообщения приложения**. Содержит информацию о работе приложения.
- **Параметры**: **Коннекторы**, **Секреты**, **Расписание IOC-проверки**, **Endpoint Agents**, **Репутационная база KPSN**, **Правила уведомлений**, **Статус VIP**, **Исключения**, **Разрешающие правила**, **Серверы Sandbox**, **Пароли к архивам** и **Лицензия**. Содержит информацию о параметрах коннекторов, секретах, расписании IOC-проверки, параметрах компонентов Endpoint Agent, параметрах публикации объектов в KPSN, присвоении алертам статуса VIP на основе информации, содержащейся в алертах, списке разрешенных объектов и исключениях из проверки правил IDS, TAA (IOA) и ICAP, паролях к архивам и добавленных ключах.

Для пользователей с ролью **Аудитор** веб-интерфейс приложения, кроме перечисленных выше, также содержит следующие разделы:

- **Режим работы**. Содержит информацию о серверах PCN и SCN и о тенантах в режиме распределенного решения и мультитенантности.
- **Серверы Sensor**. Содержит информацию о компонентах Central Node и подключенных к ним компонентам Sensor.
- **Серверы Sandbox**. Содержит информацию о подключении компонента Central Node к компонентам Sandbox.
- **Внешние системы**. Содержит информацию об интеграции приложения с почтовыми сенсорами.
- **Конфигурация серверов**. Содержит информацию о параметрах масштабирования приложения.

Рабочая область окна веб-интерфейса приложения

В рабочей области отображается информация, просмотр которой вы выбираете в разделах и на закладках окна веб-интерфейса приложения, а также элементы управления, с помощью которых вы можете настроить отображение информации.

Выбор тенанта для работы в веб-интерфейсе приложения

Если вы используете режим распределенного решения и мультитенантности под учетной записью **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности**, перед началом работы с веб-интерфейсом вам нужно выбрать тенант, в рамках которого вы хотите работать с веб-интерфейсом приложения.

Чтобы выбрать тенант для работы в веб-интерфейсе приложения:

1. В верхней части меню веб-интерфейса приложения нажмите на стрелку рядом с названием тенанта.
2. В раскрывающемся меню **Выберите тенант** выберите тенант из списка.

   Вы также можете ввести несколько символов названия тенанта в строку поиска и выбрать его из списка результатов поиска.

Все действия в веб-интерфейсе приложения будут связаны с выбранным тенантом. Если вы хотите изменить тенант, вам нужно повторить действия по выбору тенанта.

Выбор тенанта для работы в веб-интерфейсе недоступен для пользователей с ролью **Аудитор**.

Мониторинг работы приложения

Вы можете осуществлять мониторинг работы приложения с помощью виджетов в разделе **Мониторинг** окна веб-интерфейса приложения. Вы можете добавлять, удалять, перемещать виджеты, настраивать масштаб отображения виджетов и выбирать период отображения данных.

О виджетах и схемах расположения виджетов

С помощью виджетов вы можете осуществлять мониторинг работы приложения.

Схема расположения виджетов – вид рабочей области окна веб-интерфейса приложения в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать виджеты на схеме расположения виджетов, а также настраивать масштаб виджетов.

Если вы используете режим распределенного решения и мультитенантности, в разделе отображаются данные по выбранному вами тенанту. Виджеты NDR отображают информацию только по текущему или по выбранному узлу.

По умолчанию в разделе отображается информация только об алертах, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных алертах тоже отображалась, включите переключатель **Показывать закрытые алерты** в правом верхнем углу окна.

В разделе **Мониторинг** отображаются следующие виджеты:

- Алерты:
  - **Алерты по состоянию**. Отображение состояния алерта в зависимости от того, какой пользователь Kaspersky Anti Targeted Attack Platform его обрабатывает и от того, обработан этот алерт или нет.
  - **Алерты по технологии**. Отображение названий модулей или компонентов приложения, создавших алерт.
  - **Алерты по вектору атаки**. Отображение обнаруженных объектов по направлению атаки.
  - **VIP-алерты по степени важности**. Отображение важности алертов со статусом VIP в соответствии с тем, какое влияние они могут оказать на безопасность компьютера или локальной сети организации, по опыту "Лаборатории Касперского".
  - **Алерты по степени важности**. Отображение важности алертов для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние они могут оказать на безопасность компьютеров или локальной сети организации, по опыту "Лаборатории Касперского".

  В левой части каждого виджета перечислены векторы атаки, степени важности алертов, состояния алертов и технологии, при проверке которыми был создан алерт. В правой части каждого виджета отображается количество раз, которое приложение обнаружило их за выбранный период отображения данных на виджетах.

  По ссылке с названием вектора атаки, степенью важности алертов, состоянием алертов и технологией, при проверке которой был создан алерт, можно перейти в раздел **Алерты** веб-интерфейса приложения и просмотреть связанные алерты. При этом алерты будут отфильтрованы по выбранному элементу.

- Топ 10:
  - **Домены**. 10 доменов, наиболее часто встречающихся в алертах.
  - **IP-адреса**. 10 IP-адресов, наиболее часто встречающихся в алертах.
  - **Адреса отправителей**. 10 отправителей сообщений электронной почты, наиболее часто встречающихся в алертах.
  - **Адреса получателей**. 10 получателей сообщений электронной почты, наиболее часто встречающихся в алертах.
  - **Хосты TAA**. 10 хостов, наиболее часто встречающихся в событиях и алертах, Созданных при проверке технологией Targeted Attack Analyzer (TAA).
  - **Правила TAA**. 10 правил TAA (IOA), наиболее часто встречающихся в событиях и алертах, созданных при проверке технологией Targeted Attack Analyzer (TAA).

    На виджете отображается общее количество срабатываний правила TAA (IOA) за выбранный период. При этом количество срабатываний на виджете может превышать количество хостов со сработавшим правилом TAA (IOA), которое отображается в карточке алерта, так как одно и то же правило может сработать на одном хосте несколько раз (например, при повторных запусках вредоносного процесса).

    Вы можете просмотреть подробную информацию о сработавшем правиле TAA (IOA) в карточке алерта в блоке **Результаты проверки**.
  - **Отправлено в Sandbox по правилам TAA**. 10 правил TAA (IOA), по которым Kaspersky Anti Targeted Attack Platform наиболее часто отправляет файлы на проверку компоненту Sandbox.

В левой части каждого виджета перечислены домены, адреса получателей, IP-адреса и адреса отправителей сообщений, имена хостов и названия правил TAA (IOA). В правой части каждого виджета отображается количество раз, которое приложение обнаружило их за выбранный период отображения данных на виджетах.

По ссылке с именем каждого домена, адреса получателя, IP-адреса и адреса отправителя сообщений можно перейти в раздел **Алерты** веб-интерфейса приложения и просмотреть связанные алерты.

По ссылке с именем хоста и названию правила TAA (IOA) можно перейти в раздел **События** веб-интерфейса приложения и просмотреть связанные события.

При этом алерты и события будут отфильтрованы по выбранному элементу.

- NDR:

  - **Оценки событий в трафике сети**. Гистограмма распределения событий по значениям их оценок за выбранный период. Столбцы гистограммы соответствуют целочисленным значениям оценок. Вы можете изменить режим отображения данных на круговую диаграмму с распределением событий по уровням критичности. В зависимости от числового значения оценки события могут относиться к уровням критичности *Низкий* (оценки 0.0–3.9), *Средний* (оценки 4.0–7.9) или *Высокий* (оценки 8.0–10.0).

  - **События в трафике сети по технологиям**. Количественное распределение событий по технологиям регистрации событий за выбранный период.

  - **Состояние безопасности устройств**. Распределение устройств по их состояниям безопасности.

  - **Частые пользователи приложений в событиях в трафике сети**. Наиболее часто регистрируемые имена пользователей в событиях по данным от EPP-приложений за выбранный период.

  - **Частые приложения в событиях в трафике сети**. Наиболее часто регистрируемые сторонние приложения в событиях по данным от EPP-приложений за выбранный период.

  - **Частые устройства в событиях в трафике сети**. Наиболее часто регистрируемые устройства в событиях за выбранный период.

  - **Частые устройства по количеству рисков**. Наиболее часто регистрируемые устройства в обнаруженных рисках за выбранный период.

  - **Оценки рисков**. Гистограмма распределения рисков по значениям их оценок за выбранный период. Столбцы гистограммы соответствуют целочисленным значениям оценок. Вы можете изменить режим отображения данных на круговую диаграмму с распределением рисков по уровням критичности. В зависимости от числового значения оценки риска могут относиться к уровням критичности *Низкий* (оценки 0.0–3.9), *Средний* (оценки 4.0–7.9) или *Высокий* (оценки 8.0–10.0).

  - **Пользовательский виджет**. Вы можете создавать виджеты с произвольно заданным содержанием. С помощью пользовательских виджетов вы можете, например, логически разделять группы виджетов в разделе **Мониторинг**.

  - **Устройства**. Содержит информацию об устройствах в сети (используется распределение по категориям устройств).

  - **События в трафике сети**. Содержит информацию о событиях NDR и агрегирующих событиях, имеющих наиболее поздние значения даты и времени последнего появления.

  - **Ситуационная осведомленность**. Уведомления о текущих выявленных угрозах для безопасности системы (например, "Обнаружены 10 неразрешенных сетевых взаимодействий"). Виджет отображает уведомления в порядке их уровня важности.

- **Защищенность EPP-приложениями**. Количественное соотношение компьютеров, защищенных и не защищенных EPP-приложениями. В центре круговой диаграммы отображается суммарное количество защищенных и не защищенных компьютеров.

  Компьютер считается защищенным EPP-приложением, если в Kaspersky Anti Targeted Attack Platform имеются сведения о выполнении следующих условий:

  - на компьютере установлено EPP-приложение;
  - для EPP-приложения выполняется задача Постоянная защита (Real-Time Protection);
  - EPP-приложение имеет статус подключения к серверу интеграции *Активное*.

  Компьютер считается не защищенным EPP-приложением, если не выполнено хотя бы одно из перечисленных условий. Проверка на незащищенность EPP-приложением выполняется для всех устройств в Kaspersky Anti Targeted Attack Platform, содержащих название операционной системы Windows (любой версии) в качестве установленной операционной системы, или если устройства относятся к одной из следующих категорий:

  - **Сервер**;
  - **Рабочая станция**.

Чтобы на виджетах NDR отображались корректные данные, требуется настроить синхронизацию даты и времени между компонентами Central Node и Sensor.

В виджетах отображается только основная информация, которая изменяется динамически. Если вам нужно просмотреть более подробную информацию (например, об устройствах, требующих внимания), вы можете перейти из раздела **Мониторинг** к другим разделам веб-интерфейса программы. Переходы можно выполнять путем выбора элементов интерфейса виджетов с помощью мыши.

Добавление виджета на текущую схему расположения виджетов

Чтобы добавить виджет на текущую схему расположения виджетов:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на кнопку **Виджеты**.

5. В появившемся окне **Настроить виджеты** выполните следующие действия:

   - Если вы хотите добавить виджет, связанный с алертами или правилами, в списке **Алерты** или **Топ 10** включите переключатель рядом с виджетом, который вы хотите добавить.
   - Если вы хотите добавить виджет, связанный с функциональность NDR, в списке **[NDR]** около названия нужного виджета нажмите на кнопку +.

6. Закройте окно **Настроить виджеты** и нажмите на кнопку **Применить**.

Виджет будет добавлен на текущую схему расположения виджетов.

Перемещение виджета на текущей схеме расположения виджетов

Чтобы переместить виджет на текущей схеме расположения виджетов:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Изменить**.
4. Выберите виджет, который вы хотите переместить на схеме расположения виджетов.
5. Удерживая левую клавишу мыши на верхней части виджета, перетащите виджет на другое место схемы расположения виджетов.
6. Нажмите на кнопку **Применить**.

Текущая схема расположения виджетов будет сохранена.

Изменение отображения данных в виджетах NDR

После добавления виджета NDR для отображения данных используются параметры, заданные по умолчанию. При необходимости вы можете изменить параметры отображения.

Чтобы настроить параметры отображения виджета NDR:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Изменить**.
4. В правом верхнем углу виджета NDR, параметры отображения которого вы хотите поменять, нажмите на кнопку ⚙.

   Откроется окно для настройки параметров отображения.

5. Настройте параметры виджета.

   В зависимости от выбранного виджета NDR окно может содержать следующие параметры:

   - **Изменить название** – если установлен флажок **Изменить название**, вы можете задать произвольное название виджета (отличающееся от заданного по умолчанию) в поле **Название виджета**. Параметр **Изменить название** отсутствует для пользовательских виджетов.
   - **Название виджета** – поле для ввода названия виджета, отличающегося от названия по умолчанию.
   - **Изменить описание** – если установлен флажок **Изменить описание**, вы можете задать произвольное описание виджета (отличающееся от заданного по умолчанию) в поле **Описание виджета**. Параметр **Изменить описание** отсутствует для пользовательских виджетов.
   - **Описание виджета** – поле для ввода названия виджета, отличающегося от названия по умолчанию.
   - **Период обновления** – задает период времени в секундах, после которого обновляются отображаемые данные.
   - **Заданный фон** – определяет цвет фона пользовательского виджета. Вы можете выбрать вариант закрашивания цветом, который соответствует одному из уровней важности (**Информационный**, **Важный**, **Критический**), или выключить закрашивание фона с помощью варианта **Бесцветный**.
   - **Режим отображения** – определяет режим отображения данных на виджете. Вы можете настроить отображение данных в виде гистограммы или круговой диаграммы.
   - **Учитывать события со статусом Обработано** – если установлен флажок **Учитывать события со статусом Обработано**, виджет отображает данные по всем событиям.
   - **Учитывать устраненные и принятые риски** – если установлен флажок **Учитывать устраненные и принятые риски**, виджет отображает данные по всем рискам.

6. Нажмите на кнопку **Применить**.

Удаление виджета с текущей схемы расположения виджетов

Чтобы удалить виджет с текущей схемы расположения виджетов:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на значок × в правом верхнем углу виджета, который вы хотите удалить со схемы расположения виджетов.

   Виджет будет удален из рабочей области окна веб-интерфейса приложения.
5. Нажмите на кнопку **Применить**.

Виджет будет удален с текущей схемы расположения виджетов.

Сохранение схемы расположения виджетов в PDF

Виджеты функциональности NDR в схеме расположения в PDF не сохраняются.

Чтобы сохранить схему расположения виджетов в PDF:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Сохранить как PDF**.

   Откроется окно **Сохранение в PDF**.
4. В нижней части окна в раскрывающемся списке **Ориентация** выберите ориентацию страницы.
5. Нажмите на кнопку **Скачать**.

   Схема расположения виджетов в формате PDF будет сохранена на жесткий диск вашего компьютера в папку загрузки браузера.
6. Нажмите на кнопку **Закрыть**.

Настройка периода отображения данных на виджетах

Вы можете настроить отображение данных на виджетах за следующие периоды:

- **День**.
- **Неделя**.
- **Месяц**.

Для виджетов NDR доступны следующие периоды:

- **1ч**.
- **12ч**.
- **24ч**.
- **7д**.

Вы можете указать период отображения данных для каждого виджета NDR отдельно.

Настройка отображения данных в виджетах

Чтобы настроить отображение данных на виджетах за сутки (с 00:00 до 23:59):

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в раскрывающемся списке периодов отображения данных выберите **День**.
3. В календаре справа от названия периода **День** выберите дату, за которую вы хотите получить данные на виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Чтобы настроить отображение данных на виджетах за неделю (с понедельника по воскресенье):

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в раскрывающемся списке периодов отображения данных выберите **Неделя**.
3. В календаре справа от названия периода **Неделя** выберите неделю, за которую вы хотите получить данные на виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Чтобы настроить отображение данных на виджетах за месяц (календарный месяц):

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в раскрывающемся списке периодов отображения данных выберите **Месяц**.
3. В календаре справа от названия периода **Месяц** выберите месяц, за который вы хотите получить данные на виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Настройка отображения данных в виджетах NDR

Чтобы настроить отображение данных на виджете NDR:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу виджета NDR, параметры отображения которого вы хотите поменять, нажмите на кнопку с отображением нужного временного интервала.

На виджете NDR отобразятся данные за выбранный вами период.

Настройка масштаба отображения виджетов

Вы можете настроить масштаб отображения виджетов типа "Алерты". В правом верхнем углу виджетов, масштаб отображения которых можно настроить, есть значок ☰.

Чтобы настроить масштаб отображения виджетов:

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на значок ☰ в правом верхнем углу виджета.
5. В раскрывшемся списке выберите один из следующих размеров отображения виджета:
   - **1x1 размер**.
   - **2x1 размер**.
   - **3x1 размер**.

   Масштаб отображения выбранного виджета изменится.
6. Повторите действия для всех виджетов, масштаб отображения которых вы хотите изменить.
7. Нажмите на кнопку **Сохранить**.

Масштаб отображения виджетов будет настроен.

Основные принципы работы с виджетами типа "Алерты"

Для всех виджетов типа "Алерты" можно настроить масштаб отображения.

В левой части каждого виджета отображается легенда виджета по цветам, которые используются на виджетах.

Пример:
На виджете **Алерты по степени важности** отображается количество алертов различной степени важности.
Важность – важность алерта для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние этот алерт может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".
На виджете **Алерты по степени важности** важность алертов отмечена следующими цветами:

- красным – алерты высокой степени важности;
- оранжевым – алерты средней степени важности;
- зеленым – алерты низкой степени важности.

Справа от легенды отображается количество обнаружений каждого типа за выбранный период отображения данных на виджетах.

По ссылке с типом каждого алерта можно перейти в раздел **Алерты** веб-интерфейса приложения и просмотреть все алерты этого типа. При этом алерты будут отфильтрованы по данному типу.

Пример:
На виджете **Алерты по вектору атаки** отображаются алерты **Файлы из почты** – количество файлов, которые Kaspersky Anti Targeted Attack Platform обнаружило в почтовом трафике за выбранный период отображения данных на виджетах.
По ссылке **Файлы из почты** откроется раздел **Алерты** и отобразятся все алерты, связанные с обнаружением файлов в почтовом трафике за выбранный период отображения данных на виджетах. Данные будут отфильтрованы по следующим параметрам: **Тип объекта**=FILE и **Источник объекта**=MAIL.

В правой части каждого виджета отображаются столбцы данных. На вертикальной оси отображается количество событий, на горизонтальной оси отображаются дата и время создания алерта. Вы можете изменить период отображения данных на виджетах и выбрать тенант, информация о которых должна быть представлена на виджете.

При наведении курсора мыши на каждый столбец данных отображается количество алертов, подсчитанных за период, представленный этим столбцом. По умолчанию отображается количество необработанных алертов. Вы можете включить отображение обработанных алертов, установив флажок **Обработано** в правом верхнем углу окна. В этом случае будет отображаться количество всех алертов.

Информация в виджете Устройства

Виджет **Устройства** в разделе **Мониторинг** относится к функциональности NDR и отображает информацию об устройствах, входящих в список известных приложению устройств.

В виджете представлена следующая информация:

- Данные о количественном распределении известных приложению устройств по категориям. Эти данные отображаются в верхней части виджета в виде значков категорий. Под значком каждой категории указано количество устройств этой категории. Если в списке известных приложению устройств есть устройства, требующие внимания, на значках категорий этих устройств отображается значок предупреждения.

- Список категорий с устройствами, требующими внимания. Эти данные отображаются в средней части виджета при наличии таких устройств. Пространство для отображения графических элементов ограничено размером виджета.

Устройства, требующие внимания

Приложение считает, что устройство требует внимания, в любом из следующих случаев:

- устройство имеет статус *Разрешенное* и состояние безопасности устройства отличается от *OK*;

- устройство имеет статус *Неразрешенное*.

При наличии устройств, требующих внимания, для каждой категории в списке отображается следующая информация:

- Строка, содержащая значок категории, текстовый комментарий и ссылку с количеством устройств, требующих внимания.
- Строка с графическими элементами, представляющими устройства. Строка отображается, если достаточно свободного пространства в виджете. Количество графических элементов в строке зависит от текущего размера окна браузера. Если устройств, требующих внимания, больше чем отображаемых графических элементов в строке, то справа отображается количество скрытых устройств в формате + <количество устройств>.

Графические элементы устройств

Графические элементы, представляющие устройства, содержат следующую информацию:

- Имя устройства.
- Статус устройства. Отображается в виде значка, если устройство имеет статус *Неразрешенное*.
- Состояние безопасности устройства. Отображается в виде цветной линии на левой границе графического элемента. Цвет линии соответствует состояниям *ОК*, *Важное* или *Критическое*.

Графические элементы отображаются в следующем порядке:

1. Устройства с присвоенным статусом *Неразрешенное*.
2. Устройства, имеющие состояние безопасности *Критическое*.
3. Устройства, имеющие состояние безопасности *Важное*.

Переходы к другим разделам из виджета

С помощью элементов интерфейса виджета **Устройства** вы можете переходить к таблице устройств для отображения подробных сведений об устройствах. Для этого предусмотрены возможности, описанные ниже.

Переход к таблице устройств и фильтрация таблицы

Чтобы перейти к таблице устройств и просмотреть сведения о всех устройствах выбранной категории,

в верхней части виджета **Устройства** нажмите на значок нужной категории.

Откроется раздел **Активы** с таблицей устройств. В таблице будет применена фильтрация по выбранной категории устройств.

Чтобы перейти к таблице устройств и просмотреть сведения об устройствах, требующих внимания и относящихся к определенной категории,

в списке категорий с устройствами, требующими внимания, воспользуйтесь ссылкой с количеством устройств нужной категории. Ссылка отображается в конце строки со значком категории и текстовым комментарием **требующие внимания**.

Откроется раздел **Активы** с таблицей устройств. В таблице будет применена фильтрация по идентификаторам устройств, требующих внимания и относящихся к определенной категории.

Фильтрация в таблице устройств выполняется по идентификаторам тех устройств, которые отображались в виджете **Устройства** на момент перехода к таблице устройств. После перехода к таблице устройств параметры фильтрации не обновляются. Если вы хотите просмотреть текущее количество устройств, требующих внимания, вы можете снова перейти в раздел **Мониторинг**.

Чтобы перейти к таблице устройств и просмотреть сведения об устройстве, требующем внимания,

в виджете **Устройства** нажмите на графический элемент, представляющий нужное устройство.

Откроется раздел **Активы** с таблицей устройств. В таблице будет применена фильтрация по идентификатору устройства.

Чтобы перейти к таблице устройств без изменений текущих параметров фильтрации таблицы,

перейдите по ссылке **Показать все устройства** в виджете **Устройства**.

Откроется раздел **Активы** с таблицей устройств. В таблице отобразятся устройства, удовлетворяющие параметрам фильтрации, которые были заданы ранее в таблице устройств.

Переход к таблице устройств и поиск в таблице

Чтобы перейти к таблице устройств и найти устройства в таблице:

1. В виджете **Устройства** введите поисковый запрос в поле **Поиск устройств**.
2. Нажмите на кнопку **Поиск**.

   Откроется раздел **Активы** с таблицей устройств. В таблице отобразятся устройства, которые удовлетворяют условиям поиска.

Информация в виджете События

Виджет **События в трафике сети** в разделе **Мониторинг** отображает общую информацию о событиях NDR и агрегирующих событиях, имеющих наиболее поздние значения даты и времени последнего появления.

В виджете отображаются следующие элементы:

- Гистограмма событий NDR и агрегирующих событий за выбранный период. Эти данные отображаются в верхней части виджета. Гистограмма отображает распределение событий NDR и агрегирующих событий по уровням критичности.
- Список с информацией о зарегистрированных событиях NDR и агрегирующих событиях, отсортированный по дате и времени последнего появления. Эти данные отображаются в средней части виджета.

Статистика событий NDR и агрегирующих событий

На гистограмме распределения событий NDR и агрегирующих событий столбцы соответствуют суммарному количеству событий за каждый интервал времени. Внутри столбцов цветом обозначены уровни критичности событий. Уровням критичности соответствуют следующие цвета:

- Синий цвет. Этот цвет используется для событий NDR и агрегирующих событий с уровнем критичности *Низкий*.
- Желтый цвет. Этот цвет используется для событий NDR и агрегирующих событий с уровнем критичности *Средний*.
- Красный цвет. Этот цвет используется для событий NDR и агрегирующих событий с уровнем критичности *Высокий*.

Для вывода информации о столбце гистограммы наведите на него курсор мыши. Во всплывающем окне отобразятся сведения о дате и времени интервала, а также о количестве событий NDR и агрегирующих событий по уровням критичности.

Длительность интервалов времени зависит от выбранного периода для отображения. Вы можете выбрать нужный период для построения гистограммы с помощью следующих кнопок:

- **1ч** – период в один час, делится на интервалы по одной минуте.
- **12ч** – период в 12 часов, делится на интервалы по одному часу.
- **24ч** – период в 24 часа, делится на интервалы по одному часу.
- **7д** – период в семь дней, делится на интервалы по одному дню.

Список событий NDR и агрегирующих событий

Список событий NDR и агрегирующих событий в виджете **События в трафике сети** обновляется в онлайн-режиме. События NDR и агрегирующие события с наиболее поздними значениями даты и времени последнего появления помещаются в начало списка.

Количество отображаемых элементов списка событий NDR и агрегирующих событий ограничено размером виджета.

Для каждого события в списке представлены следующие сведения:

- заголовок события NDR или агрегирующего события;
- дата и время последнего появления;
- значок, обозначающий уровень критичности события NDR или агрегирующего события:
  - – уровень критичности *Низкий*;
  - – уровень критичности *Средний*;
  - – уровень критичности *Высокий*.

Агрегирующие события в списке обозначаются значком .

Переходы к другим разделам из виджета

С помощью элементов интерфейса виджета **События в трафике сети** вы можете переходить к таблице событий для отображения подробных сведений о событиях NDR и агрегирующих событиях. Для этого предусмотрены возможности, описанные ниже.

Переход к таблице событий в трафике сети и фильтрация таблицы

Вы можете просмотреть подробные сведения о событии NDR или агрегирующем событии, нажав на нужное событие в списке виджета **События в трафике сети**. После этого откроется раздел **События в трафике сети**, в котором будет применена фильтрация таблицы по идентификатору выбранного события NDR или агрегирующего события. Также для фильтрации будет задан период от даты и времени регистрации события NDR или агрегирующего события до текущего момента (без указания конечной границы периода).

Если вы хотите перейти к таблице событий в трафике сети без изменения текущих параметров фильтрации таблицы в разделе **События в трафике сети**, перейдите по ссылке **Показать все события** в виджете **События в трафике сети**.

Переход к таблице событий и поиск в таблице

Чтобы перейти к таблице устройств и найти устройства в таблице:

1. В виджете **События в трафике сети** введите поисковый запрос в поле **Поиск событий**.
2. Нажмите на кнопку **Поиск**.

   Откроется раздел **События в трафике сети**. В таблице событий отобразятся события NDR и агрегирующие события, которые удовлетворяют условиям поиска.

Просмотр состояния работоспособности модулей и компонентов приложения

Если в работе модулей и компонентов приложения возникли проблемы, на которые администратору рекомендуется обратить внимание, в верхней части окна раздела **Мониторинг** веб-интерфейса приложения отображается рамка желтого цвета с предупреждениями.

Пользователю с ролью **Администратор** или **Аудитор** доступна информация о работоспособности того сервера Central Node, PCN или SCN, на котором он сейчас работает.

Пользователю с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** или **Аудитор** доступна следующая информация о работоспособности:

- Если вы используете отдельный сервер Central Node, пользователю доступна информация о работоспособности того сервера Central Node, на котором он сейчас работает.
- Если вы используете режим распределенного решения и мультитенантности и пользователь работает на сервере SCN, пользователю доступна информация о работоспособности этого сервера SCN в рамках тех тенантов, к данным которых у него есть доступ.
- Если вы используете режим распределенного решения и мультитенантности и пользователь работает на сервере PCN, пользователю доступна информация о работоспособности этого сервера PCN и всех серверов SCN, подключенных к этому серверу, в рамках тех тенантов, к данным которых у него есть доступ.

Чтобы получить более подробную информацию о работоспособности модулей и компонентов приложения,

по ссылке **Просмотреть сведения** откройте окно **Работоспособность системы**.

В окне **Работоспособность системы** в зависимости от работоспособности модулей и компонентов приложения отображается один из следующих значков:

- Значок OK, если модули и компоненты приложения работают нормально.
- Значок с количеством проблем (например, 1), если обнаружены проблемы, на которые администратору рекомендуется обратить внимание. В этом случае в правой части окна **Работоспособность системы** отображается подробная информация о проблемах.

Окно **Работоспособность системы** содержит разделы:

- **Работоспособность компонентов** – статус работы модулей и компонентов приложения, карантина, а также обновления баз на всех серверах, на которых работает приложение.

  Пример:
  Если базы одного или нескольких компонентов приложения не обновлялись в течение 24 часов, рядом с именем сервера, на котором установлены модули и компоненты приложения, отображается значок .
  Для решения проблемы убедитесь, что серверы обновлений доступны. Если для соединения с серверами обновлений вы используете прокси-сервер, убедитесь, что на прокси-сервере нет ошибок, связанных с подключением к серверам Kaspersky Anti Targeted Attack Platform.

- **Обработано** – статус приема и обработки входящих данных. Статус формируется на основе следующих критериев:
  - Состояние получения данных с серверов с компонентом Sensor, с сервера или виртуальной машины с почтовым сенсором, с хостов с компонентом Endpoint Agent.
  - Информация о превышении максимально допустимого времени, которое объекты ожидают в очереди на проверку модулями и компонентами приложения.
- **Соединение с серверами** – состояние соединения между сервером PCN и подключенными серверами SCN (отображается, если вы используете режим распределенного решения и мультитенантности).

В случае обнаружения проблем в работоспособности модулей и компонентов приложения, которые вы не можете решить самостоятельно, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Управление технологиями

В Kaspersky Anti Targeted Attack Platform используются различные технологии для анализа трафика сети. Вы можете включать и выключать использование технологий по отдельности. Для технологии Обнаружение активности устройств (AM) доступна возможность выбора режима работы: режим обучения или режим наблюдения.

Режим обучения рекомендуется включать на заранее определенное время, чтобы приложение автоматически переводило технологию в режим наблюдения в нужный момент. Режим наблюдения является штатным для использования технологии (в отличие от режима обучения, при котором приложение только накапливает данные для дальнейшего использования). При настройке режима обучения вы можете задать нужное время для автоматического переключения технологии в режим наблюдения.

Вы можете настроить одинаковые параметры использования технологии для всех компонентов и точек мониторинга или настроить специфические параметры для некоторых компонентов и/или точек мониторинга. Параметры использования технологии могут автоматически наследоваться от родительских объектов к дочерним. Если включено наследование технологии для компонента или точки мониторинга, на этом объекте применяются параметры использования технологии, заданные для родительского объекта (Central Node или Sensor). Если наследование технологии выключено, вы можете настроить для этого компонента или точки мониторинга специфические параметры использования технологии.

По умолчанию после установки приложения включены все технологии. Для технологий, поддерживающих изменение режима, по умолчанию включен режим обучения.

Включение и выключение технологий

Вы можете включать и выключать использование технологий для компонентов Central Node и Sensor и точек мониторинга. При этом включение и выключение технологий для компонентов Senor и точек мониторинга доступно, если на этих объектах выключено наследование технологий.

Некоторые технологии включают в себя методы, которые можно включать или выключать по отдельности. Если технология или метод выключены, приложение не контролирует взаимодействия устройств по этой технологии или по этому методу. При этом вы можете настраивать параметры работы приложения, относящиеся к выключенным технологиям или методам (например, добавлять или изменять правила).

Включение и выключение поддерживается для следующих технологий и методов:

- Контроль активов (Asset Management, далее также "AM"):
  - Обнаружение активности устройств.
  - Обнаружение сведений об устройствах.
  - Обнаружение сетевых сессий.
- Обнаружение вторжений (Intrusion detection, далее также "IDS"):
  - Обнаружение вторжений по правилам.
  - Обнаружение ARP-спуфинга.
  - Обнаружение аномалий в протоколе IP.
  - Обнаружение аномалий в протоколе TCP.
  - Обнаружение атак подбора и сканирования.

Чтобы изменить состояние технологий и методов:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента или точки мониторинга и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте или точке мониторинга.
3. Если вы хотите изменить состояние технологий и методов для компонента Sensor или для точки мониторинга, переведите переключатель **Наследовать технологии Сервера** в положение **Выключено**.
4. Включите или выключите применение нужных технологий и/или методов с помощью переключателей слева. Вы можете включить или выключить все технологии и методы одновременно с помощью ссылок **Включить все** и **Выключить все**.
5. После включения или выключения технологии или метода дождитесь применения изменений. До завершения перевода в другое состояние переключатель недоступен.

Состояние технологий и методов будет изменено.

Настройка режима работы технологии Обнаружение активности устройств

Вы можете настроить режим обучения или включить режим наблюдения для технологии Обнаружение активности устройств (AM).

Чтобы изменить и настроить режим технологии:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента или точки мониторинга и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте или точке мониторинга.
3. Если вы хотите настроить режим работы технологии для компонента Sensor или для точки мониторинга, переведите переключатель **Наследовать технологии Сервера** в положение **Выключено**.
4. В раскрывающемся списке справа от названия технологии выберите нужный режим (**Обучение** или **Наблюдение**).
5. После выбора режима дождитесь применения изменений. До применения режима в раскрывающемся списке отображается статус **Изменение**.
6. Если вы хотите указать дату и время автоматического переключения в режим наблюдения для технологии в режиме обучения, нажмите на ссылку **Указать срок** и выберите дату и время. Если дата и время были настроены ранее, то они отображаются напротив названия режима.

Режим работы технологии будет настроен.

Управление наследованием технологий

Если вы хотите, чтобы компонент Sensor или точка мониторинга автоматически получали параметры использования технологий, настроенные для родительского объекта, вы можете включить наследование технологий. При этом компонент Sensor получает параметры использования технологий, заданные для компонента Central Node, а точка мониторинга получает параметры, заданные для того компонента, на котором точка мониторинга была добавлена (Central Node или Sensor).

При необходимости вы можете выключить наследование технологий для компонента Sensor или точки мониторинга. Это позволит настроить на этом объекте специфические параметры использования технологий.

Чтобы включить или выключить наследование технологий для компонента Sensor или точки мониторинга:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента или точки мониторинга и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте или точке мониторинга.
3. Установите переключатель **Наследовать технологии Сервера** в нужное положение.

Наследование технологий для компонента Sensor или точки мониторинга будет включено или выключено.

Просмотр таблицы алертов

Обнаруженные признаки целевых атак и вторжений в IT-инфраструктуру организации в отображаются виде таблицы алертов.

В таблице алертов не отображается информация об объектах, для которых выполняется хотя бы одно из следующих условий:

- Объект имеет репутацию *Доверенный* в базе KSN.
- Объект имеет цифровую подпись одного из доверенных производителей:
  - "Лаборатория Касперского".
  - Google.
  - Apple.
  - Microsoft.

Информация об этих алертах сохраняется в журнал приложения. Вы можете просмотреть эту информацию.

Информация об алертах в журнале приложения ротируется ежедневно в ночное время при достижении максимально разрешенного количества алертов:

- Алерты, созданные компонентами **(IDS) Intrusion Detection System**, **(URL) URL Reputation** – 100 000 алертов для каждого из компонентов.
- Все остальные алерты – 20 000 алертов для каждого из модулей или компонентов.

Если вы используете режим распределенного решения и мультитенантности, то ротация производится на всех SCN, а затем происходит синхронизация с PCN. После синхронизации все удаленные алерты автоматически удаляются также на PCN.

Алерты функциональности NDR создаются при наличии действующего лицензионного ключа KATA+NDR. После истечения срока действия лицензионного ключа созданные алерты остаются доступны для просмотра, новые алерты не создаются.

Таблица алертов находится в разделе **Алерты**. В ней отображаются общие алерты KATA и алерты для функциональности NDR.

> По умолчанию в разделе отображается информация только об алертах, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных алертах тоже отображалась, включите переключатель **Показывать закрытые алерты** в правом верхнем углу окна.

Вы можете сортировать алерты в таблице по столбцам **Создано** или **Обновлено**, **Важность**, **Адрес источника**, **Адрес назначения**, **Технологии** и **Состояние**.

В таблице алертов содержится следующая информация:

1. **VIP** – наличие у алерта статуса с особыми правами доступа. Например, алерты со статусом VIP недоступны для просмотра пользователями с ролью **Сотрудник службы безопасности**.

2. **Создано** – время, когда был создан алерт и **Обновлено** – время, когда алерт был обновлен.

3. – важность алерта для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние этот алерт может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

   Алерты могут иметь одну из следующих степеней важности:

   - **Высокая**, отмеченную знаком , – алерт высокой степени важности.
   - **Средняя**, отмеченную знаком , – алерт средней степени важности.
   - **Низкая**, отмеченную знаком , – алерт низкой степени важности.

4. **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если приложение обнаружило файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого алерта.

5. **Сведения** – краткая информация об алерте. Например, имя обнаруженного файла или URL-адрес вредоносной ссылки.

6. **Адрес источника** – адрес источника обнаруженного объекта. Например, адрес электронной почты, с которого был отправлен вредоносный файл, или URL-адрес, с которого был загружен вредоносный файл.

7. **Адрес назначения** – адрес назначения обнаруженного объекта. Например, адрес электронной почты почтового домена вашей организации, на который был отправлен вредоносный файл, или IP-адрес компьютера локальной сети вашей организации, на который был загружен вредоносный файл.

8. **Технологии** – названия модулей или компонентов приложения, в результате проверки которыми был создан алерт.

   В столбце **Технологии** могут быть указаны следующие модули и компоненты приложения:

   - **(YARA) YARA**.
   - **(SB) Sandbox**.
   - **(URL) URL Reputation**.
   - **(IDS) Intrusion Detection System**.
   - **(AM) Anti-Malware Engine**.
   - **(TAA) Targeted Attack Analyzer**.
   - **(IOC) IOC**.
   - **(NDR: IDS) Intrusion Detection System**.
   - **(AA) Aggregated Alerts**.

9. **Состояние** – состояние алерта в зависимости от того, обработал пользователь Kaspersky Anti Targeted Attack Platform этот алерт или нет.

   Алерты могут быть в одном из следующих состояний:

   - **Новое** – новые алерты.
   - **В обработке** – алерты, которые один из пользователей Kaspersky Anti Targeted Attack Platform уже обрабатывает.
   - **Повторная проверка** – алерты, выполненные в результате повторной проверки объекта.
   - **Закрыто** – закрытые алерты. Закрытые алерты отображаются в таблице, если включен переключатель **Показывать закрытые алерты**.

- **Серверы** – имена серверов, на которых созданы алерты. Серверы относятся к тому тенанту, с которым вы работаете в веб-интерфейсе приложения. Столбец отображается, если вы используете режим распределенного решения и мультитенантности.
- **Назначено** – имя пользователя, которому назначен алерт.

Если информация в столбце таблицы отображается в виде ссылки, по ссылке раскрывается меню фильтрации, в котором вы можете выбрать параметры фильтрации по столбцу.

Особенности обновления алертов и агрегации событий в них

Модуль **Targeted Attack Analyzer** обновляет список хостов и количество событий в алерте, если при обработке событий были найдены события с аналогичным идентификатором сработавшего правила TAA (IOA). Обновление выполняется в пределах текущих суток - с 00:00 до 00:00 следующего дня. Если на момент обновления алерт закрыт, система автоматически переоткрывает его.

Модуль **Intrusion Detection System** консолидирует информацию об обработанных сетевых событиях в одном алерте при одновременном соблюдении следующих условий:

- для сетевых событий совпадает название сработавшего правила, версия баз приложения и источник;
- между событиями прошло не более 24 часов.

Для всех сетевых событий, удовлетворяющих этим условиям, отображается один алерт. В уведомлении об алерте содержится информация только о первом сетевом событии.

Настройка отображения таблицы алертов

Вы можете настроить отображение столбцов, а также порядок их следования в таблице алертов.

Чтобы настроить отображение таблицы алертов:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.

3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.

5. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.

6. Нажмите на кнопку **Применить**.

Отображение таблицы алертов будет настроено.

Фильтрация, сортировка и поиск алертов

Вы можете отфильтровать алерты для отображения в таблице алертов по одному или нескольким столбцам таблицы или выполнить поиск алертов по некоторым столбцам таблицы.

Вы можете создавать, сохранять и удалять фильтры, а также запускать фильтрацию и поиск алертов по условиям, заданным в сохраненных фильтрах.

> Если вы используете режим распределенного решения и мультитенантности, вы не сможете сохранять фильтры на PCN.

Фильтры сохраняются для каждого из пользователей на том сервере, на котором они созданы.

Вы также можете сортировать алерты в таблице по столбцам **Создано** или **Обновлено**, **Важность**, **Адрес источника**, **Адрес назначения**, **Технологии** и **Состояние**.

> По умолчанию в разделе отображается информация только об алертах, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных алертах тоже отображалась, включите переключатель **Показывать закрытые алерты** в правом верхнем углу окна.

Фильтрация алертов по наличию статуса VIP

Вы можете отфильтровать алерты, а также осуществить их поиск в таблице алертов по показателю ☆ – наличие у алерта статуса с особыми правами доступа. Например, алерты со статусом VIP недоступны для просмотра пользователями с ролью **Сотрудник службы безопасности**.

Чтобы отфильтровать алерты по наличию статуса VIP:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Нажатием на заголовок столбца **VIP** раскройте список параметров фильтрации.

3. Настройте фильтрацию алертов:

   - Если вы хотите, чтобы в таблице алертов отобразились только алерты со статусом VIP, выберите **VIP**.
   - Если вы хотите, чтобы в таблице алертов отобразились все алерты, выберите **Все**.

   Если ни одно из значений не выбрано, в таблице отображаются все алерты.

В таблице алертов отобразятся только алерты, соответствующие заданным вами условиям.

Фильтрация и поиск алертов по времени

Вы можете отфильтровать алерты, а также осуществить их поиск в таблице алертов по показателю **Создано** – время, когда был создан алерт, а также **Обновлено** – время, когда алерт был обновлен.

Чтобы отфильтровать или найти алерты по времени:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. По ссылке **Создано** или **Обновлено** раскройте список периодов отображения алертов.

3. В раскрывающемся списке выберите один из следующих периодов отображения алертов:

   - **Все**, если вы хотите, чтобы приложение отображало в таблице все алерты.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице алерты, произошедшие за последний час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице алерты, произошедшие за последний день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице алерты, произошедшие за указанный вами период.

4. Если вы выбрали период отображения событий **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения алертов.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

В таблице алертов отобразятся только алерты, соответствующие заданным вами условиям.

Фильтрация алертов по степени важности

Вы можете отфильтровать алерты по показателю **Важность** – важность алерта для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние этот алерт может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

Чтобы отфильтровать алерты по степени важности:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. По значку раскройте список параметров фильтрации.

3. Выберите одну или несколько из следующих степеней важности алертов:

   - **Низкая** – алерты низкой степени важности.
   - **Средняя** – алерты средней степени важности.
   - **Высокая** – алерты высокой степени важности.

   Если ни одно из значений не выбрано, в таблице отображаются алерты всех степеней важности.

4. Нажмите на кнопку **Применить**.

В таблице алертов отобразятся только алерты, соответствующие заданным вами условиям.

Фильтрация и поиск алертов по категориям обнаруженных объектов

Вы можете отфильтровать алерты, а также осуществить их поиск в таблице алертов по показателю **Обнаружено** – одна или несколько категорий объекта, обнаруженного в событии. Например, если вы хотите, чтобы приложение отображало в таблице алертов файлы, зараженные определенным вирусом, вы можете задать фильтр по названию этого вируса.

Чтобы отфильтровать или найти алерты по категориям обнаруженных объектов:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. По ссылке **Обнаружено** откройте окно настройки фильтрации.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации алертов:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода введите название категории (например, Trojan) или несколько символов из названия категории.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Нажмите на кнопку **Применить**.

В таблице алертов отобразятся только алерты, соответствующие заданным вами условиям.

Фильтрация и поиск алертов по полученной информации

Вы можете отфильтровать алерты, а также осуществить их поиск в таблице алертов по показателю **Сведения** – краткая информация об алерте. Например, имя обнаруженного файла или URL-адрес вредоносной ссылки.

Чтобы отфильтровать или найти алерты по полученной информации:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. По ссылке **Сведения** откройте окно настройки фильтрации.

3. В левом раскрывающемся списке выберите один из следующих критериев поиска:

   - **Сведения**. Поиск будет осуществляться по всем сведениям об обнаруженном объекте.
   - **ID**.
   - **Файл**.
   - **Тип файла**.
   - **MD5**.
   - **SHA256**.
   - **URL**.
   - **Домен**.
   - **Агент пользователя**.
   - **Тема**.
   - **HTTP-статус**.
   - **Источник объекта**.
   - **Тип объекта**.
   - **Автоотправка в Sandbox**.

- **Правило TAA (IOA)**.
- **ID события (NDR)**.
- **ID актива (NDR)**.

4. В правом раскрывающемся списке выберите один из следующих операторов фильтрации алертов:
   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.
5. В поле ввода укажите один или несколько символов информации об алерте.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице алертов отобразятся только алерты, соответствующие заданным вами условиям.

Фильтрация и поиск алертов по адресу источника

Вы можете отфильтровать алерты, а также осуществить их поиск в таблице алертов по показателю **Адрес источника** – адрес источника обнаруженного объекта. Например, адрес электронной почты, с которого был отправлен вредоносный файл, или IP-адрес компьютера локальной сети вашей организации, на который был загружен вредоносный файл.

Чтобы отфильтровать или найти алерты по адресу источника:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.
2. По ссылке **Адрес источника** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации алертов:
   - **Содержит**.
   - **Не содержит**.
   - **Соответствует шаблону**.
   - **Не соответствует шаблону**.
4. В поле ввода укажите один или несколько символов адреса источника обнаруженного объекта.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Нажмите на кнопку **Применить**.

В таблице алертов отобразятся только алерты, соответствующие заданным вами условиям.

Фильтрация и поиск алертов по адресу назначения

Вы можете отфильтровать алерты, а также осуществить их поиск в таблице алертов по показателю **Адрес назначения** – адрес назначения обнаруженного объекта. Например, адрес электронной почты почтового домена вашей организации, на который был отправлен вредоносный файл, или IP-адрес компьютера локальной сети вашей организации, на который был загружен вредоносный файл.

Чтобы отфильтровать или найти алерты по адресу назначения:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. По ссылке **Адрес назначения** откройте окно настройки фильтрации.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации алертов:

   - **Содержит**.
   - **Не содержит**.
   - **Соответствует шаблону**.
   - **Не соответствует шаблону**.

4. В поле ввода укажите один или несколько символов адреса назначения обнаруженного объекта.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Нажмите на кнопку **Применить**.

В таблице алертов отобразятся только алерты, соответствующие заданным вами условиям.

Фильтрация и поиск алертов по имени сервера

Вы можете отфильтровать алерты, а также осуществить их поиск в таблице алертов по показателю **Серверы** – имена серверов, на которых были созданы алерты.

Если вы используете режим распределенного решения и мультитенантности, серверы относятся к тому тенанту, с которым вы работаете в веб-интерфейсе приложения. Фильтрация доступна только на PCN.

Чтобы отфильтровать или найти алерты по имени сервера:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. По ссылке **Серверы** раскройте список серверов, на которых были созданы алерты.

3. Установите флажки рядом с одним или несколькими именами серверов.

4. Нажмите на кнопку **Применить**.

В таблице алертов отобразятся только алерты, соответствующие заданным вами условиям.

Фильтрация и поиск алертов по названию технологии

Вы можете отфильтровать алерты, а также осуществить их поиск в таблице алертов по показателю **Технологии** – названия модулей или компонентов приложения, создавших алерт.

Чтобы отфильтровать алерты по названию технологии:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. По ссылке **Технологии** откройте окно настройки фильтрации.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации алертов:

   - **Содержит**, если вы хотите, чтобы приложение отображало алерты, созданные в результате проверки модулем или компонентом приложения, который вы укажете.
   - **Не содержит**, если вы хотите, чтобы приложение скрывало алерты, созданные в результате проверки модулем или компонентом приложения, который вы укажете.
   - **Равняется**, если вы хотите, чтобы приложение отображало алерты, выполненные модулем или компонентом приложения, который вы укажете.
   - **Не равняется**, если вы хотите, чтобы приложение скрывало алерты, выполненные модулем или компонентом приложения, который вы укажете.

4. В раскрывающемся списке справа от выбранного вами оператора фильтрации алертов выберите название технологии, по которой вы хотите отфильтровать алерты:

   - **(YARA) YARA**.
   - **(SB) Sandbox**.
   - **(URL) URL Reputation**.
   - **(IDS) Intrusion Detection System**.
   - **(AM) Anti-Malware Engine**.
   - **(TAA) Targeted Attack Analyzer**.

- **(IOC) IOC**.
- **(NDR: IDS) Intrusion Detection System**.
- **(AA) Aggregated Alerts**.

Например, если вы хотите, чтобы приложение отобразило в списке алерты, созданные в результате проверки компонентом Sandbox, выберите оператор фильтрации **Содержит** и название компонента **(SB) Sandbox**.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице алертов отобразятся только алерты, соответствующие заданным вами условиям.

Фильтрация и поиск алертов по состоянию их обработки пользователем

Вы можете отфильтровать алерты, а также осуществить их поиск в таблице алертов по показателю **Состояние** – состояние алерта в зависимости от того, обработал пользователь Kaspersky Anti Targeted Attack Platform этот алерт или нет.

Чтобы отфильтровать или найти алерты по состоянию их обработки пользователем Kaspersky Anti Targeted Attack Platform:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.
2. Если вы хотите включить в фильтр обработанные алерты, включите переключатель **Показывать закрытые алерты** в правом верхнем углу окна.
3. По ссылке **Состояние** раскройте список вариантов алертов в зависимости от состояния их обработки пользователем Kaspersky Anti Targeted Attack Platform.
4. Выберите одно из следующих значений:
   - **Новое**, если вы хотите, чтобы приложение отображало новые алерты, которые ни один из пользователей еще не начал обрабатывать.
   - **В обработке**, если вы хотите, чтобы приложение отображало алерты, которые один из пользователей Kaspersky Anti Targeted Attack Platform уже обрабатывает.
   - **Повторная проверка**, если вы хотите, чтобы приложение отображало алерты, произошедшие в результате повторной проверки.
   - **Закрыто**, если вы хотите, чтобы приложение отображало закрытые алерты. Фильтр доступен, если включен переключатель **Показывать закрытые алерты**.
5. Нажмите на кнопку **Применить**.

В таблице алертов отобразятся только алерты, соответствующие заданным вами условиям.

Фильтрация и поиск алертов по имени пользователя, которому они назначены

Вы можете отфильтровать алерты, а также осуществить их поиск в таблице алертов по показателю **Назначено** – имя пользователя, которому назначен алерта.

Чтобы отфильтровать или найти алерты по имени пользователя, которому они назначены:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. По ссылке **Назначено** откройте окно настройки фильтрации.

3. Установите флажок около имени нужного пользователя.

   Если нужно найти имя пользователя в отображаемом списке, начните вводить имя пользователя в текстовом поле, а затем установите флажок около найденного имени пользователя.

   Вы можете выбрать несколько имен пользователей.

4. Нажмите на кнопку **Применить**.

В таблице алертов отобразятся только алерты, назначенные указанному пользователю.

Сортировка алертов в таблице

Вы можете сортировать алерты в таблице по столбцам **Создано** или **Обновлено**, **Важность**, **Адрес источника**, **Адрес назначения**, **Технологии** и **Состояние**.

Чтобы отсортировать алерты в таблице алертов:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Если вы хотите отсортировать алерты по дате, справа от названия столбца **Создано** (если в таблице отображается дата создания алертов) или **Обновлено** (если в таблице отображается дата обновления алертов) нажмите на один из значков:

   - ↑ – новые алерты отобразятся вверху таблицы.
   - ↓ – старые алерты отобразятся вверху таблицы.

3. Если вы хотите отсортировать алерты по степени важности, справа от значка ≣ нажмите на один из значков:

   - ↑ – алерты высокой степени важности отобразятся вверху таблицы.
   - ↓ – алерты низкой степени важности отобразятся вверху таблицы.

4. Если вы хотите отсортировать алерты по адресу источника обнаруженного объекта, справа от названия столбца **Адрес источника** нажмите на один из значков:

   - ↑ – сортировка выполнится по возрастанию.
   - ↓ – сортировка выполнится по убыванию.

5. Если вы хотите отсортировать алерты по адресу назначения обнаруженного объекта, справа от названия столбца **Адрес назначения** нажмите на один из значков:

   - ↑ – сортировка выполнится по возрастанию.
   - ↓ – сортировка выполнится по убыванию.

6. Если вы хотите отсортировать алерты по имени технологии, выполнившей обнаружение, справа от названия столбца **Технологии** нажмите на один из значков:

   - ↑ – сортировка выполнится по алфавиту A–Z.
   - ↓ – сортировка выполнится по алфавиту Z–A.

7. Если вы хотите отсортировать алерты по состоянию их обработки пользователем, справа от названия столбца **Состояние** нажмите на один из значков:

   - ↑ – алерты будут отсортированы по порядку их обработки **Новое** - **Повторная проверка** - **В обработке** - **Закрыто**.
   - ↓ – алерты будут отсортированы по порядку их обработки **Закрыто** - **В обработке** - **Повторная проверка** - **Новое**.

Быстрое создание фильтра алертов

Чтобы быстро создать фильтр алертов:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:

   a. Наведите курсор мыши на ссылку с тем значением столбца таблицы, которое вы хотите добавить в качестве условия фильтрации.

   b. Нажмите на левую клавишу мыши.

   Откроется список действий над значением.

   c. В открывшемся списке выберите одно из следующих действий:

   - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
   - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.

3. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице алертов отобразятся только алерты, соответствующие заданным вами условиям.

Сохранение фильтров

Вы можете сохранить набор примененных фильтров содержимого таблицы алертов.

Чтобы сохранить примененные фильтры:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Настройте параметры фильтрации по одному или нескольким столбцам таблицы.

3. Нажмите на кнопку **Сохраненные фильтры** и выберите **Сохранить текущий фильтр**.

   Фильтр будет сохранен с названием по умолчанию, которое содержит выбранные параметры фильтрации.

4. Если вы хотите изменить название сохраненного фильтра, выполните следующие действия:

   a. Нажмите на кнопку **Сохраненные фильтры**.

      Отобразится список сохраненных фильтров.

   b. Наведите курсор мыши на нужный фильтр и нажмите на значок .

   c. Измените название фильтра и нажмите на значок .

Фильтр будет сохранен.

Сброс фильтра алертов

Чтобы сбросить фильтр алертов по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Нажмите на кнопку справа от того заголовка столбца таблицы алертов, условия фильтрации по которому вы хотите сбросить.

   > Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице алертов отобразятся только алерты, соответствующие заданным вами условиям.

Рекомендации по обработке алертов

В составе информации об алертах, выполненных технологиями AM (Anti-Malware Engine), SB (Sandbox), YARA, IOC, IDS (intrusion Detection System), NDR: IDS и AA (Aggregated Alerts) в правой части окна отображаются рекомендации по обработке этих алертов.

Чтобы просмотреть информацию об алерте:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Левой клавишей мыши нажмите на строку с тем алертом, информацию о котором вы хотите просмотреть.

Откроется окно с информацией об алерте.

Рекомендации по обработке AM-алертов

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество алертов или событий, имеющих общие признаки с алертом, над которым вы работаете.

Вы можете выполнить следующие рекомендации:

- В разделе **Оценка** раскройте список **Найти похожие алерты**.

  Отобразится список признаков, по которым вы можете найти похожие алерты, и количество похожих алертов по каждому признаку.

  Выберите один из следующих признаков:

  - **По MD5**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения** - MD5-хешу. MD5-хеш файла из алерта, над которым вы работаете, выделен желтым цветом.

  - **По SHA256**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения** - SHA256-хешу. SHA256-хеш файла из алерта, над которым вы работаете, выделен желтым цветом.

  - **По имени хоста**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес источника**. Имя хоста из алерта, над которым вы работаете, выделено желтым цветом.

  - **По адресу отправителя**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес источника**. Адрес отправителя сообщения электронной почты из алерта, над которым вы работаете, выделен желтым цветом.

  - **По адресу получателя**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес назначения**. Адрес получателя сообщения электронной почты из алерта, над которым вы работаете, выделен желтым цветом.

  - **По URL**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения** - URL-адресу из алерта, над которым вы работаете.

- В разделе **Оценка** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска выбран тип события **Результат обработки обнаружения** и настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства алерта, над которым вы работаете. Например, MD5 файла из алерта.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства алерта, над которым вы работаете. Например, MD5 файла из алерта.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

Рекомендации по обработке TAA-алертов

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество алертов или событий, имеющих общие признаки с алертов, над которым вы работаете.

Вы можете выполнить следующие рекомендации:

- В разделе **Оценка** раскройте список **Найти похожие алерты**.

  Отобразится список признаков, по которым вы можете найти похожие алерты, и количество похожих алертов по каждому признаку.

  Выберите один из следующих признаков:

  - **По имени правила (TAA-алерты)**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцам **Обнаружено** и **Технологии** - имени правила TAA (IOA), в соответствии с которым был создан алерт, и названию технологии **(TAA) Targeted Attack Analyzer**.

  - **По имени правила (SB-алерта)**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцам **Обнаружено** и **Технологии** - имени правила TAA (IOA), в соответствии с которым был создан алерт, и названию технологии **(SB) Sandbox**.

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства алертов, над которым вы работаете. Например, MD5 файла из алерта.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

Рекомендации по обработке SB-алертов

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество алертов или событий, имеющих общие признаки с алертом, над которым вы работаете.

Вы можете выполнить следующие рекомендации:

- В разделе **Оценка** раскройте список **Найти похожие алерты**.

  Отобразится список признаков, по которым вы можете найти похожие алерты, и количество похожих алертов по каждому признаку.

  Выберите один из следующих признаков:

  - **По MD5**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения** - MD5-хешу. MD5-хеш файла из алерта, над которым вы работаете, выделен желтым цветом.

  - **По SHA256**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения** - SHA256-хешу. SHA256-хеш файла из алерта, над которым вы работаете, выделен желтым цветом.

  - **По имени хоста**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес источника**. Имя хоста из алерта, над которым вы работаете, выделено желтым цветом.

  - **По адресу отправителя**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес источника**. Адрес отправителя сообщения электронной почты из алерта, над которым вы работаете, выделен желтым цветом.

  - **По адресу получателя**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес назначения**. Адрес получателя сообщения электронной почты из алерта, над которым вы работаете, выделен желтым цветом.

  - **По URL**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения** - URL-адресу из алерта, над которым вы работаете.

  - **По URL из Sandbox**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения** - URL-адресу из алерта, над которым вы работаете, и всем URL-адресам, связь с которыми нашел компонент Sandbox в процессе обработки алерта.

- В разделе **Оценка** выберите **Найти похожие EPP-события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска выбран тип события **Результат обработки обнаружения** и настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства алерта, над которым вы работаете. Например, MD5 файла из алерта.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства алерта, над которым вы работаете. Например, MD5 файла из алерта.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

Рекомендации по обработке IOC-алертов

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество алертов, имеющих общие признаки с алертом, над которым вы работаете.

Вы можете выполнить следующие рекомендации:

- В разделе **Оценка** выберите **Найти похожие алерты по имени хоста**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес источника**. Имя хоста из алерта, над которым вы работаете, выделено желтым цветом.

- В разделе **Оценка** выберите **Найти похожие алерты по IOC**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Алерты**, отфильтрованных по столбцу **Обнаружено** - имени IOC-файла из алерта, над которым вы работаете.

- В разделе **Сдерживание** выберите **Изолировать <имя хоста>**. Откроется окно создания правила сетевой изоляции.

Рекомендации по обработке YARA-алертов

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество алертов или событий, имеющих общие признаки с алертом, над которым вы работаете.

Вы можете выполнить следующие рекомендации:

- В разделе **Оценка** раскройте список **Найти похожие алерты**.

  Отобразится список признаков, по которым вы можете найти похожие алерты, и количество похожих алертов по каждому признаку.

  Выберите один из следующих признаков:

  - **По MD5**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения** - MD5-хешу. MD5-хеш файла из алерта, над которым вы работаете, выделен желтым цветом.

  - **По SHA256**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения** - SHA256-хешу. SHA256-хеш файла из алерта, над которым вы работаете, выделен желтым цветом.

  - **По имени хоста**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес источника**. Имя хоста из алерта, над которым вы работаете, выделено желтым цветом.

- **По адресу отправителя**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес источника**. Адрес отправителя сообщения электронной почты из алерта, над которым вы работаете, выделен желтым цветом.

- **По адресу получателя**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес назначения**. Адрес получателя сообщения электронной почты из алерта, над которым вы работаете, выделен желтым цветом.

- **По URL**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения** - URL-адресу из алерта, над которым вы работаете.

- В разделе **Оценка** выберите **Найти похожие алерты по имени хоста**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска выбран тип события **Результат обработки обнаружения** и настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства алерта, над которым вы работаете. Например, MD5 файла из алерта.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства алерта, над которым вы работаете. Например, MD5 файла из алерта.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

- В разделе **Сдерживание** выберите **Изолировать <имя хоста>**. Откроется окно создания правила сетевой изоляции.

Рекомендации по обработке IDS-алертов

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество алертов или событий, имеющих общие признаки с алертом, над которым вы работаете.

Вы можете выполнить следующие рекомендации:

- В разделе **Оценка** выберите **Найти похожие алерты по IP-адресу**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес источника**. Имя хоста или IP-адрес из алерта, над которым вы работаете, выделено желтым цветом.

- В разделе **Оценка** выберите **Найти похожие алерты по URL**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения** - URL-адресу. URL-адрес из алерта, над которым вы работаете, выделен желтым цветом.

- В разделе **Оценка** выберите **Добавить в исключения**.

  Откроется окно **Добавить правило IDS в исключения**. Если вы хотите добавить правило IDS, по которому создан алерт, в исключения, введите комментарий в поле **Описание** и нажмите на кнопку **Добавить**.

  Правило IDS будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса приложения, подразделе **Исключения** на закладке **IDS**.

- В разделе **Расследование** выберите **Найти похожие события по URL**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска по **URI** из алерта, над которым вы работаете.

- В разделе **Расследование** выберите **Найти похожие события по IP-адресу**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска по **RemoteIP** из алерта, над которым вы работаете.

- В разделе **Расследование** по ссылке **Скачать артефакт IDS** вы можете скачать файл с данными об алерте.

- В разделе **Расследование** по ссылке **Скачать PCAP-файл** вы можете скачать файл с данными перехваченного трафика.

Рекомендации по обработке NDR:IDS- и AA-алертов

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество алертов или событий, имеющих общие признаки с алертом, над которым вы работаете.

Вы можете выполнить следующие рекомендации:

- В разделе **Оценка** выберите **Найти похожие алерты по IP источника**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес источника**. Имя хоста или IP-адрес из алерта, над которым вы работаете, выделено желтым цветом.

- В разделе **Оценка** выберите **Найти похожие алерты по IP назначения**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Адрес назначения**. Имя хоста или IP-адрес из алерта, над которым вы работаете, выделено желтым цветом.

- В разделе **Оценка** выберите **Найти похожие события по URL**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения**. URL из алерта, над которым вы работаете, выделен желтым цветом.

- В разделе **Оценка** выберите **Найти похожие алерты по правилу обнаружения вторжений**. По ссылке в новой вкладке браузера откроется таблица алертов **Алерты**, отфильтрованных по столбцу **Сведения**. Результат проверки из алерта, над которым вы работаете, выделен желтым цветом.

- В разделе **Скачать** по ссылке **Скачать PCAP-файл** вы можете скачать файл с данными перехваченного трафика.

Просмотр алертов

В веб-интерфейсе приложения отображаются следующие типы алертов, на которые пользователю Kaspersky Anti Targeted Attack Platform рекомендуется обратить внимание:

- На компьютер локальной сети организации был загружен файл или была предпринята попытка загрузки файла. Приложение обнаружило этот файл в зеркалированном трафике локальной сети организации или в ICAP-данных HTTP- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на прокси-сервере.

- На адрес электронной почты пользователя локальной сети организации был отправлен файл. Приложение обнаружило этот файл в копиях сообщений электронной почты, полученных по протоколу POP3 или SMTP, или полученных с виртуальной машины или сервера с программой Kaspersky Secure Mail Gateway, если она используется в вашей организации.

- На компьютере локальной сети организации была открыта ссылка на веб-сайт. Приложение обнаружило эту ссылку на веб-сайт в зеркалированном трафике локальной сети организации или в ICAP-данных HTTP- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на прокси-сервере.

- IP-адрес или доменное имя компьютера локальной сети организации были замечены в сетевой активности. Приложение обнаружило эту сетевую активность в зеркалированном трафике локальной сети организации.

- На компьютере локальной сети организации были запущены процессы. Приложение обнаружило эти процессы с помощью компонента Endpoint Agent, установленного на компьютеры, входящие в IT-инфраструктуру организации.

Если обнаружен файл, в зависимости от того, какие модули или компоненты приложения создали алерт, в веб-интерфейсе приложения может отображаться следующая информация:

- общая информация об алерте и обнаруженном файле (например, IP-адрес компьютера, на котором обнаружен файл, имя обнаруженного файла);

- результаты антивирусной проверки файла, выполненной ядром AM Engine;

- результаты проверки файла на наличие признаков вторжения в IT-инфраструктуру организации, выполненной модулем YARA;

- результаты исследования поведения файла, выполненного компонентом Sandbox;

- результаты анализа исполняемых файлов формата APK в облачной инфраструктуре на основе технологии машинного обучения.

Если обнаружена ссылка на веб-сайт, в зависимости от того, какие модули или компоненты приложения создали алерт, в веб-интерфейсе приложения может отображаться следующая информация:

- детали алерта и обнаруженной ссылки на веб-сайт (например, IP-адрес компьютера, на котором обнаружена ссылка на веб-сайт, адрес ссылки на веб-сайт);

- результаты проверки ссылки на наличие признаков вредоносного, фишингового URL-адреса или URL-адреса, который ранее использовался злоумышленниками для целевых атак на IT-инфраструктуру организаций, выполненной модулем URL Reputation.

Если обнаружена сетевая активность IP-адреса или доменного имени компьютера локальной сети организации, в веб-интерфейсе приложения может отображаться следующая информация:

- детали алерта и обнаруженной сетевой активности;
- результаты проверки интернет-трафика на наличие признаков вторжения в IT-инфраструктуру организации по предустановленным правилам, выполненной модулем Intrusion Detection System (IDS);
- результаты исследования сетевой активности, выполненного по пользовательским правилам IDS.

Управлять алертами могут пользователи с ролью **Сотрудник службы безопасности** или **Старший сотрудник службы безопасности**. Пользователи с ролью **Аудитор** могут просматривать алерты.

Просмотр информации об алерте

Чтобы просмотреть информацию об алерте:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Левой клавишей мыши нажмите на строку с тем алертом, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об алерте.

Общая информация об алерте любого типа

В заголовке окна с деталями алерта отображается идентификатор алерта. Рядом с состоянием отображается значок ☆ или ★ в зависимости от наличия у алерта статуса VIP.

В верхней части окна с деталями алерта может отображаться следующая общая информация об алерте:

- **Состояние** – состояние алерта в зависимости от того, обработал пользователь Kaspersky Anti Targeted Attack Platform этот алерт или нет.
- **Важность** – важность алерта для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние этот алерт может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".
- **Сервер** – имя сервера, на котором выполнено обнаружение. Серверы относятся к той организации, с которой вы работаете в веб-интерфейсе приложения. Столбец отображается, если вы используете режим распределенного решения и мультитенантности.
- **Хост** – доменное имя компьютера, на котором создан алерт.
- **Источник данных** – источник данных. Например, SMTP Sensor или SPAN Sensor.
- **Время создания** – время, когда был создан алерт.
- **Время обновления** – время, когда были обновлены детали алерта.

Вы можете настроить получение уведомлений о новых алертах на электронную почту.

Информация в блоке Информация об объекте

В блоке **Информация об объекте** может отображаться следующая информация об обнаруженном объекте:

- Имя файла.

  По ссылке с именем файла раскрывается действие **Скопировать значение в буфер**.

- Тип файла. Например, ExecutableWin32.

  Кнопка **Найти на Kaspersky TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

  Кнопка **Создать правило запрета** позволяет запретить запуск файла.

  Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

  Файл загружается в формате ZIP-архива, зашифрованного паролем infected. Имя файла внутри архива заменено на MD5-хеш файла. Расширение файла внутри архива не отображается.

- Размер файла в килобайтах.

- **MD5** – MD5-хеш файла.

  По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на Kaspersky TIP**.
  - **Найти события**.
  - **Найти алерты**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

- **SHA256** – SHA256-хеш файла.

  По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на Kaspersky TIP**.
  - **Найти на virustotal.com**.
  - **Найти события**.
  - **Найти алерты**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

- **Адрес отправителя** – адрес электронной почты, с которого было отправлено сообщение, содержащее файл.

- **Адрес получателя** – один или несколько адресов электронной почты, на которые было отправлено сообщение, содержащее файл.

- **Исходный адрес отправителя** – исходный адрес электронной почты, с которого было отправлено сообщение, содержащее файл.

  Данные для этого поля берутся из заголовка Received.

- **Исходный адрес получателя** – исходный адрес или адреса электронной почты, на которые было отправлено сообщение, содержащее файл.

  Данные для этого поля берутся из заголовка Received.

- **Тема** – тема сообщения.

- **IP сервера-отправителя** – IP-адрес первого в цепочке отправки сообщения почтового сервера.

  По ссылке **IP сервера-отправителя** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - **Найти алерты**.
  - **Скопировать значение в буфер**.

- **Заголовки** – расширенный набор заголовков сообщения электронной почты. Например, может содержать информацию об адресах электронной почты отправителя и получателей сообщения, о почтовых серверах, передавших сообщение, о типе контента сообщения электронной почты.

Информация в блоке Детали алерта

В блоке **Информация об алерте** может отображаться следующая информация об алерте:

- , или – важность алерта для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние этот алерт может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

- **Время** – время, когда был создан алерт.

- **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если приложение обнаружило файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого алерта.

- **Метод** – метод HTTP-запроса. Например, Get, Post или Connect.

- **URL** – обнаруженный URL-адрес. Может также содержать код ответа.

  По ссылке с **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на Kaspersky TIP по URL**.
  - **Найти на Kaspersky TIP по имени домена**.
  - **Найти события**.
  - **Найти алерты**.
  - **Скопировать значение в буфер**.

- **Referrer** – URL-адрес, с которого произошло перенаправление на ссылку на веб-сайт, требующую внимания. В HTTP-протоколе это один из заголовков запроса клиента, содержащий URL-адрес источника запроса.
- **IP назначения** – IP-адрес ресурса, к которому обращался пользователь или приложение.

  По ссылке с **IP назначения** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на Kaspersky TIP**.
  - **Найти события**.
  - **Найти алерты**.
  - **Скопировать значение в буфер**.
- **Имя пользователя** – имя учетной записи пользователя, действия которого привели к возникновению события.
- **Запрос/Ответ** – длина запроса и ответа.

Информация в блоке Сведения о проверке технологиями NDR

В блоке **Сведения о проверке технологиями NDR** могут отображаться следующие результаты:

- **Точка мониторинга** – имя точки мониторинга, трафик с которой привел к регистрации события в трафике сети и возникновению алерта.
- **ID сетевого интерфейса** – идентификатор точки мониторинга, трафик с которой привел к регистрации события в трафике сети и возникновению алерта.

Информация в блоке Результаты проверки

В блоке **Результаты проверки** могут отображаться следующие результаты:

- Названия модулей или компонентов приложения, создавших алерт.
- Одна или несколько категорий обнаруженного объекта. Например, может отображаться название вируса Virus.Win32.Chiton.i.
- Версии баз модулей и компонентов Kaspersky Anti Targeted Attack Platform, создавших алерт.
- Результаты проверки алерта модулями и компонентами приложения:
  - **YARA** – результаты потоковой проверки файлов и объектов, поступающих на Central Node, или результаты проверки хостов с компонентом Endpoint Agent. Может принимать следующие значения:
    - Категория обнаруженного файла в правилах YARA (например, может отображаться название категории susp_fake_Microsoft_signer).

      Отображается при потоковой проверке.

Кнопка **Создать правило запрета** позволяет запретить запуск файла.

Кнопка **Найти на Kaspersky TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

- Путь к файлу и/или имя дампа памяти.

  Отображается при проверке хостов с компонентом Endpoint Agent.

  По ссылке с путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - **Найти алерты**.
  - **Скопировать значение в буфер**.

  Кнопка **Создать задачу** позволяет создать следующие задачи:

  - **Собрать данные** → **Файл**, **Образ диска**, **Дамп памяти**.
  - **Удалить файл**.
  - **Поместить файл на карантин**.

  Кнопка **Создать правило запрета** позволяет запретить запуск файла.

- Кнопка **Найти на Kaspersky TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

  Кнопка **Просмотреть на карантине** позволяет просмотреть информацию об объекте, помещенном на карантин.

- **SB** (Sandbox) – результаты исследования поведения файла, выполненного компонентом Sandbox.

  Нажатием на кнопку **Sandbox-обнаружение** вы можете открыть окно с подробной информацией о результатах исследования поведения файла.

  > Результаты исследования поведения файла отображаются, только если для этого файла было выполнено обнаружение компонентом Sandbox. Если файл был загружен в систему и затем проверен в Sandbox, но компонент при этом не обнаружил угрозу, результаты исследования не отображаются.

  Кнопка **Найти на Kaspersky TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

  Кнопка **Создать правило запрета** позволяет запретить запуск файла.

  Вы можете загрузить подробный журнал исследования поведения файла во всех операционных системах, нажав на кнопку **Скачать сведения об отладке**.

  Файл загружается в формате ZIP-архива, зашифрованного паролем infected. Имя проверенного файла внутри архива заменено на MD5-хеш файла. Расширение файла внутри архива не отображается.

  > По умолчанию максимальный объем жесткого диска для хранения журналов исследования поведения файлов во всех операционных системах составляет 300 ГБ. По достижении этого ограничения приложение удаляет журналы исследования поведения файлов, созданные раньше остальных, и заменяет их новыми журналами.

- **URL** (URL Reputation) – категория обнаруженного вредоносного, фишингового URL-адреса или URL-адреса, который ранее использовался злоумышленниками для целевых атак на IT-инфраструктуру организаций.

- **AM** (Anti-Malware Engine) – категория обнаруженного объекта по антивирусной базе. Например, может отображаться название вируса Virus.Win32.Chiton.i.

  По ссылке открывается информация о категории объекта в базе угроз "Лаборатории Касперского" Kaspersky Threats.

  Кнопка **Найти на Kaspersky TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

  Кнопка **Создать правило запрета** позволяет запретить запуск файла.

  Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

- **TAA** (Targeted Attack Analyzer) – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому был создан алерт.

  По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

- **IOC** – название IOC-файла, по которому был создан алерт.

  При выборе IOC-файла открывается окно с результатами IOC-проверки.

  По ссылке **Все события, связанные с алертом** в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **MD5**, **FileFullName**. В значениях фильтрации указаны свойства алерта, над которым вы работаете. Например, MD5 файла из алерта.

- **AA** (Aggregated Alerts) – алерт создан в результате обработки агрегирующих и вложенных событий NDR, которые поступают в Kaspersky Anti Targeted Attack Platform от сторонних систем с использованием методов API NDR. События регистрируются по технологии EXT.

- **NDR: IDS** (Intrusion Detection System) – алерт создан в результате обработки события NDR, связанного с обнаружением в трафике аномалий, которые являются признаками атаки (например, событие NDR при обнаружении признаков ARP-спуфинга). Соответствует названию события в трафике сети, на основании которого создан алерт.

Информация в блоке Правило IDS

В блоке **Правило IDS** отображается информация об алерте, созданном технологией IDS (Intrusion Detection System), в формате матрицы HEX-редактора.

HEX-редактор (англ. hex-editor), шестнадцатеричный редактор — приложение для редактирования данных, в котором данные представлены как последовательность байтов.

В верхней части матрицы отображается длина правила IDS.

В левой части матрицы отображаются данные правила в текстовом формате.

В разделе **Содержание правила** блока **Правило IDS** отображается заголовок правила IDS и данные IDS-алерта в формате Suricata. Например, могут отображаться данные о направлении трафика (`flow`), метод HTTP-запроса (`http_method`), HTTP-заголовок (`http_header`), идентификатор безопасности (`sid`).

Информация в блоке URL

В блоке **URL** отображается URL-адрес, по которому сработало обнаружение.

По ссылке **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP по URL**.
- **Найти на Kaspersky TIP по имени домена**.
- **Скопировать значение в буфер**.

Информация в блоке IP устройств, связанных с обнаружением

В блоке **IP устройств, связанных с обнаружением** отображаются сведения об устройствах, связанных с алертом:

- **Протокол**.
- **IP источника**.
- **MAC источника**.
- **IP назначения**.
- **MAC назначения**.

Информация в блоке Сетевое событие

В блоке **Сетевое событие** может отображаться следующая информация о ссылке на веб-сайт, открытой на компьютере пользователя:

- **Дата** и **Время** – дата и время сетевого события.
- **Метод** – тип HTTP-запроса, например, GET или POST.
- **IP источника** – IP-адрес компьютера, на котором была открыта ссылка на веб-сайт.
- **IP назначения** – IP-адрес компьютера, с которого была открыта ссылка на веб-сайт.
- **URL** – тип HTTP-запроса, например, GET или POST, URL-адрес веб-сайта.

Если алерт создан для файла, извлеченного из трафика, в URL-адресе указывается протокол, использованный для передачи трафика, из которого файл был извлечен. Возможные протоколы: HTTP, HTTPS, FTP, SMTP, POP3, SMB, NFS.

По ссылке с URL-адресом раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky TIP по URL**.
- **Найти на Kaspersky TIP по имени домена**.
- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

- **Агент пользователя** – информация о браузере, с помощью которого был загружен файл или была предпринята попытка загрузки файла, или была открыта ссылка на веб-сайт. Текстовая строка в составе HTTP-запроса, обычно содержащая название и версию браузера, а также название и версию операционной системы, установленной на компьютере пользователя.

Результаты проверки в Sandbox

Результаты исследования поведения файла отображаются, только если для этого файла было выполнено обнаружение компонентом Sandbox. Если файл был загружен в систему и затем проверен в Sandbox, но компонент при этом не обнаружил угрозу, результаты исследования не отображаются.

В окне результатов проверки объекта в Sandbox могут отображаться следующие сведения:

- **Файл** – полное имя и путь проверенного файла.
- **Размер файла** – размер файла.
- **MD5** – MD5-хеш файла.
- По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:
  - **Найти на Kaspersky TIP.**
  - **Найти события.**
  - **Найти алерты.**
  - **Создать правило запрета.**
  - **Скопировать значение в буфер.**
- **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если приложение обнаружило файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого обнаружения.

- **Время обработки** – время выполнения проверки файла.
- **Версии баз** – версии баз модулей и компонентов Kaspersky Anti Targeted Attack Platform, создавших алерт.

Кнопка **Новое правило запрета** в правом верхнем углу окна позволяет запретить запуск файла.

Информация о результатах исследования поведения файла приводится для каждой операционной системы, в которой компонент Sandbox выполнил проверку. Для операционной системы Windows 7 (64-разрядная) вы можете просмотреть журналы активности файла для двух режимов проверки компонента Sandbox – **Режим быстрой проверки** и **Режим ведения полного журнала**.

Для каждого режима проверки могут быть доступны следующие журналы активности:

- **Список активностей** – действия файла внутри операционной системы.
- **Дерево активностей** – графическое представление процесса исследования файла.
- **Журнал HTTP-активности** – журнал HTTP-активности файла. Содержит следующую информацию:
  - **IP назначения** – IP-адрес, на который файл пытается перейти из операционной системы.
  - **Метод** – метод HTTP-запроса, например, GET или POST.
  - **URL** – URL-адрес ссылки на веб-сайт, которую файл пытается открыть из операционной системы.

  По ссылкам в столбце **IP назначения** раскрывается список, в котором вы можете выбрать одно из следующих действий:
  - **Найти на Kaspersky TIP**.
  - **Найти события**.
  - **Найти алерты**.
  - **Скопировать значение в буфер**.

  По ссылкам в столбце **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:
  - **Найти на Kaspersky TIP по URL**.
  - **Найти на Kaspersky TIP по имени домена**.
  - **Найти события**.
  - **Найти алерты**.
  - **Скопировать значение в буфер**.
- **Журнал действий IDS** – журнал сетевой активности файла. Содержит следующую информацию:
  - **IP источника** – IP-адрес хоста, на котором хранится файл.
  - **IP назначения** – IP-адрес, на который файл пытается перейти из операционной системы.

- **Метод** – метод HTTP-запроса, например, GET или POST.
- **URL** – URL-адрес ссылки на веб-сайт, которую файл пытается открыть из операционной системы.

По ссылкам в столбце **IP назначения** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky TIP**.
- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

По ссылкам в столбце **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky TIP по URL**.
- **Найти на Kaspersky TIP по имени домена**.
- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

- **Журнал DNS-активности** – журнал DNS-активности файла. Содержит следующую информацию:
  - Тип запроса (Request или Response).
  - **DNS-имя** – доменное имя сервера.
  - **Тип** – тип DNS-запроса (например, A или CNAME).
  - **Хост** – имя хоста или IP-адрес, с которым осуществлялось взаимодействие.

  По ссылкам в столбцах **DNS-имя** и **Хост** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на Kaspersky TIP**.
  - **Найти события**.
  - **Найти алерты**.
  - **Скопировать значение в буфер**.

- **Снимки экрана** – содержит снимки экрана, сделанные во время выполнения файла.

  Вы можете просмотреть снимки экрана в веб-интерфейсе приложения или скачать архив в формате Zip, содержащий эти снимки экрана.

Кнопка **Скачать полный журнал** в нижней части каждого из режимов проверки **Режим быстрой проверки** и **Режим ведения полного журнала** позволяет скачать журнал исследования поведения файла в каждой операционной системе на компьютер.

Результаты IOC-проверки

В зависимости от типа обработанного объекта, в окне результатов поиска индикаторов компрометации могут отображаться следующие данные:

- **ARP-протокол**:
  - IP-адрес из ARP-таблицы.
  - Физический адрес из ARP-таблицы.
- **DNS-запись**:
  - Тип и имя записи DNS.
  - IP-адрес защищаемого компьютера.
- **Событие в журнале Windows**:
  - Идентификатор записи в журнале событий.
  - Имя источника данных в журнале.
  - Имя журнала.
  - Учетная запись пользователя.
  - Время события.
- **Файл**:
  - MD5-хеш файла.
  - SHA256-хеш файла.
  - Полное имя файла (включая путь).
  - Размер файла.
- **Порт**:
  - Удаленный IP-адрес, с которым было установлено соединение в момент проверки.
  - Удаленный порт, с которым было установлено соединение в момент проверки.
  - IP-адрес локального адаптера.
  - Порт, открытый на локальном адаптере.
  - Протокол в виде числа (в соответствии со стандартом IANA).

- **Процесс**:
  - Имя процесса.
  - Аргументы процесса.
  - Путь к файлу процесса.
  - Windows идентификатор (PID) процесса.
  - Windows идентификатор (PID) родительского процесса.
  - Имя учетной записи пользователя, запустившего процесс.
  - Дата и время запуска процесса.
- **Служба**:
  - Имя службы.
  - Описание службы.
  - Путь и имя DLL-службы (для svchost).
  - Путь и имя исполняемого файла службы.
  - Windows идентификатор (PID) службы.
  - Тип службы (например, драйвер ядра или адаптер).
  - Статус службы.
  - Режим запуска службы.
- **Пользователь**:
  - Имя учетной записи пользователя.
- **Том**:
  - Наименование тома.
  - Буква тома.
  - Тип тома.
- **Реестр**:
  - Значение реестра Windows.
  - Значение куста реестра.
  - Путь к ключу реестра (без куста и без имени значения).
  - Параметр реестра.

- **Переменные окружения**:
  - Физический адрес (MAC) защищаемого компьютера.
  - Система (окружение).
  - Имя ОС с версией.
  - Сетевое имя защищаемого устройства.
  - Домен или группа, к которой принадлежит защищаемый компьютер.

В разделе **IOC** отображается структура IOC-файла. При совпадении обработанного объекта с одним из условий IOC-правила, это условие подсвечивается. Если обработанный объект совпадает с несколькими условиями, выделяется текст всей ветки.

Информация в блоке Хосты

В блоке **Хосты** отображается следующая информация о хостах, на которых сработало правило TAA (IOA):

- **Имя хоста** – IP-адрес или доменное имя компьютера, на котором произошло событие. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим ID выбранного правила и выбранный хост.
- **IP** – IP-адрес компьютера, на котором произошло событие.

  Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный компьютеру на момент создания или обновления обнаружения.

  Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес компьютера не отображается.
- **Количество событий** – количество событий, произошедших на хосте.
- **Найти события**. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим ID выбранного правила.

Информация в блоке Журнал изменений

В блоке **Журнал изменений** может отображаться следующая информация об обнаружении:

- Дата и время изменения алерта.
- Автор изменений.

  Например, **Система** или имя пользователя приложения.

- Изменение, произошедшее с алертом.

  Например, алерту может быть присвоена принадлежность группе VIP, или он может быть отмечен как обработанный.

Отправка данных об алерте

Вы можете предоставить в "Лабораторию Касперского" информацию об алерте (кроме технологий URL Reputation и IOC) для дальнейшего исследования.

Для этого необходимо скопировать детали алерта в буфер обмена, а затем отправить их в "Лабораторию Касперского" по электронной почте.

Детали алерта могут содержать данные о вашей организации, которые вы считаете конфиденциальными. Вам необходимо самостоятельно согласовать отправку этих данных для дальнейшего исследования в "Лабораторию Касперского" со Службой безопасности вашей организации.

Чтобы скопировать детали алерта в буфер обмена:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Левой клавишей мыши нажмите на строку с тем алертом, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об алерте.

3. Нажмите на ссылку **Предоставить данные об алерте в "Лабораторию Касперского"** в нижней части окна с информацией об алерте.

   Откроется окно **Подробнее**.

4. Просмотрите данные алерта для отправки в "Лабораторию Касперского".

5. Если вы хотите скопировать эти данные, нажмите на кнопку **Скопировать в буфер**.

   Данные алерта будут скопированы в буфер обмена. Вы сможете отправить их в "Лабораторию Касперского" для дальнейшего исследования.

Просмотр связей алерта

Из карточки алерта вы можете перейти к таблице событий, активов или сетевых сессий, связанных с этим алертом.

Чтобы просмотреть связи алерта:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Откройте алерт, связи которого вы хотите просмотреть.

3. В карточке алерта нажмите на стрелку рядом с кнопкой **Показать связи**.

4. Выберите из списка нужную связь для алерта:

   - **События**.
   - **Активы**.
   - **Сетевые сессии**.

Откроется соответствующий раздел веб-интерфейса с таблицей связей.

Действия пользователей с алертами

При работе в веб-интерфейсе приложения под учетной записью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** вы можете выполнять следующие действия с алертами:

- Назначать алерты себе или другому пользователю веб-интерфейса приложения.

  Вы можете просмотреть все алерты, назначенные определенному пользователю, используя фильтр алертов по состоянию их обработки пользователем.

- Отметить алерт как обработанный.

  Вы можете просмотреть все алерты, обработанные определенным пользователем, используя фильтр алертов по состоянию их обработки пользователем.

- Добавить комментарий к алерту.

  Вы можете найти алерты, содержащие комментарий, по ключевым словам комментария, используя фильтр алертов по полученной информации.

- Присвоить алерту статус VIP.

  Это действие доступно только пользователям с ролью **Старший сотрудник службы безопасности**. Пользователи с этой ролью могут просмотреть все алерты со статусом VIP, используя фильтр алертов по наличию статуса VIP.

Пользователи с ролью **Аудитор** могут просматривать информацию об алертах без возможности редактирования.

Назначение алертов определенному пользователю

Пользователи с ролью **Старший сотрудник службы безопасности** могут назначить алерт или несколько алертов себе или другому пользователю веб-интерфейса приложения с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности**.

Чтобы назначить алерт себе или другому пользователю веб-интерфейса приложения:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Установите флажок напротив алерта или алертов, которые вы хотите назначить себе или другому пользователю.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все алерты.

3. В появившейся панели в нижней части окна раскройте список пользователей, нажав на стрелку справа от кнопки **Назначить**.

4. Выберите пользователя, которому вы хотите назначить алерты.

   Откроется окно подтверждения действия. Вы также можете оставить комментарий, который отобразится в истории изменения алерта.

5. Нажмите на кнопку **Продолжить**.

Алерты будут назначены выбранному пользователю.

Вы можете просмотреть все алерты, назначенные определенному пользователю, используя фильтр алертов по состоянию их обработки пользователем.

Пользователи с ролью **Аудитор** не могут назначать алерты себе или другим пользователям веб-интерфейса приложения. Пользователи с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** также не могут назначать алерты пользователям с ролью **Аудитор**.

Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** в процессе работы с алертом могут назначить этот алерт себе или другому пользователю веб-интерфейса приложения с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности**.

Чтобы назначить алерт себе или другому пользователю в процессе работы с этим алертом:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Откройте алерт, который вы хотите назначить себе или другому пользователю приложения.

   Откроется карточка алерта.

3. Если вы хотите назначить алерт себе, нажмите на кнопку **Назначить @Мне**.

4. Если вы хотите назначить алерт другому пользователю приложения, нажмите на стрелку справа от кнопки **Назначить** и выберите пользователя, которому вы хотите назначить алерт.

Алерт будет назначен выбранному пользователю.

Отметка о завершении обработки одного алерта

Для пользователей с ролью **Аудитор** недоступны функции назначения и обработки алертов.

Чтобы закрыть один алерт в таблице алертов:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. В столбце **Состояние** того алерта, который вы хотите закрыть, нажмите на состояние алерта.
3. В списке действий выберите **Закрыть алерт**.

Алерт будет закрыт.

Чтобы закрыть алерт в процессе работы с этим алертом:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.
2. Откройте алерт, который вы хотите закрыть.
3. В правом верхнем углу окна нажмите на кнопку **Закрыть алерт**.

Алерт будет закрыт. Если алерт был назначен другому пользователю, он будет отмечен как обработанный вами.

Вы можете просмотреть все алерты, обработанные определенным пользователем, используя фильтр алертов по состоянию их обработки пользователем или переключатель **Показывать закрытые алерты**.

Если в течение суток (с 00:00 до 23:59) в результате проверки по технологиям TAA (IOA), IDS, URL создается алерт, аналогичный обработанному, приложение либо создаст новый алерт, либо обновит информацию в идентичном алерте со статусом **Новое** или **В обработке**.

При закрытии алерта функциональности NDR связанные с ним агрегирующее событие и вложенные события NDR отмечаются как обработанные, а также закрываются связанные с этими событиями другие алерты. Если закрытый алерт функциональности NDR открывается вновь, связанное с ним закрытое событие NDR не открывается.

Отметка о завершении обработки алертов

Для пользователей с ролью **Сотрудник службы безопасности** недоступны массовые операции с алертами. Для пользователей с ролью **Аудитор** недоступны функции назначения и обработки алертов.

Чтобы закрыть один или несколько алертов:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.
2. Установите флажки напротив тех алертов, которые вы хотите закрыть.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все алерты.
3. В появившейся панели в нижней части окна нажмите на кнопку **Закрыть алерт**.

   Откроется окно подтверждения действия.

Вы также можете оставить комментарий, который отобразится в истории изменения алерта.

4. Нажмите на кнопку **Продолжить**.

Выбранные алерты будут закрыты. Если алерты были назначены другим пользователям, они будут отмечены как закрытые вами.

Вы можете просмотреть все закрытые алерты, используя фильтр алертов по состоянию их обработки пользователем или переключатель **Показывать закрытые алерты**.

Если в течение суток (с 00:00 до 23:59) в результате проверки по технологиям TAA (IOA), IDS, URL создается алерт, аналогичный обработанному, приложение либо создаст новый алерт, либо обновит информацию в идентичном алерте со статусом **Новое** или **В обработке**.

При закрытии алерта функциональности NDR связанные с ним агрегирующее событие и вложенные события NDR отмечаются как обработанные, а также закрываются связанные с этими событиями другие алерты. Если закрытый алерт функциональности NDR открывается вновь, связанное с ним закрытое событие NDR не открывается.

Изменение статуса VIP алертов

Пользователи с ролью **Старший сотрудник службы безопасности** могут присваивать алертам статус VIP и лишать алерты статуса VIP.

Чтобы изменить статус VIP для алертов:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Установите флажки напротив алертов, для которых вы хотите изменить статус VIP.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все алерты.

3. Выполните одно из следующих действий:

   - Если вы хотите присвоить алертам статус VIP, в появившейся панели в нижней части окна нажмите на кнопку **Присвоить статус VIP**.
   - Если вы хотите лишить алерты статуса VIP, в появившейся панели в нижней части окна в раскрывающемся списке **Присвоить статус VIP** выберите **Лишить статуса VIP**.

   Откроется окно подтверждения действия.

   Вы также можете оставить комментарий, который отобразится в истории изменения алерта.

4. Нажмите на кнопку **Продолжить**.

Статус VIP для алертов будет изменен.

Пользователи с ролью **Старший сотрудник службы безопасности** и **Аудитор** могут просмотреть все алерты со статусом VIP, используя фильтр алертов по наличию статуса VIP.

Добавление комментария к алерту

Пользователи с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут добавить комментарий к алерту.

Чтобы добавить комментарий к алерту:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. Выберите алерт, к которому вы хотите добавить комментарий.

   Откроется окно с информацией об алерте.

3. В поле добавления комментария под блоком **Журнал изменений** введите комментарий к алерту.

4. Нажмите на кнопку **Добавить**.

Комментарий к алерту будет добавлен и отобразится в блоке **Журнал изменений** этого алерта.

Вы можете найти алерты, содержащие комментарий, по ключевым словам комментария, используя фильтр алертов по полученной информации.

Пользователи с ролью **Аудитор** могут просматривать комментарии к алертам без возможности редактирования.

Мониторинг событий в трафике сети

При анализе трафика сети приложение регистрирует события. Анализ трафика сети является частью функциональности NDR.

*Событие в трафике сети (*далее также *событие NDR)* – это запись, содержащая информацию об обнаружении в трафике сети определенных изменений или условий, которые требуют внимания специалиста по безопасности. События NDR регистрируются и передаются на сервер Central Node. Сервер обрабатывает полученные события и сохраняет их в базе данных.

Агрегирующее событие – это событие особого типа, которое регистрируется при получении определенной последовательности событий NDR. Агрегирующие события группируют события NDR, имеющие некоторые общие признаки или относящиеся к одному процессу.

Приложение регистрирует агрегирующие события по правилам корреляции событий. *Правило корреляции событий* описывает условия для проверки последовательностей событий. При обнаружении последовательности событий NDR, удовлетворяющих условиям правила, приложение регистрирует агрегирующее событие, в котором указано название сработавшего правила. Для регистрации агрегирующих событий используется системный тип события, которому присвоен код 8000000001.

Правила корреляции событий встроены в приложение и применяются независимо от политики безопасности.

После установки приложения используются исходные правила корреляции событий. Для повышения эффективности работы правил специалисты "Лаборатории Касперского" регулярно обновляют базы с наборами правил. Вы можете обновлять правила корреляции, устанавливая обновления.

Сервер Kaspersky Anti Targeted Attack Platform регистрирует события NDR в соответствии с параметрами, заданными для регистрации типов событий. Вы можете настроить эти параметры в разделе Настройка типов событий.

Для сокращения количества часто повторяющихся событий NDR, которые не требуют внимания пользователя, предусмотрена возможность создания разрешающих правил на события. События NDR, удовлетворяющие разрешающим правилам, не регистрируются. Например, с помощью разрешающего правила можно временно выключить регистрацию всех событий с определенной точки мониторинга. Вы можете просматривать разрешающие правила для событий в разделе **Параметры**, подразделе **Разрешающие правила**. Для таких правил указан тип EVT.

Приложение сохраняет события NDR и агрегирующие события в базе данных на Central Node. Суммарный объем сохраняемых записей не может превышать заданного ограничения. Если объем превышает заданное ограничение, приложение автоматически удаляет самые старые записи. При этом если включено ограничение на минимальное время хранения, при удалении записей, время хранения которых меньше заданного ограничения, в журнале сообщений приложения появляется соответствующее сообщение. Вы можете настроить параметры хранения событий и инцидентов.

Вы можете просматривать информацию о событиях NDR и агрегирующих событиях в разделе **События в трафике сети**. В разделе отображается подробная информация о событиях NDR и агрегирующих событиях и предоставляется возможность загрузки информации из базы данных сервера за любой период.

Действия с событиями в трафике сети доступны пользователям с ролью **Сотрудник службы безопасности** или **Старший сотрудник службы безопасности**. Пользователи с ролью **Аудитор** могут просматривать события.

События NDR создаются при наличии действующего лицензионного ключа KATA+NDR. После истечения срока действия лицензионного ключа созданные события остаются доступны для просмотра, связанные алерты не создаются.

Оценки и уровни критичности событий NDR

События NDR в Kaspersky Anti Targeted Attack Platform оцениваются по шкале от 0.0 до 10.0.

Если событие NDR связано с устройством, приложение рассчитывает оценку с учетом имеющихся сведений об устройстве. Учитывается уровень значимости устройства и риски, связанные с этим устройством.

В качестве исходного значения для расчета оценки используется *базовая оценка*, заданная для типа события NDR в таблице типов событий.

Если событие NDR не связано с устройством, значение оценки этого события равно значению базовой оценки.

Оценка определяет уровень критичности события NDR. В зависимости от числового значения оценки событие NDR может относиться к одному из следующих уровней критичности:

- *Низкий* (оценки 0.0–3.9).

  События NDR низкого уровня критичности обычно не требуют немедленной реакции.

- *Средний* (оценки 4.0–7.9).

  События NDR среднего уровня критичности содержат сведения, на которые нужно обратить внимание. Эти события могут требовать реакции.

- *Высокий* (оценки 8.0–10.0).

  События NDR высокого уровня критичности содержат сведения, которые могут оказать критическое влияние. Эти события требуют немедленной реакции.

Технологии регистрации событий NDR

Kaspersky Anti Targeted Attack Platform регистрирует события NDR по одной из следующих технологий:

- *Обнаружение вторжений* (IDS).

  По этой технологии регистрируются события NDR, связанные с обнаружением в трафике аномалий, которые являются признаками атак (например, событие NDR при обнаружении признаков ARP-спуфинга).

- *Внешние системы* (EXT).

  К этой технологии относятся агрегирующие и вложенные события NDR, которые поступают в Kaspersky Anti Targeted Attack Platform от сторонних систем с использованием методов API NDR.

- *Контроль активов* (AM).

  По этой технологии регистрируются события NDR, связанные с обнаружением информации об устройствах в трафике или в полученных данных от EPP-приложений (например, событие NDR при обнаружении нового IP-адреса у устройства).

- *Защита конечных устройств* (EPP).

  По этой технологии регистрируются события NDR об угрозах, обнаруженных приложениями "Лаборатории Касперского", которые выполняют функции защиты рабочих станций и серверов (например, событие при обнаружении вредоносной программы).

Статусы событий NDR

Статусы событий NDR позволяют отобразить в приложении последовательность обработки полученной информации сотрудниками службы безопасности.

Событиям NDR и агрегирующим событиям могут быть присвоены следующие статусы:

- *Новое*.

  Этот статус присваивается всем событиям NDR и агрегирующим событиям при их регистрации в Kaspersky Anti Targeted Attack Platform.

- *В обработке*.

  Этот статус вы можете присвоить событиям NDR и агрегирующим событиям, которые находятся в обработке (например, во время расследования причин регистрации этих событий и инцидентов).

- *Обработано*.

  Этот статус вы можете присвоить событиям NDR и агрегирующим событиям, которые уже обработаны (например, завершено расследование причин их регистрации).

  > После присвоения статуса *Обработано* приложение не учитывает события NDR и агрегирующие события с этим статусом при определении состояния безопасности устройств, отображаемых в таблице устройств и на карте сетевых взаимодействий.

Изменение статусов событий NDR и агрегирующих событий выполняется вручную. Вы можете последовательно присваивать статусы в порядке от статуса *Новое* до статуса *Обработано*. При этом можно не присваивать промежуточный статус *В обработке*. После изменения статуса события NDR и агрегирующего события ему невозможно присвоить предыдущий статус.

Если статус *Обработано* присвоен агрегирующему событию, все вложенные события NDR автоматически меняют статус на *Обработано*, а также закрываются связанные алерты.

Если статус *Обработано* присвоен событию NDR, агрегирующие события, в которые вложено это событие NDR, и связанные алерты не закрываются.

Таблица зарегистрированных событий NDR

Вы можете просмотреть таблицу зарегистрированных событий NDR и агрегирующих событий в разделе **События в трафике сети**.

По умолчанию таблица зарегистрированных событий NDR и агрегирующих событий обновляется в онлайн-режиме. В начале таблицы отображаются события с наиболее поздними значениями даты и времени последнего появления.

> Дата и время последнего появления события NDR или агрегирующего события может не совпадать с датой и временем его регистрации. Для события NDR дата и время последнего появления может обновляться в течение времени разрешения повтора для типа этого события. Для агрегирующего события дата и время последнего появления обновляется в соответствии с датой и временем последнего появления вложенных событий NDR.

Параметры событий NDR и агрегирующих событий отображаются в следующих столбцах таблицы:

- **Начало**.

  Для события NDR – дата и время регистрации события. Для агрегирующего события – дата и время регистрации первого вложенного события. Вы можете просматривать в таблице дату совместно со временем либо только дату или только время. Для выбора отображаемой информации нужно установить флажки напротив параметров **Дата** и **Время**.

- **Последнее появление**.

  Для события NDR – дата и время последнего появления события NDR. Может содержать дату и время регистрации события или дату и время увеличения счетчика повторов события, если повторились условия для регистрации события в течение времени разрешения повтора. Значение счетчика повторов отображается в столбце **Всего появлений**. Для агрегирующего события – самые поздние дата и время последнего появления событий, входящих в агрегирующее событие. Аналогично столбцу **Начало**, вы можете просматривать в таблице дату совместно со временем либо только дату или только время.

- **Заголовок**.

  Заголовок, заданный для типа события NDR.

- **Оценка**.

  Рассчитанное значение оценки для события NDR. Числовое значение определяет, к какому уровню критичности относится событие NDR. В зависимости от уровня критичности, значение оценки может быть окрашено одним из следующих цветов:

  - Красный – событие с уровнем критичности *Высокий*.
  - Желтый – событие с уровнем критичности *Средний*.
  - Синий – событие с уровнем критичности *Низкий*.

- **Отправитель**.

  Адрес отправителя сетевых пакетов. Отображение адресов и портов адресной информации можно включать и выключать с помощью следующих параметров (в скобках указаны сокращенные названия для отображения в ячейках таблицы): **IP-адрес**, **Номер порта (P)**, **MAC-адрес**, **VLAN ID (VID)**, **Адрес прикладного уровня**. Если в приложение добавлены дополнительные адресные пространства, при настройке таблицы устройств можно включать и выключать отображение имен адресных пространств с помощью параметра **Отображать адресные пространства**.

- **Получатель**.

  Адрес получателя сетевых пакетов. Отображение адресной информации можно настраивать аналогично, как для столбца **Отправитель**.

- **Протокол**.

  Протокол прикладного уровня, при отслеживании которого приложение зарегистрировало событие.

- **Технология**.

  Значок, соответствующий технологии, которая использовалась для регистрации события NDR.

- **Всего появлений**.

  Для события NDR – значение счетчика повторов после регистрации события NDR в течение времени разрешения повтора события. Значение больше 1 означает, что условия для регистрации события NDR повторялись N – 1 раз. Для агрегирующего события в этом столбце отображается значение 1.

- **ID**.

  Уникальный идентификатор зарегистрированного события NDR или агрегирующего события.

- **Приложение**.

  Сведения о приложениях, при работе которых возникли условия для регистрации события NDR. В событии NDR сохраняются данные о приложениях, полученные от EPP-приложений.

- **Пользователь приложения**.

  Сведения о пользователе, от имени которого выполнен запуск приложения, указанного в столбце **Приложение**.

- **Статус**.

  Значок, соответствующий статусу события NDR или агрегирующего события.

- **Описание**.

  Описание, заданное для типа события NDR.

- **Завершение**.

  Для события NDR – дата и время присвоения статуса *Обработано* или дата и время разрешения повтора события NDR. Для агрегирующего события – самые поздние дата и время завершения вложенных событий NDR. Аналогично столбцу **Начало**, вы можете просматривать в таблице дату совместно со временем либо только дату или только время.

- **Сработавшее правило**.

  Для события NDR – имя правила контроля процесса или правила обнаружения вторжений, при срабатывании которого зарегистрировано событие NDR. Для агрегирующего события – имя правила корреляции, при срабатывании которого зарегистрировано агрегирующее событие.

- **Точка мониторинга**.

  Точка мониторинга, трафик с которой вызвал регистрацию события NDR.

- **Тип события**.

  Числовой код, присвоенный типу события NDR.

- **Метка**.

  Набор значков, которые вы можете установить для любого события NDR или агрегирующего события, чтобы легко находить события NDR или агрегирующие события по критерию, отсутствующему в таблице.

При просмотре таблицы событий в трафике сети вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Настройка таблицы зарегистрированных событий

Вы можете настраивать следующие параметры отображения таблицы событий:

- отображение информационной панели;
- отображение событий, включенных в инциденты;
- состав и порядок граф, отображаемых в таблице.

Чтобы настроить параметры отображения таблицы событий:

1. В разделе **События в трафике сети** нажмите на значок .

   Откроется окно для настройки отображения таблицы.

2. Если вы хотите включить отображение информационной панели, показывающей количество событий со статусами *Новое* и *В обработке*, установите флажок **Отображать информационную панель**.

3. В блоке параметров **Отображение вложенных списков** выберите нужный режим отображения событий NDR, вложенных в агрегирующие события:

   - **Простой вид**. В этом режиме в таблице событий отображаются все события NDR без учета вложенности событий.

   - **Структурное представление**. В этом режиме агрегирующие события отображаются в виде дерева вложенных событий и других агрегирующих событий. Если вы хотите, чтобы вложенные элементы отображались независимо от текущих параметров фильтрации и поиска, установите флажок **Показывать вложенные при фильтрации**.

4. В блоке параметров **Отображаемые столбцы** установите флажки напротив тех параметров, которые вы хотите просматривать в таблице. Необходимо выбрать хотя бы один параметр.

5. Если вы хотите изменить порядок отображения столбцов, выделите название столбца, которую вы хотите разместить левее или правее в таблице, и используйте кнопки с изображением стрелок вверх и вниз.

   Для столбцов **Начало**, **Последнее появление** и **Завершение** вы также можете изменить порядок отображения даты и времени, а для столбцов **Отправитель** и **Получатель** – адресов отправителей и получателей сетевых пакетов. Для этого выделите значение, которое вы хотите разместить левее или правее в таблице, и используйте кнопки с изображением стрелок вверх и вниз.

Выбранные столбцы отобразятся в указанном вами порядке в таблице в разделе **События в трафике сети**.

Просмотр событий, вложенных в агрегирующее событие

Для просмотра событий NDR, вложенных в агрегирующие события, в таблице событий трафика в сети предусмотрены следующие режимы:

- Простой режим отображения. В этом режиме в таблице событий NDR отображаются все события без учета вложенности событий.

- Режим отображения структур. В этом режиме агрегирующие события отображаются в виде структур, которые могут быть свернуты и развернуты с помощью кнопок ⊞ и ⊟ рядом с заголовками агрегирующих событий.

Вы можете изменить режим отображения при настройке таблицы событий.

Просмотр подробных данных о событии NDR

Подробные сведения о событиях NDR и агрегирующих событиях отображаются в области деталей в разделе **События в трафике сети** веб-интерфейса приложения.

Чтобы просмотреть подробные данные о событии NDR или агрегирующем событии,

в разделе **События в трафике сети** выберите нужное событие.

В правой части окна веб-интерфейса появится область деталей, в которой отобразятся подробные сведения о выбранном событии NDR или агрегирующем событии.

Изменение статусов событий NDR

Вы можете изменять следующие статусы событий NDR и агрегирующих событий:

- *Новое*. Этот статус можно изменить на статус *В обработке* или на статус *Обработано*;
- *В обработке*. Этот статус можно изменить на статус *Обработано*.

Статус *Обработано* изменить невозможно.

Если событие NDR связано с риском, вы можете присвоить этому событию статус *Обработано* одновременно с изменением статуса риска на статус *Принят*.

Чтобы изменить статус событий NDR и агрегирующих событий при работе с таблицей событий:

1. В разделе **События в трафике сети** в таблице событий выберите события NDR или агрегирующие события, статус которых вы хотите изменить.
2. Откройте раскрывающийся список **Изменить статус** в панели инструментов.
3. В раскрывающемся списке выберите пункт для присвоения нужного статуса.

   Некоторые пункты раскрывающегося списка недоступны в следующих случаях:

   - Пункт **В обработке** недоступен, если среди выбранных элементов отсутствуют события NDR или агрегирующие события со статусом *Новое*.
   - Пункт **Обработано** недоступен, если среди выбранных элементов отсутствуют события NDR или агрегирующие события со статусами *Новое* или *В обработке*.

   > Если выбраны все события NDR или агрегирующие события, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных элементов более 1000, приложение не проверяет их статусы. В этом случае доступны оба пункта с названиями статусов **В обработке** и **Обработано**. При этом с помощью пункта **В обработке** вы можете присвоить статус *В обработке* только событиям и инцидентам со статусом *Новое*.

   Откроется окно с запросом подтверждения.
4. Если с выбранными событиями NDR связаны риски и вы хотите одновременно присвоить статус *Принят* всем этим рискам, установите флажок **Присвоить статус Принят для всех рисков, связанных с событием** (если выбрано одно событие) или **Присвоить статус Принят для всех рисков, связанных с событиями** (если выбрано несколько событий).

   Риски могут быть связаны с событиями при регистрации событий NDR некоторых типов по технологии Контроль активов.
5. В окне запроса нажмите на кнопку **ОК**.

Установка меток

Пользователи с ролью **Старший сотрудник службы безопасности** могут присваивать событиям NDR и агрегирующим событиям определенные метки в разделе **События в трафике сети** веб-интерфейса приложения.

Метка – значок, который позволяет легко находить события NDR и агрегирующие события по критерию, отсутствующему в таблице.

Чтобы установить метку для события NDR или агрегирующие события:

1. В разделе **События в трафике сети** для строки с нужным событием NDR или агрегирующим событием в столбце ☆ нажмите на левую кнопку мыши.

2. В открывшемся меню выберите метку, которую вы хотите установить для этого события NDR или агрегирующего события.

   Вы можете выбрать одну из семи меток, предусмотренных в приложении. Назначение каждой метки вы выбираете самостоятельно.

3. Если вам потребуется снять метку, выберите в меню пункт **Без метки**.

Пользователи с ролью **Старший сотрудник службы безопасности** и **Аудитор** могут просматривать события NDR или агрегирующие события с меткой.

Копирование событий NDR в текстовый редактор

Вы можете скопировать информацию о событиях NDR и агрегирующих событиях, отображаемых в таблице событий в трафике сети, в любой текстовый редактор. Информация копируется из столбцов, отображаемых в таблице в текущий момент.

Возможность копирования доступна, если выбрано не более 200 событий NDR и агрегирующих событий.

Чтобы скопировать события NDR и агрегирующие события в текстовый редактор:

1. В разделе **События в трафике сети** выберите события NDR и агрегирующие события, информацию о которых вы хотите скопировать в текстовый редактор.

2. По правой кнопке мыши откройте контекстное меню одного из выбранных событий.

3. В контекстном меню выберите один из следующих пунктов:

   - **Копировать детали события**, если выбрано одно событие NDR или агрегирующее событие.

   - **Копировать детали выбранных событий**, если выбрано несколько событий NDR или агрегирующих событий.

4. Откройте любой текстовый редактор.

5. В окне текстового редактора выполните вставку (например, с помощью комбинации клавиш **CTRL+V**).

Скопированная информация о событии будет доступна для изменения в текстовом редакторе. Информация о нескольких событиях будет разделена пустой строкой.

Загрузка трафика для событий

При просмотре таблицы событий вы можете загружать трафик, относящийся к зарегистрированным событиям NDR и агрегирующим событиям. Загрузка трафика выполняется в файл формата PCAP (при выборе одного события) или в архив формата ZIP, содержащий файлы формата PCAP (при выборе нескольких событий).

Возможность загрузки трафика доступна, если в таблице событий выбрано не более 200 событий (в том числе в составе агрегирующих событий).

Трафик для событий загружается из базы данных приложения. В базе данных трафик может сохраняться при регистрации событий NDR, для которых включено сохранение трафика. Также приложение может сохранять трафик в базе данных непосредственно при запросе на загрузку трафика, используя файлы дампа трафика. Эти файлы предназначены для временного хранения и автоматически удаляются по мере поступления трафика (периодичность удаления файлов зависит от интенсивности поступающего трафика и от заданных параметров хранения данных приложения). Для гарантированной загрузки трафика рекомендуется включить сохранение трафика для нужных типов событий и настроить параметры хранения трафика в базе данных в соответствии с интенсивностью его поступления и регистрации событий.

Чтобы загрузить файл трафика для событий NDR или агрегирующих событий:

1. В разделе **События в трафике сети** выберите события NDR и агрегирующие события, для которых вы хотите загрузить трафик.

2. Нажмите на кнопку **Скачать трафик**.

3. Если формирование файла занимает длительное время (более 15 секунд), операция по формированию файла переводится в список фоновых операций. В этом случае для загрузки файла выполните следующие действия:

   a. Нажмите на кнопку в меню веб-интерфейса приложения.

      Откроется список фоновых операций.

   b. Дождитесь завершения операции формирования файла.

   c. Нажмите на кнопку **Скачать файл**.

Браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Создание директории для экспорта событий на сетевой ресурс

Вы можете экспортировать события и сохранять файл с экспортированными событиями на сетевом ресурсе компьютера Сервера. Для работы сетевого ресурса вы можете использовать протокол Network File System (NFS), с помощью которого выполняется монтирование общего сетевого ресурса другого компьютера (например, точки экспорта сервера NFS) в локальной файловой системе компьютера Сервера. Создание директории и монтирование общего сетевого ресурса выполняется с помощью стандартных средств операционной системы.

При использовании протокола NFS в операционной системе активируется программный пакет rpcbind. Следует учитывать, что злоумышленники могут попытаться использовать этот программный пакет для проведения некоторых типов DDoS-атак. Для устранения угрозы проникновения требуется выполнить настройку сетевого экрана. В операционной системе CentOS Stream рекомендуется использовать программу настройки сетевой защиты firewalld.

Создание директории и монтирование общего сетевого ресурса вручную

Чтобы создать директорию для сохранения файлов на сетевой ресурс:

1. Откройте консоль операционной системы.
2. Создайте локальную директорию для монтирования общего сетевого ресурса. Для этого введите команду:

   ```
   mkdir <полный путь локальной директории>
   ```

   Например:

   ```
   mkdir ~/nfsshare
   ```

3. После создания директории введите команду монтирования сетевого ресурса:

   ```
   sudo mount -t nfs <имя или IP-адрес удаленного компьютера>:\
   <полный путь общего сетевого ресурса>\
   <полный путь локальной директории>
   ```

   Например:

   ```
   sudo mount -t nfs nfs-server.example:/nfsshare ~/nfsshare
   ```

4. Проверьте результат монтирования с помощью команды:

   ```
   mount | grep <полный путь локальной директории>
   ```

   Например:

   ```
   mount | grep ~/nfsshare
   ```

   При успешном монтировании будут выведены данные, содержащие имя или IP-адрес удаленного компьютера, имя общего сетевого ресурса и имя родительской директории.

Автоматическое монтирование общего сетевого ресурса

Чтобы настроить автоматическое монтирование общего ресурса в операционной системе CentOS,

откройте файл /etc/fstab для редактирования с root-правами и в тексте файла добавьте строку:

```
<имя или IP-адрес удаленного компьютера>:<полный путь общего сетевого ресурса> <полный путь локальной директории> nfs defaults 0 0
```

Например:

```
nfs-server.example:/nfsshare /home/user1/nfsshare nfs defaults 0 0
```

Поиск угроз по базе событий

При работе в веб-интерфейсе приложения вы можете формировать поисковые запросы и использовать файлы формата IOC и YAML для поиска угроз по базе событий в рамках тех тенантов, к данным которых у вас есть доступ.

Для формирования поисковых запросов по базе событий вы можете использовать *режим конструктора* или *режим исходного кода*.

В режиме конструктора вы можете создавать и изменять поисковые запросы с помощью раскрывающихся списков с вариантами типа значения поля и операторов.

В режиме исходного кода вы можете создавать и изменять поисковые запросы с помощью текстовых команд.

Вы можете загрузить IOC-файл или YAML-файл с Sigma-правилом и искать события по условиям, заданным в этом файле.

Пользователи с ролью **Старший сотрудник службы безопасности** также могут создавать правила TAA (IOA) на основе условий поиска событий.

Поиск событий в режиме конструктора

Один поисковый запрос может содержать до 25 условий. Большее количество условий в одном запросе не поддерживается.

Чтобы задать условия поиска событий в режиме конструктора:

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**, закладку **Конструктор**.

   Откроется форма поиска событий.

2. В раскрывающемся списке выберите критерий для поиска событий.

   Вы можете посмотреть описание критериев для поиска событий в разделе *Критерии для поиска событий*.

3. В раскрывающемся списке выберите оператор.

   Вы можете посмотреть список доступных операторов в разделе *Операторы*.

   Для каждого типа значения поля будет доступен свой релевантный набор операторов. Например, при выборе типа значения поля **EventType** будут доступны операторы **=** и **!=**.

4. В зависимости от выбранного типа значения поля выполните одно из следующих действий:

   - Укажите в поле один или несколько символов, по которым вы хотите выполнить поиск событий.
   - В раскрывающемся списке выберите вариант значения поля, по которому вы хотите выполнить поиск событий.

   Например, для поиска полного совпадения по имени пользователя введите имя пользователя.

5. Если вы хотите добавить новое условие, используйте логический оператор **AND** или **OR** и повторите действия по добавлению условия.

6. Если вы хотите добавить группу условий, нажмите на кнопку **Group** и повторите действия по добавлению условий.

7. Если вы хотите удалить группу условий, нажмите на кнопку **Remove group**.

8. Если вы хотите выполнить поиск событий за определенный период, в раскрывающемся списке **Прошедшие сутки** выберите один из следующих периодов поиска событий:

   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий день.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий час.
   - **Прошедшая неделя**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущую неделю.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице события, найденные за указанный вами период.

9. Если вы выбрали **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

10. Нажмите на кнопку **Найти**.

    Отобразится таблица событий, соответствующих условиям поиска.

    Если вы используете режим распределенного решения и мультитенантности, отобразятся уровни группировки найденных событий: Сервер – Названия тенантов – Имена серверов.

11. Нажмите на имя того сервера, события которого вы хотите просмотреть.

Отобразится таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей.

Вы можете конвертировать запрос, созданный в конструкторе, в запрос для поиска событий в режиме исходного кода.

Поиск событий в режиме исходного кода

Один поисковый запрос может содержать до 25 условий. Большее количество условий в одном запросе не поддерживается.

Чтобы задать условия поиска событий в режиме исходного кода:

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**, вкладку **Редактор кода**.

   Откроется форма с полем ввода условий поиска событий в режиме исходного кода.

2. Введите условия поиска событий, используя критерии, операторы, логические операторы `OR` и `AND`, а также скобки для создания групп условий.

   Условие поиска должно соответствовать следующему синтаксису: `<критерий> <оператор> <значение критерия>`.

   Пример:

   ```
   EventType == 'filechange' AND
   (
   (
   FileName == '*example*' OR
   DllName == '*example*' OR
   DroppedName == '*example*' OR
   BlockedName == '*example*' OR
   InterpretedFileName == '*example*' OR
   InterpretedFiles.FileName == '*example*' OR
   TargetName == '*example*' OR
   HandleSourceName == '*example*' OR
   HandleTargetName == '*example*'
   ) OR
   UserName == '*example*'
   )
   ```

   Вы можете использовать функцию автозаполнения. Для этого установите курсор в строке запроса и нажмите комбинацию клавиш **Ctrl**+**Space**.

3. Если вы хотите выполнить поиск событий за определенный период, нажмите на кнопку **За все время** и выберите один из следующих периодов поиска событий:

   - **За все время**, если вы хотите, чтобы приложение отображало в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице события, найденные за указанный вами период.

4. Если вы выбрали **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

5. Нажмите на кнопку **Найти**.

   Отобразится таблица событий, соответствующих условиям поиска.

   Если вы используете режим распределенного решения и мультитенантности, отобразятся уровни группировки найденных событий: **Сервер** – Названия тенантов – Имена серверов.

6. Нажмите на имя того сервера, события по которому вы хотите просмотреть.

   Отобразится таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей.

Конвертация в запрос для поиска событий в режиме исходного кода

Вы можете конвертировать запрос, созданный в конструкторе, в запрос для поиска событий в режиме исходного кода.

При конвертации запроса его синтаксис адаптируется для поиска событий в режиме исходного кода.

Чтобы конвертировать запрос:

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**, закладку **Конструктор**.

   Откроется форма поиска событий.

2. В раскрывающемся списке выберите критерий для поиска событий.

   Вы можете посмотреть описание критериев для поиска событий в разделе *Критерии для поиска событий*.

3. В раскрывающемся списке выберите оператор.

   Вы можете посмотреть список доступных операторов в разделе *Операторы*.

   Для каждого типа значения поля будет доступен свой релевантный набор операторов. Например, при выборе типа значения поля **EventType** будут доступны операторы **=** и **!=**.

4. В зависимости от выбранного типа значения поля выполните одно из следующих действий:

   - Укажите в поле один или несколько символов, по которым вы хотите выполнить поиск событий.
   - В раскрывающемся списке выберите вариант значения поля, по которому вы хотите выполнить поиск событий.

   Например, для поиска полного совпадения по имени пользователя введите имя пользователя.

5. Если вы хотите добавить новое условие, используйте логический оператор **AND** или **OR** и повторите действия по добавлению условия.

6. Если вы хотите добавить группу условий, нажмите на кнопку **Group** и повторите действия по добавлению условий.

7. Если вы хотите удалить группу условий, нажмите на кнопку **Remove group**.

8. Если вы хотите выполнить поиск событий за определенный период, в раскрывающемся списке **За все время** выберите один из следующих периодов поиска событий:

   - **За все время**, если вы хотите, чтобы приложение отображало в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице события, найденные за указанный вами период.

9. Если вы выбрали **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

10. Перейдите на вкладку **Редактор кода**.

    Отобразится предупреждение о невозможности обратной конвертации.

11. Нажмите на кнопку **Конвертировать**.

Запрос будет конвертирован в запрос для поиска событий в режиме исходного кода.

Критерии для поиска событий

Для поиска событий в режиме конструктора доступны следующие критерии:

- **Общие сведения**:
  - Host – имя хоста.
  - HostIP – IP-адрес хоста.
  - EventType – тип события.
  - UserName – имя пользователя.
  - OsFamily – семейство операционной системы.
  - OsVersion – версия операционной системы, используемой на хосте.

- **Свойства TAA**:
  - IOAId – идентификатор правила TAA (IOA).
  - IOATag – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.
  - IOATechnique – техника MITRE.
  - IOATactics – тактика MITRE.
  - IOAImportance – степень важности, присвоенная событию, выполненному по этому правилу TAA (IOA).
  - IOAConfidence – уровень надежности в зависимости от вероятности ложных срабатываний правила.
- **Свойства файла**:
  - CreationTime – время создания события.
  - FileName – имя файла.
  - FilePath – путь к директории, в которой располагается файл.
  - FileFullName – полный путь к файлу. Включает путь к директории и имя файла.
  - ModificationTime – время изменения файла.
  - FileSize – размер файла.
  - MD5 – MD5-хеш файла.
  - SHA256 – SHA256-хеш файла.
  - SimilarDLLPath – вредоносная DLL, помещенная в директорию по стандартному пути обхода, чтобы система загрузила ее раньше, чем исходную DLL.
- **Процессы Linux**:
  - LogonRemoteHost – IP-адрес хоста, с которого был выполнен удаленный вход.
  - RealUserName – имя пользователя, назначенное ему при регистрации в системе.
  - EffectiveUserName – имя пользователя, которое было использовано для входа в систему.
  - FileOwnerUserName – имя владельца файла.
  - RealGroupName – имя группы пользователя.
  - EffectiveGroupName - имя группы пользователя, которое используется для работы.
  - Environment – переменные окружения.
  - ProcessType – тип процесса.
  - OperationResult – результат операции.

- **Запущен процесс**:
  - PID – идентификатор процесса.
  - ParentFileFullName – путь к файлу родительского процесса.
  - ParentMD5 – MD5-хеш файла родительского процесса.
  - ParentSHA256 – SHA256-хеш файла родительского процесса.
  - StartupParameters – параметры запуска процесса.
  - ParentPID – идентификатор родительского процесса.
  - ParentStartupParameters – параметры запуска родительского процесса.
- **Удаленное соединение**:
  - HTTPMethod – метод HTTP-запроса. Например, Get, Post или Connect.
  - ConnectionDirection – направление соединения (входящее или исходящее).
  - LocalIP – IP-адрес локального компьютера, с которого была произведена попытка удаленного соединения.
  - LocalPort – порт локального компьютера, с которого была произведена попытка удаленного соединения.
  - RemoteHostName – имя компьютера, на который была произведена попытка удаленного соединения.
  - RemoteIP – IP-адрес компьютера, на который была произведена попытка удаленного соединения.
  - RemotePort – порт компьютера, на который была произведена попытка удаленного соединения.
  - URI – адрес ресурса, к которому произведен запрос HTTP.
  - TlsVersion – версия протокола.
  - TlsSni – Server Name Indication, имя ресурса, к которому производится подключение.
  - TlsCertificateMd5 – MD5 TLS-сертификата.
  - TlsCertificateSha1 – SHA1 TLS-сертификата.
  - TlsCertificateSubjectNames – основное и дополнительные DNS-имена.
  - TlsCertificateIssuerName – название организации владельца сертификата.
  - TlsCertificateSerialNumber – серийный номер сертификата.
  - TlsCertificateCheckResult – результат проверки сертификата.
  - TlsCipherSuite – наборы шифрования сертификата.

- TlsCertificateValidFrom – дата, от которой отсчитывается срок годности сертификата.
- TlsCertificateValidTo – дата, после которой истекает срок годности сертификата.

- **DNS**:
  - DnsServerIpAddress – IP-адрес сервера DNS.
  - DnsQueryDomainName – имя домена из запроса.
  - DnsAnswerData – данные ответа.
  - DnsQueryTypeId – ID типа записи.
- **LDAP**:
  - LDAPSearchFilter – фильтр поиска.
  - LDAPSearchDistinguishedName – уникальное имя.
  - LDAPSearchAttributeList – список атрибутов поиска.
  - LDAPSearchScope – область поиска.
- **Именованный канал**:
  - PipeName – именованный канала.
  - PipeOperationType – тип операции с именованным каналом.
- **WMI**:
  - WmiOperationType – тип операции WMI: *Активность WMI* или *Имя потребителя событий WMI*.
  - WmiHostName – имя машины.
  - WmiUserName – имя пользователя.
  - WmiNamespaceName – пространство имен.
  - WmiQuery – текст запроса.
  - WmiFilterName – фильтр событий.
  - WmiConsumerName – имя потребителя событий.
  - WmiConsumerText – исходный код потребителя событий.
- **Изменение в реестре**:
  - RegistryKey – путь к ключу реестра.
  - RegistryValueName – имя параметра реестра.
  - RegistryValue – значение параметра реестра.

- RegistryOperationType – тип операции с реестром.
- RegistryPreviousKey – предыдущий путь к ключу реестра.
- RegistryPreviousValue – предыдущее имя параметра реестра.

- **Журнал событий ОС**:
  - WinLogEventID – идентификатор типа события безопасности в журнале Windows.
  - LinuxEventType – тип события. Данный критерий используется для операционных систем Linux и macOS.
  - WinLogName – имя журнала.
  - WinLogEventRecordID – идентификатор записи в журнале.
  - WinLogProviderName – идентификатор системы, записавшей событие в журнал.
  - WinLogTargetDomainName – доменное имя удаленного компьютера.
  - WinLogObjectName – имя объекта, инициировавшего событие.
  - WinlogPackageName – имя пакета, инициировавшего событие.
  - WinLogProcessName – имя процесса, инициировавшего событие.
- **Обнаружение и результат обработки**:
  - DetectName – имя обнаруженного объекта.
  - RecordID – идентификатор сработавшего правила.
  - ProcessingMode – режим проверки.
  - ObjectName – имя объекта.
  - ObjectType – тип объекта.
  - ThreatStatus – режим обнаружения.
  - UntreatedReason – статус обработки события.
  - ObjectContent (for AMSI events too) – содержание скрипта, переданного на проверку.
  - ObjectContentType (for AMSI events too) – тип содержимого скрипта.
- **Интерактивный ввод команд в консоли**:
  - InteractiveInputText – текст, введенный в командную строку.
  - InteractiveInputType – тип ввода (консоль или канал).

- **Изменен файл**:
  - FileOperationType – тип операции с файлом.
  - FilePreviousPath – путь к директории, в которой файл располагался ранее.
  - FilePreviousName - предыдущее имя файла.
  - FilePreviousFullName – полное имя файла, включающее предыдущий путь к директории, в которой файл располагался ранее, и / или предыдущее имя файла.
  - DroppedFileType – тип измененного файла.
- **Внедрение кода и доступ к процессу**:
  - AccessMethod – метод доступа.
  - InjectAddress – адресное пространство процесса-реципиента.
  - InjectedDllName – имя внедренной DLL.
  - ModifiedStartupParameters – измененные параметры запуска.
  - InjectedDllPath – путь к внедренной DLL.
  - CallTrace – трассировка вызова.
  - TargetStartupParameters – команда,с которой был запущен процесс-реципиент.
- **Доступ к процессу**:
  - AccessOperationType – тип операции: *Открыт доступ к процессу* или *Продублированный дескриптор*.
  - ProccessAccessRights – запрошенные права доступа к процессу.
  - HandleSourceStartupParameters – команда запуска исходного дескриптора.
  - HandletargetStartupParameters – команда запуска целевого дескриптора.
- **Другие**:
  - File type – тип файла.
  - TlsJa3Md5 – десятичные значения байтов в пакете приветствия клиента для следующих полей: версия TLS, набор шифров, список расширений протоколов TLS, эллиптические кривые и форматы эллиптических кривых.
  - TlsJa3sMd5 – десятичные значения байтов в пакете приветствия сервера для следующих полей: версия TLS, набор шифров и список расширений протоколов TLS.
  - DotNetAssemblyName – имя сборки .NET.
  - DotNetAssemblyFlags – флаги сборки .NET.

Вы можете посмотреть список полей для поиска событий в режиме исходного кода, скачав файл.

Операторы

Операторы, доступные для поиска в режиме конструктора и исходного кода, приведены в таблице ниже.

Операторы, доступные для поиска в режиме конструктора и исходного кода

Режим конструктора	Режим исходного кода
=	==
!=	NOT (example)
CONTAINS	==*example*
!CONTAINS	NOT (example=='*example*')
STARTS	=='example*'
!STARTS	NOT (example=='example*')
ENDS	==’*example’
!ENDS	NOT (example==’*example’)

Сортировка событий в таблице

Вы можете сортировать события в таблице по столбцам **Время события**, **Тип события**, **Хост** и **Имя пользователя**.

Чтобы отсортировать события в таблице событий:

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.

   Откроется окно **Поиск угроз**.

2. Задайте условия для поиска событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий, соответствующих условиям поиска.

3. Если вы хотите отсортировать события по времени, справа от названия столбца **Время события** нажмите на один из значков:

   - ↑ – новые события отобразятся вверху таблицы.
   - ↓ – старые события отобразятся вверху таблицы.

4. Если вы хотите отсортировать события по названию типов событий, справа от названия столбца **Тип события** нажмите на один из значков:

   - ↑ – сортировка выполнится по алфавиту А–Я.
   - ↓ – сортировка выполнится по алфавиту Я–А.

5. Если вы хотите отсортировать события по именам хостов, на которых были выполнены обнаружения, справа от названия столбца **Хост** нажмите на один из значков:

   - ↑ – сортировка выполнится по алфавиту А–Я.
   - ↓ – сортировка выполнится по алфавиту Я–А.

6. Если вы хотите отсортировать события по именам пользователей хостов, справа от названия **Имя пользователя** нажмите на один из значков:

   - ↑ – сортировка выполнится по алфавиту А–Я.
   - ↓ – сортировка выполнится по алфавиту Я–А.

7. Если вы хотите сгруппировать события по именам хостов или по названию типов событий, выберите в раскрывающемся списке **Группировать по** одно из значений:

   - **Группировать по имени хоста**, если хотите сгруппировать события по именам хостов.
   - **Группировать по типу события**, если хотите сгруппировать события по названиям типов событий.

   Если события были отсортированы по полю **Хост** или **Тип события**, при группировке событий по аналогичному признаку результат сортировки сбрасывается. Чтобы вернуться к результатам сортировки, выберите в раскрывающемся списке **Группировать по** значение **Группировать по**.

По умолчанию события в таблице отсортированы по времени: новые события располагаются вверху таблицы.

Вы можете отсортировать события только по одному признаку.

При сортировке по типу события на русском языке события сортируются в соответствии с внутренним наименованием типа события на английском языке.

Изменение условий поиска событий

*Чтобы изменить условия поиска событий, выполните следующие действия в разделе **Поиск угроз** окна веб-интерфейса приложения:*

1. Нажмите на форму с условиями поиска событий в верхней части окна.
2. Выберите одну из следующих закладок:

   - **Конструктор**, если вы хотите изменить условия поиска событий в режиме конструктора.
   - **Редактор кода**, если вы хотите изменить условия поиска событий в режиме исходного кода.

3. Внесите необходимые изменения.

4. Нажмите на одну из следующих кнопок:

   - **Обновить**, если вы хотите обновить текущий поиск событий новыми условиями.
   - **Новый поиск**, если вы хотите выполнить новый поиск событий.

Отобразится таблица событий, соответствующих условиям поиска.

Поиск событий типа Обнаружение и Результат обработки обнаружения

Чтобы выполнить поиск событий типа Обнаружение и Результат обработки обнаружения:

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**, закладку **Конструктор**.

   Откроется форма поиска событий.

2. Если вы хотите выполнить поиск событий по статусу обработки, выполните следующие действия:

   a. В раскрывающемся списке критериев поиска событий в группе **Обнаружение и результат обработки** выберите критерий **ThreatStatus**.

   b. В раскрывающемся списке операторов сравнения выберите один из вариантов:

      - **=** (равно);
      - **!=** (не равно).

   c. В раскрывающемся списке статусов обработки события выберите один из вариантов:

      - **Объект не заражен**.
      - **Объект вылечен**.
      - **Ложное срабатывание**.
      - **Объект добавлен пользователем**.
      - **Объект добавлен в исключения**.
      - **Объект удален**.
      - **Объект помещен на карантин**.
      - **Объект не найден**.
      - **Выполнен откат к предыдущему состоянию**.
      - **Объект не поддается обработке**.
      - **Объект не обработан**.

- **Обработка прервана**.
- **Неизвестно**.

3. Если вы хотите выполнить поиск событий по причинам, по которым они не были обработаны, выполните следующие действия:

   a. В раскрывающемся списке критериев поиска событий в группе **Обнаружение и результат обработки** выберите критерий **UntreatedReason**.

   b. В раскрывающемся списке операторов сравнения выберите один из вариантов:

      - **=** (равно);
      - **!=** (не равно).

   c. В раскрывающемся списке причин, по которым события не были обработаны, выберите один из вариантов:

      - **Объект уже был обработан**.
      - **Приложение работает в режиме Только отчет**.
      - **Не удалось создать резервную копию объекта**.
      - **Не удалось создать копию объекта**.
      - **Устройство не готово**.
      - **Объект заблокирован**.
      - **Нет прав на выполнение действия**.
      - **Объект невозможно вылечить**.
      - **Объект невозможно перезаписать**.
      - **Объект не найден**.
      - **Нет места на диске**.
      - **Обработка отменена**.
      - **Действие отложено**.
      - **Задача на обработку прервана**.
      - **Ошибка чтения данных**.
      - **Нет данных**.
      - **Объект является критическим системным**.
      - **Ошибка записи данных**.

- **Запись данных не поддерживается**.
- **Объект защищен от записи**.

4. Если вы хотите добавить новое условие, используйте логический оператор **AND** или **OR** и повторите действия по добавлению условия.
5. Если вы хотите добавить группу условий, нажмите на кнопку **Group** и повторите действия по добавлению условий.
6. Если вы хотите удалить группу условий, нажмите на кнопку **Remove group**.
7. Если вы хотите выполнить поиск событий за определенный период, в раскрывающемся списке **За все время** выберите один из следующих периодов поиска событий:
   - **За все время**, если вы хотите, чтобы приложение отображало в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице события, найденные за указанный вами период.
8. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.
9. Нажмите на кнопку **Найти**.

Отобразится таблица событий, соответствующих условиям поиска.

Поиск событий по условиям, заданным в файле формата IOC и YAML

При создании IOC-файла ознакомьтесь со списком IOC-терминов, которые можно использовать для поиска событий в разделе **Поиск угроз**. Вы можете посмотреть список поддерживаемых IOC-терминов, скачав файл по ссылке ниже.

IOC-термины для поиска событий в разделе **Поиск угроз**

Чтобы найти события по условиям, заданным в файле формата IOC или YAML:

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.

2. Нажмите на кнопку **Импортировать**.

   Откроется окно выбора файлов.

3. Выберите файл, который хотите загрузить, и нажмите на кнопку **Открыть**.

   Файл загрузится.

   На закладке **Редактор кода** в форме с условиями поиска событий отобразятся условия, заданные в загруженном файле.

   Вы можете искать события по этим условиям. Вы также можете изменить условия, заданные в загруженном файле, или добавить условия поиска событий в режиме исходного кода.

4. Если вы хотите выполнить поиск событий за определенный период, нажмите на кнопку **За все время** и выберите один из следующих периодов поиска событий:

   - **За все время**, если вы хотите, чтобы приложение отображало в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице события, найденные за указанный вами период.

5. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

6. Нажмите на кнопку **Найти**.

Отобразится таблица событий, соответствующих условиям, заданным в загруженном файле.

Создание правила TAA (IOA) на основе условий поиска событий

Чтобы создать правило TAA (IOA) на основе условий поиска событий:

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.

2. Выполните поиск событий в режиме конструктора или режиме исходного кода.

3. Нажмите на кнопку **Сохранить как правило TAA (IOA)**.

   Откроется окно **Новое правило TAA (IOA)**.

4. В поле **Имя** введите имя правила.

5. Нажмите на кнопку **Сохранить**.

Условие поиска событий будет сохранено. В таблице правил TAA (IOA) раздела **Пользовательские правила**, в подразделе **TAA** веб-интерфейса отобразится новое правило с заданным именем.

Не рекомендуется в условиях поиска событий, сохраняемых как пользовательское правило TAA (IOA), использовать следующие поля:

- IOAId.
- IOATag.
- IOATechnique.
- IOATactics.
- IOAImportance.
- IOAConfidence.

На момент сохранения пользовательского правила TAA (IOA) в приложении может не быть событий, содержащих данные для этих полей. Когда события с этими данными появятся, пользовательское правило TAA (IOA), созданное ранее, не сможет разметить события по этим полям.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания правила TAA (IOA) на основе условий поиска событий недоступна.

Информация о событиях

Если вы используете режим распределенного решения и мультитенантности, при работе в веб-интерфейсе приложения вы можете просматривать информацию о событиях в рамках тех тенантов, к данным которых у вас есть доступ.

В информации о событиях отображаются локальные метки времени того компьютера с компонентом Endpoint Agent, на котором было обнаружено событие. Администратору приложения требуется контролировать актуальность времени на компьютерах с компонентом Endpoint Agent.

Чтобы включить отображение событий по всем тенантам, выполните следующие действия:

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.
2. Включите переключатель **Искать по всем тенантам**.

   В таблице событий отобразятся события по всем тенантам.

Рекомендации по обработке событий

В окне события в рамке между деревом событий и текстовой информацией для пользователей с ролью **Старший сотрудник службы безопасности** отображаются кнопки с действиями, доступными для обработки этого события.

Вы можете выполнить следующие действия:

- **Изолировать <имя хоста>** – изолировать хост с компонентом Endpoint Agent, на котором обнаружено событие, от сети. Применяется для всех типов событий.
- **Создать правило запрета** – запретить запуск файла, обнаруженного в событии. Не применяется для событий **USB-устройство**. На устройствах под управлением операционной системы Windows не применяется также для событий **Журнал событий ОС**.
- **Создать задачу** – создать задачу. Не применяется для событий **USB-устройство**. На устройствах под управлением операционной системы Windows не применяется также для событий **Журнал событий ОС**.

Кроме того, вы можете выполнить действия по обработке события по ссылкам с именем файла, путем к файлу, MD5-хешем, SHA256-хешем файла и именем хоста при просмотре текстовой информации о событии в нижней части окна.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.

- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- Найти на Kaspersky TIP.
- Найти события.
- Найти алерты.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Найти на Kaspersky TIP.
- **Найти на virustotal.com**.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.

- Выполнить задачи:
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Получить файл**.
  - **Собрать форензику**.
  - **Поместить файл на карантин**.
  - **Запустить программу**.
- **Скопировать значение в буфер**.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** рекомендации по обработке событий не отображаются.

Выполнение рекомендации по изоляции хоста

Чтобы выполнить рекомендацию по изоляции хоста от сети:

1. В рамке с рекомендациями выберите **Изолировать <имя хоста>**.

   Откроется окно параметров изоляции хоста из события, с которым вы работаете.

2. В поле **Отключить изоляцию через** введите количество часов от 1 до 9999, в течение которых будет действовать сетевая изоляция хоста.

3. В блоке параметров **Исключения для правила изоляции хоста** в списке **Направление трафика** выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.

4. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.

   Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent, вы можете использовать прокси-сервер для соединения Kaspersky Endpoint Agent для Windows с Kaspersky Anti Targeted Attack Platform. При добавлении этого прокси-сервера в исключения сетевые ресурсы, к которым открыт доступ через прокси-сервер, также добавляются в исключения. Если в исключения добавлены сетевые ресурсы, соединение с которыми происходит через прокси-сервер, но при этом исключение для самого прокси-сервера не настроено, исключение не будет работать.

5. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.

6. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия по заполнению полей **Направление трафика**, **IP** и **Порты**.

7. Нажмите на кнопку **Сохранить**.

Информация об изоляции хоста отобразится в разделе **Endpoint Agents** веб-интерфейса.

Вы также можете создать правило сетевой изоляции по ссылке **Изолировать <имя хоста>** в информации об обнаружении и в разделе **Endpoint Agents** веб-интерфейса.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изоляции хоста от сети недоступна.

Выполнение рекомендации по запрету запуска файла

Чтобы выполнить рекомендацию по запрету запуска файла:

1. В рамке с рекомендациями выберите **Создать правило запрета**.

   Откроется окно создания правила запрета с MD5- или SHA256-хешем файла из события, с которым вы работаете.

2. Задайте значения следующих параметров:

   a. **Состояние** – состояние правила запрета:

   - Если вы хотите включить правило запрета, переведите переключатель в положение **Вкл**.
   - Если вы хотите отключить правило запрета, переведите переключатель в положение **Откл**.

   b. **Имя** – имя правила запрета.

   c. Если вы хотите, чтобы приложение выводило уведомление о срабатывании правила запрета пользователю компьютера, на который распространяется запрет, установите флажок **Показывать пользователю уведомление о блокировке запуска файла**.

   d. Если вы хотите изменить область применения правила запрета, настройте параметр **Запрет для**:

   - Если вы хотите применить правило запрета на всех хостах всех серверов, выберите вариант **Всех хостов**.
   - Если вы хотите применить правило запрета на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите применить правило запрета.

     Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
   - Если вы хотите применить правило запрета на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

3. Нажмите на кнопку **Добавить**.

Запрет на запуск файла будет создан.

Информация о созданном запрете отобразится в разделе **Политики** веб-интерфейса.

Если вы установили флажок **Показывать пользователю уведомление о блокировке запуска файла**, при попытке запуска запрещенного файла пользователю будет показано уведомление о том, что сработало правило запрета запуска этого файла.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция запрета запуска файла недоступна.

Выполнение рекомендации по созданию задачи

Чтобы выполнить рекомендацию по созданию задачи:

1. В рамке с рекомендациями по ссылке **Создать задачу** раскройте список типов задач.
2. Выберите один из типов задач:
   - **Завершить процесс**.
   - **Собрать форензику**.
   - **Запустить YARA-проверку**.
   - **Управлять службами**.
   - **Получить дамп памяти процесса**.
   - **Получить метафайлы NTFS**.
   - **Запустить программу**.
   - **Получить файл**.
   - **Удалить файл**.
   - **Поместить файл на карантин**.
   - **Восстановить файл из карантина**.

   Откроется окно создания задачи с предзаполненными данными (например, именем хоста, путем к файлу, MD5- или SHA256-хешем файла) из события, с которым вы работаете.
3. Если вы хотите изменить предзаполненные данные из события, внесите изменения в соответствующие поля.
4. Если вы хотите добавить комментарий к задаче, введите его в поле **Описание**.

5. Если вы создаете задачу **Завершить процесс**, **Удалить файл**, **Запустить YARA-проверку** или **Управлять службами** и хотите изменить область применения задачи, настройте параметр **Задача для**:

   - Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
   - Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

     Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
   - Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

6. Нажмите на кнопку **Добавить**.

   Задача будет создана.

Информация о созданной задаче отобразится в разделе **Задачи** веб-интерфейса.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания задачи недоступна.

Информация о событиях в дереве событий

Дерево событий отображается в верхней части окна информации о событии.

В дереве событий содержится следующая информация:

- Событие, информацию о котором вы просматриваете.

  Просматриваемое событие располагается справа.
- Родительский процесс.

  Родительский процесс располагается слева от просматриваемого события. Если для просматриваемого события нет родительского процесса, вместо него отображается имя хоста, на котором было зафиксировано просматриваемое событие.

При нажатии на имя родительского процесса слева отображается процесс, который инициировал появление этого процесса и является родительским по отношению к нему. Если родительского процесса нет, отображается имя хоста.

Справа от имени каждого родительского процесса отображается общее количество событий, вызванных этим процессом. Вы можете просмотреть список событий и информацию о выбранном событии.

Просмотр информации о родительском процессе в дереве событий

Чтобы просмотреть информацию о родительском процессе для просматриваемого события:

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии. В верхней части окна отобразится дерево событий.

3. Нажмите на имя родительского процесса.

   В нижней части окна на закладке **Сведения** отобразится информация о процессе, который является родительским по отношению к просматриваемому событию.

Просмотр информации о событиях, инициированных родительским процессом, в дереве событий

Чтобы просмотреть таблицу всех событий, инициированных родительским процессом:

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии. В верхней части окна информации о событии отобразится дерево событий.

3. Нажмите на имя родительского процесса в дереве событий.

   В нижней части окна на закладке **Сведения** отобразится информация о событии, которое является родительским по отношению к просматриваемому событию.

4. Перейдите на закладку **События**.

   Отобразится таблица всех событий, инициированных родительским процессом. По умолчанию события в таблице отсортированы по времени: новые события располагаются вверху таблицы.

   Вы можете просмотреть информацию о событии, нажав на строку с этим событием. Узел события отобразится в дереве событий.

Чтобы просмотреть таблицу событий, сгруппированных по типу, выполните следующие действия:

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии. В верхней части окна информации о событии отобразится дерево событий.

3. Нажмите на раскрывающийся список справа от имени узла родительского процесса в дереве событий.

   Отобразится список всех событий, инициированных родительским процессом. По умолчанию события в списке сгруппированы по типу.

4. В дереве событий в раскрывающемся списка справа от имени родительского процесса выберите один из следующих элементов:

   - Если вы хотите просмотреть все события, инициированные родительским процессом, выберите **Все события**.

     Отобразится таблица всех событий, инициированных родительским процессом. По умолчанию события в таблице отсортированы по времени: новые события располагаются вверху таблицы.

   - Если вы хотите просмотреть все события одного типа, инициированные родительским процессом, выберите имя нужного типа событий.

     Отобразится таблица всех событий, инициированных родительским процессом и сгруппированных по типу.

   Вы можете просмотреть информацию о событии, нажав на строку с этим событием. Событие отобразится в дереве событий.

Просмотр информации о хосте в дереве событий

Если для просматриваемого события или родительского процесса нет процесса, инициировавшего его появление, вместо узла процесса в дереве событий отображается узел хоста, на котором было зафиксировано событие или был запущен родительский процесс.

Чтобы просмотреть информацию о хосте, на котором было зафиксировано событие или был запущен родительский процесс:

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии. В верхней части окна отобразится дерево событий.

3. Нажмите на имя хоста в дереве событий.

   В нижней части окна отобразится информация о хосте, на котором было зафиксировано событие или был запущен родительский процесс.

Просмотр таблицы событий

Таблица событий отображается в разделе **Поиск угроз** окна веб-интерфейса приложения после выполнения поиска угроз по базе событий. Вы можете сортировать события в таблице по столбцам **Время события**, **Тип события**, **Хост** и **Имя пользователя**.

Если вы используете режим распределенного решения и мультитенантности, события в таблице сгруппированы по хостам выбранных серверов и тенантов.

В таблице событий содержится следующая информация:

1. **Время события** – дата и время обнаружения события.
2. **Тип события** – например, **Запущен процесс**.
3. **Имя хоста** – имя хоста, на котором было выполнено обнаружение.
4. **Сведения** – сведения о событии.
5. **Имя пользователя** – имя пользователя компьютера с компонентом Endpoint Agent, под учетной записью которого было обнаружено событие.

В таблице событий для каждого типа событий в столбце **Тип события** отображается свой набор данных в столбце **Сведения** (см. таблицу ниже).

Набор данных в столбце **Тип события** для каждого типа событий в столбце **Сведения**

Тип события	Сведения
Запущен процесс	Имя файла процесса, который был запущен. SHA256- и MD5-хеш.
Загружен модуль	Имя динамической библиотеки, которая была загружена. SHA256- и MD5-хеш.
Удаленное соединение	URL-адрес, к которому была произведена попытка удаленного подключения. Имя файла, который пытался осуществить удаленное подключение.
Правило запрета	Имя файла приложения, запуск которого был заблокирован. SHA256- и MD5-хеш.
Заблокирован документ	Имя документа, запуск которого был заблокирован. SHA256- и MD5-хеш.
Изменен файл	Имя созданного файла. SHA256- и MD5-хеш.
Журнал событий ОС	Канал записи событий в системный журнал. Идентификатор типа события.
Изменение в реестре	Имя ключа в реестре. `<имя переменной в ключе>=<значение переменной>`.
Прослушан порт	Адрес сервера и порт. Имя файла процесса, который осуществляет прослушивание порта.
Загружен драйвер	Имя файла драйвера, который был загружен. SHA256- и MD5-хеш.
Обнаружение	Имя файла, в котором обнаружен объект. Имя обнаруженного объекта. SHA256- и MD5-хеш.
Результат обработки обнаружения	Имя файла, в котором обнаружен объект. Имя обнаруженного объекта. SHA256- и MD5-хеш.
AMSI-проверка	Имя проверенного объекта. Тип скрипта. Содержимое скрипта, переданного на проверку.
Интерпретированный запуск файла	Имя запущенного файла. SHA256- и MD5-хеш.
Интерактивный ввод команд в консоли	Текст команды.
Завершен процесс	Имя файла остановленного процесса. SHA256- и MD5-хеш.
DNS	Имя запрашиваемого домена. Идентификатор типа ресурсной записи.
LDAP	Область и фильтр поиска.
Именованный канал	Имя канала. Тип операции с каналом.
WMI	Тип операции WMI. Исходный код потребителя событий.
Внедрение кода	Имя файла целевого процесса или имя динамической библиотеки, содержащей процедуру перехватчика и имя функции, которой передается управление после внедрения. Метод доступа к файлу целевого процесса. SHA256- и MD5-хеш файла целевого процесса.
Доступ к процессу	Имя файла процесса-реципиента. Степень важности события. Тип операции, проведенной над файлом процесса. Права доступа к процессу.
USB-устройство	Тип подключенного устройства. Имя подключенного устройства. Тип операции с подключенным устройством. Признак системного диска (поле отображается, если подключенное устройство является системным диском).

По ссылке с названием типа события, сведениями, дополнительной информацией и именем пользователя раскрывается список, в котором вы можете выбрать действие над объектом. В зависимости от значения в ячейке вы можете выполнить одно из следующих действий:

- Для всех значений в ячейке:
  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Скопировать значение в буфер**.
- Имя хоста:
  - **Найти события**.
  - **Найти алерты**.
  - **Изолировать от сети**.
- Имя файла:
  - **Завершить процесс**.
  - **Завершить по уникальному PID**.
  - **Удалить файл**.
  - **Получить файл**.
  - **Собрать форензику**.
  - **Поместить файл на карантин**.
- MD5-хеш:
  - **Найти события**.
  - **Найти алерты**.
  - **Найти на Kaspersky TIP**.
  - **Создать правило запрета**.
  - **Найти в Хранилище**.
- SHA256-хеш:
  - **Найти события**.
  - **Найти алерты**.
  - **Найти на Kaspersky TIP**.
  - **Найти на virustotal.com**.

- Создать правило запрета.
- Найти в Хранилище.

Настройка отображения таблицы событий

Вы можете настроить отображение столбцов, а также порядок их следования в таблице событий.

Чтобы настроить отображение таблицы событий:

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.

3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.

5. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.

6. Нажмите на кнопку **Применить**.

Отображение таблицы событий будет настроено.

Просмотр информации о событии

Чтобы просмотреть информацию о событии:

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**, закладку **Конструктор** или **Редактор кода**.

   Откроется форма поиска событий.

2. Если вы используете режим распределенного решения и мультитенантности и хотите включить отображение событий по всем тенантам, включите переключатель **Искать по всем тенантам**.

3. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

4. Выберите событие, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о событии.

Информация о событии Запущен процесс

В окне с информацией о событиях типа **Запущен процесс** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- Раздел **Запущен процесс**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла процесса.
  - **ID процесса** – идентификатор процесса.
  - **Параметры запуска** – параметры запуска процесса.

    Если событие было записано в базу событий Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, вместо поля **Параметры запуска** отображается поле **Команда** – команда, с помощью которой был запущен процесс.
  - **Текущая директория** – текущая директория процесса.
  - **MD5** – MD5-хеш файла процесса.
  - **SHA256** – SHA256-хеш файла процесса.
  - **Размер** – размер файла процесса.
  - **Тип файла** – тип файла процесса.
  - **Время события** – время запуска процесса.
  - **Время изменения атрибутов** – время изменения атрибутов файла процесса.
  - **Время создания** – время создания файла процесса.
  - **Время изменения** – время последнего изменения файла процесса.

- Раздел **Сведения**:
  - **Название приложения** – например, название операционной системы.
  - **Производитель** – например, производитель операционной системы.
  - **Описание файла** – например, Example File.
  - **Исходное имя файла** – например, ExampleFile.exe.
  - **Получатель сертификата** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи** – например, "Недействительна" или "OK".
  - **Свойства** – атрибут файла по классификации Windows. Например, A (архив), D (директория) или S (системный).

  Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, в разделе **Сведения** также отображаются следующие поля:

  - **Свойства** – свойства файла процесса.
  - **Тип процесса** – например, exec.
  - **Переменные окружения** – переменные окружения процесса.
  - **Настоящее имя пользователя** – имя пользователя, назначенное при регистрации в системе.
  - **Настоящее имя группы** – группа, к которой принадлежит пользователь.
  - **Действующее имя пользователя** – имя пользователя, которое использовалось для входа в систему.
  - **Действующее имя группы** – группа, к которой принадлежит пользователь, чье имя использовалось для входа в систему.
  - **Имя пользователя-владельца** – имя пользователя, создавшего файл процесса.
  - **Имя группы-владельца** – название группы, пользователи которой могут изменить или удалить файл процесса.
  - **Разрешенные привилегии файла** – разрешения, которые могут использоваться для доступа к файлу процесса. Данное поле не отображается, если событие было записано приложением Kaspersky Endpoint Security для Mac.
  - **Наследуемые привилегии файла** – разрешения, которые есть у группы пользователей для выполнения операций с родительским каталогом файла процесса. Данное поле не отображается, если событие было записано приложением Kaspersky Endpoint Security для Mac.
  - **Актуальные привилегии файла** – разрешения, которые актуальны для файла процесса на данный момент. Данное поле не отображается, если событие было записано приложением Kaspersky Endpoint Security для Mac.
  - **Загружен с URL** – URL-адрес, с которого был скачан файл процесса.
  - **Адрес источника** – мета-данные о письме, из которого был получен файл процесса.

- **Свойства учетной записи** – флаги учетной записи пользователя, под которой был запущен процесс.
- **Флаги создания процесса** – флаги создания процесса.
- **Символическая ссылка** – путь к символической ссылке.
- **Трассировка вызова** – стек вызовов.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
  - **Параметры запуска** – параметры запуска родительского процесса.

    Если событие было записано в базу событий Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, вместо поля **Параметры запуска** отображается поле **Команда** – команда, с помощью которой был запущен родительский процесс.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был запущен процесс.
  - **IP хоста** – IP-адрес хоста, на котором был запущен процесс.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Тип учетной записи** – тип учетной записи, под которой был запущен процесс. Например, администратор.
  - **Тип входа в систему** – например, с помощью запущенной службы.
  - **Имя пользователя** – имя пользователя, запустившего процесс.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

    Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, в разделе **Сведения о системе** также отображается поле **Вход с удаленного хоста** – имя хоста, с которого был совершен удаленный вход в систему.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачу Получить файл.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Запустить программу**.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Завершить процесс.
  - **Удалить файл**.
  - Получить файл.
  - **Поместить файл на карантин.**
  - Запустить программу.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Mac, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачу Получить файл.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Найти на Kaspersky TIP.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Найти на Kaspersky TIP.

- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Завершен процесс

В окне с информацией о событиях типа **Завершен процесс** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- Раздел **Завершен процесс**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла процесса.
  - **ID процесса** – идентификатор процесса.
  - **Параметры запуска** – параметры запуска процесса.

    Если событие было записано в базу событий Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, вместо поля **Параметры запуска** отображается поле **Команда** – команда, с помощью которой был запущен процесс.
  - **MD5** – MD5-хеш файла процесса.
  - **SHA256** – SHA256-хеш файла процесса.
  - **Размер** – размер файла процесса.
  - **Время события** – время завершения процесса.
- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
  - **Параметры запуска** – параметры запуска родительского процесса.

    Если событие было записано в базу событий Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, вместо поля **Параметры запуска** отображается поле **Команда** – команда, с помощью которой был запущен родительский процесс.

- **MD5** – MD5-хеш файла родительского процесса.
- **SHA256** – SHA256-хеш файла родительского процесса.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был запущен процесс.
  - **IP хоста** – IP-адрес хоста, на котором был запущен процесс.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

  - **Тип учетной записи** – тип учетной записи, под которой был завершен процесс. Например, администратор.
  - **Имя пользователя** – имя пользователя, запустившего процесс.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

  Если событие было записано в базу событий Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, в разделе **Сведения о системе** также отображается поле **Вход с удаленного хоста** – имя хоста, с которого был совершен удаленный вход в систему.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.

- Выполнить задачу **Получить файл**.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачи:
  - **Собрать данные** → **Файл**, **Форензика**, **Образ диска**, **Дамп памяти**.
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Запустить программу**.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачи:
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Получить файл**.
  - **Поместить файл на карантин.**
  - **Запустить программу**.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Mac, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачу **Получить файл**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Загружен модуль

В окне с информацией о событиях типа **Загружен модуль** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- Раздел **Загружен модуль**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла загруженного модуля.
  - **MD5** – MD5-хеш файла загруженного модуля.
  - **SHA256** – SHA256-хеш файла загруженного модуля.

- **Размер** – размер загруженного модуля.
- **Время события** – время загрузки модуля.

- Раздел **Сведения**:
  - **Название приложения** – например, название операционной системы.
  - **Производитель** – например, производитель операционной системы.
  - **Описание файла** – например, Example File.
  - **Исходное имя файла** – например, Example File.
  - **Получатель сертификата** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи** – например, "Подпись недействительна" или "Подпись OK".
  - **Время создания** – время создания загруженного модуля.
  - **Время изменения** – дата последнего изменения загруженного модуля.
  - **Следующая по пути обхода DLL** – поле содержит путь к библиотеке DLL, которая могла быть загружена вместо существующей библиотеки.

    Поле отображается при выполнении следующих условий:

    - Источник загруженной библиотеки DLL не является доверенным.
    - В папке по стандартному пути обхода есть одноименная библиотека с другим хешем.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был загружен модуль.
  - **IP хоста** – IP-адрес хоста, на котором был загружен модуль.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – имя пользователя, загрузившего модуль.
- **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу в разделе **Загружен модуль** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем файла или путем к файлу в разделе **Инициатор события** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.

- Выполнить задачи:
  - **Собрать данные** → **Файл**, **Форензика**, **Образ диска**, **Дамп памяти**.
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Запустить программу**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Удаленное соединение

В окне с информацией о событиях типа **Удаленное соединение** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.

- Раздел **Удаленное соединение**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Направление соединения** – направление соединения (входящее или исходящее).
  - **Удаленный IP-адрес** – IP-адрес хоста, на который была произведена попытка удаленного соединения.
  - **Локальный IP-адрес** – IP-адрес локального компьютера, с которого была произведена попытка удаленного соединения.
  - **Время события** – время попытки удаленного соединения.
- Раздел **TLS**:
  - **Версия** – версия протокола.
  - **SNI** – имя веб-сайта, с которым требуется установить соединение.
  - **Зашифрованный SNI** – зашифрованное имя веб-сайта
  - **MD5 сертификата** – MD5-хеш файла сертификата.
  - **SHA1 сертификата** – SHA1-хеш файла сертификата.
  - **Имя издателя сертификата** – имя организации, подписавшей сертификат.
  - **Серийный номер сертификата** – уникальный номер сертификата.
  - **Результат проверки сертификата** – результат проверки сертификата.
  - **Сертификат действует с** – дата, начиная с которой годен сертификат.
  - **Сертификат действует до** – дата, после которой истекает срок действия сертификата.
  - **JA3** – десятичные значения байтов для следующих полей в пакете приветствия клиента: версия протокола TLS, набор шифров, список расширений протоколов TLS, эллиптические кривые и форматы эллиптических кривых. Для разграничения полей используется символ ",", для разграничения значений в каждом поле используется "-".
  - **JA3S** – десятичные значения байтов для следующих полей в пакете приветствия сервера: версия TLS, набор шифров и список расширений протоколов TLS. Для разграничения полей используется символ ",", для разграничения значений в каждом поле используется "-".
  - **JA3 MD5** – отпечаток JA3.
  - **JA3S MD5** – отпечаток JA3S.

- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, с которого была произведена попытка удаленного соединения.
  - **IP хоста** – IP-адрес хоста, с которого была произведена попытка удаленного соединения.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, который пытался установить удаленное соединение.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу в разделе **Удаленное соединение** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем файла или путем к файлу в разделе **Инициатор события** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.

- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Запустить программу**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Найти на Kaspersky TIP.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.

- **Найти на Kaspersky TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Правило запрета

В окне с информацией о событиях, в которых сработали правила запрета – событиях типа **Правило запрета** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- Раздел **Правило запрета**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла, запуск которого был запрещен.
  - **Параметры запуска** – параметры, с которыми была произведена попытка запуска файла.
  - **MD5** – MD5-хеш файла, запуск которого был запрещен.
  - **SHA256** – SHA256-хеш файла, запуск которого был запрещен.
  - **Размер** – размер файла, запуск которого был запрещен.
  - **Время события** – время срабатывания запрета запуска файла.
- Раздел **Сведения**:
  - **Название приложения** – например, название операционной системы.
  - **Производитель** – например, производитель операционной системы.
  - **Описание файла** – например, Example File.
  - **Исходное имя файла** – например, ExampleFile.exe.
  - **Получатель сертификата** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи** – например, "Подпись недействительна" или "Подпись OK".

- **Время создания** – время создания файла, запуск которого был запрещен.
- **Время изменения** – дата последнего изменения файла, запуск которого был запрещен.

- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором сработал запрет запуска файла.
  - **IP хоста** – IP-адрес хоста, на котором сработал запрет запуска файла.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, под учетной записью которого был произведен запуск файла.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачи:
  - **Собрать данные** → **Файл**, **Форензика**, **Образ диска**, **Дамп памяти**.
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Запустить программу**.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Завершить процесс.
  - **Удалить файл**.
  - Получить файл.
  - **Поместить файл на карантин.**
  - Запустить программу.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Найти на Kaspersky TIP.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Заблокирован документ

В окне с информацией о событиях типа **Заблокирован документ** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- Раздел **Заблокирован документ**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя заблокированного документа.
  - **MD5** – MD5-хеш заблокированного документа.
  - **SHA256** – SHA256-хеш заблокированного документа.
  - **Время события** – время блокирования документа.
  - **Файл процесса** – имя файла процесса, который попытался открыть документ.
  - **MD5 процесса** – MD5-хеш процесса, который попытался открыть документ.
  - **SHA256 процесса** – SHA256-хеш процесса, который попытался открыть документ.
- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.

- **SHA256** – SHA256-хеш файла родительского процесса.
- **ID процесса** – идентификатор родительского процесса.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был заблокирован документ.
  - **IP хоста** – IP-адрес хоста, на котором был заблокирован документ.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

  - **Имя пользователя** – имя пользователя, попытавшегося открыть документ.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу в разделе **Заблокирован документ** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем файла или путем к файлу в разделе **Инициатор события** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.

- Получить файл.
- Собрать форензику.
- Поместить файл на карантин.

- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Запустить программу**.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Завершить процесс.
  - **Удалить файл**.
  - Получить файл.
  - **Поместить файл на карантин.**
  - Запустить программу.
  - **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Найти на Kaspersky TIP.

- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Изменен файл

В окне с информацией о событиях типа **Изменен файл** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- В зависимости от типа операции, которая была проведена с файлом, в информации о событии отображается одно из следующих названий раздела:
  - **Создан файл**.
  - **Изменен файл**.
  - **Переименован файл**.
  - **Изменены атрибуты файла**.
  - **Удален файл**.
  - **Прочитан файл**.
  - **Создана жесткая ссылка**.
  - **Символическая ссылка создана**.
  - **Изменено время создания файла**.

В разделе может отображаться следующая информация:

- **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

  По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

  Поле отображается, если при создании события сработало правило TAA (IOA).

- **Файл** – имя созданного, удаленного или измененного файла.
- **MD5** – MD5-хеш созданного, удаленного или измененного файла.
- **MD5 файла, на который создана ссылка** – MD5-хеш файла, на который была создана ссылка.
- **SHA256** – SHA256-хеш созданного, удаленного или измененного файла.
- **SHA256 файла, на который создана ссылка** – SHA256-хеш файла, на который была создана ссылка.
- **Символическая ссылка** – полное имя файла, для которого создана символическая ссылка.
- **Размер** – размер созданного, удаленного или измененного файла.
- **Время события** – время обнаружения события.
- **Время создания** – время создания файла.
- **Время изменения** – время последнего изменения файла.
- **Время изменения атрибутов** – время изменения атрибутов файла.
- **Предыдущая версия** – имя предыдущей версии файла.

  Поле **Предыдущая версия** отображается в информации о событии только для операции типа **Переименован файл**.

- **Удалить после перезагрузки** – статус файла, предназначенного к удалению.

  Если файл, к которому была применена операция "удалить", открыт в каком-либо приложении или задействован в других процессах, он будет удален по завершении этих процессов после перезагрузки хоста. В этом случае в поле **Удалить после перезагрузки** отображается Да.

  Если файл, к которому была применена операция "удалить", был удален сразу, в поле **Удалить после перезагрузки** отображается Нет.

  Поле **Удалить после перезагрузки** отображается в информации о событии только для операции типа **Удален файл**.

Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, в разделе также отображаются следующие поля:

- **Тип файла** – расширение созданного, удаленного или измененного файла.
- **Флаги открытия файла** – значение флагов открытия созданного, удаленного или измененного файла.
- **Имя пользователя-владельца** – имя пользователя, создавшего файл.
- **Имя группы-владельца** – название группы, пользователи которой могут изменить или удалить файл.
- **Разрешенные привилегии файла** – разрешения, которые могут использоваться для доступа к созданному, удаленному или измененному файлу. Данное поле не отображается, если событие было записано приложением Kaspersky Endpoint Security для Mac.
- **Наследуемые привилегии файла** – разрешения, которые есть у группы пользователей для выполнения операций с родительским каталогом созданного, удаленного или измененного файла. Данное поле не отображается, если событие было записано приложением Kaspersky Endpoint Security для Mac.
- **Актуальные привилегии файла** – разрешения, которые актуальны для созданного или измененного файла на данный момент. Данное поле не отображается, если событие было записано приложением Kaspersky Endpoint Security для Mac.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

  Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, в разделе **Инициатор события** также отображаются следующие поля:
  - **Переменные окружения** – переменные окружения процесса.
  - **Настоящее имя пользователя** – имя пользователя, назначенное ему при регистрации в системе.
  - **Настоящее имя группы** – группа, к которой принадлежит пользователь.
  - **Действующее имя пользователя** – имя пользователя, которое было использовано для входа в систему.
  - **Действующее имя группы** – группа, к которой принадлежит пользователь, имя которого использовалось для входа в систему.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был создан файл.
  - **IP хоста** – IP-адрес хоста, на котором был создан файл.

Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – имя пользователя, создавшего файл.
- **Версия ОС** – версия операционной системы, используемой на хосте.

Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, в разделе **Сведения о системе** также отображается поле **Вход с удаленного хоста** – имя хоста, с которого был совершен удаленный вход в систему.

По ссылке с именем файла или путем к файлу в разделе со сведениями о файле, с которым была произведена операция, раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем файла или путем к файлу в разделе **Инициатор события** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.

- Собрать форензику.
- Поместить файл на карантин.

- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачу Получить файл.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Запустить программу**.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Завершить процесс.
  - **Удалить файл**.
  - Получить файл.

- **Поместить файл на карантин.**
- Запустить программу.

- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Mac, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачу Получить файл.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Найти на Kaspersky TIP.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Найти на Kaspersky TIP.
- **Найти на virustotal.com**.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

Информация о событии Журнал событий ОС

В окне с информацией о событиях типа **Журнал событий ОС** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- Раздел **Журнал событий ОС**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Время события** – время обнаружения события.
  - **ID события безопасности** – идентификатор типа события безопасности в журнале Windows.

  Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux, в разделе **Журнал событий ОС** также отображаются следующие поля:
  - **Тип события** – тип события.
  - **Результат операции** – например, **Успешно** или **Сбой**.
- Раздел **Информация о событии**, содержащий данные из системного журнала. Состав данных зависит от типа события Windows.

  > Раздел **Информация о событии** не отображается в информации о событиях, записанных в базу событий приложением Kaspersky Endpoint Security для Linux.
- Раздел **Инициатор события**:
  - **Файл** – имя файла процесса.
  - **ID процесса** – идентификатор процесса.
  - **Команда** – команда, с помощью которой был запущен родительский процесс.
  - **Переменные окружения** – переменные окружения процесса.
  - **Настоящее имя пользователя** – имя пользователя, назначенное при регистрации в системе.
  - **Настоящее имя группы** – группа, к которой принадлежит пользователь.

Раздел **Инициатор события** не отображается в информации о событиях, записанных в базу событий приложением Kaspersky Endpoint Security для Windows.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором произошло событие.
  - **IP хоста** – IP-адрес хоста, на котором произошло событие.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, который запустил процесс, инициировавший запись в системный журнал.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

    В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, также отображается поле **Вход с удаленного хоста** – имя компьютера, с которого был совершен удаленный вход в систему.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачу Получить файл.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - **Завершить процесс**.
  - **Удалить файл**.

    - **Поместить файл на карантин.**
    - **Запустить программу**.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
    - Завершить процесс.
    - **Удалить файл**.
    - Получить файл.
    - **Поместить файл на карантин.**
    - Запустить программу.
- **Скопировать значение в буфер**.

Информация о событии Изменение в реестре

В окне с информацией о событиях типа **Изменение в реестре** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- В зависимости от типа операции, которая была проведена с реестром, в информации о событии отображается одно из следующих названий раздела:
    - **Создан ключ реестра**.
    - **Удален ключ реестра**.
    - **Изменен реестр**.
    - **Запрошен ключ реестра**.
    - **Переименован ключ реестра**.
    - **Сохранен ключ реестра**.

В разделе отображается следующая информация:

- **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

  По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

  Поле отображается, если при создании события сработало правило TAA (IOA).

- **Файл** – полный путь к файлу, в который был сохранен ключ реестра.

  > Поле отображается для типа события **Сохранен ключ реестра**.

- **Путь к ключу** – путь к разделу реестра, в котором произошло изменение.
- **Имя параметра** – например, RegistrySizeLimit.
- **Значение параметра** – значение параметра реестра.
- **Тип параметра** – например, REG_DWORD.
- **Время события** – время внесения изменения в реестр.

  При изменении имени или параметра ключа реестра могут отображаться дополнительные поля с информацией о состоянии ключа реестра до его изменения:

  - поле **Предыдущий путь к ключу** отображается при изменении имени ключа реестра;
  - поле **Предыдущее значение параметра** отображается при изменении значения параметра реестра;
  - поле **Предыдущий тип параметра** отображается при изменении типа параметра реестра.

- Раздел **Инициатор события**:

  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - Найти события.
    - Найти алерты.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - Завершить процесс.
    - Завершить по уникальному PID.
    - Удалить файл.
    - Получить файл.

- Собрать форензику.
- Поместить файл на карантин.

- **MD5** – MD5-хеш файла родительского процесса.

  По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - **Найти алерты**.
  - Найти на Kaspersky TIP.
  - **Найти в Хранилище**.
  - **Создать правило запрета**.

  Скопировать значение в буфер.

- **SHA256** – SHA256-хеш файла родительского процесса.

  По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - **Найти алерты**.
  - Найти на Kaspersky TIP.
  - **Найти в Хранилище**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

- Раздел **Сведения о системе**:

  - **Имя хоста** – имя хоста, на котором было произведено изменение в реестре.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - Найти события.
    - Найти алерты.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
    - Завершить процесс.
    - Удалить файл.

- Поместить файл на карантин.
- Запустить программу.

- **IP хоста** – IP-адрес хоста, на котором было произведено изменение в реестре.

  Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

  Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – имя пользователя, совершившего изменение в реестре.
- **Версия ОС** – версия операционной системы, используемой на хосте.

Информация о событии Прослушан порт

В окне с информацией о событиях типа **Прослушан порт** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- Раздел **Прослушан порт**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Локальный порт** – порт, который был прослушан.
  - **Локальный IP-адрес** – IP-адрес сетевого интерфейса, порт которого был прослушан.
  - **Время события** – время прослушивания порта.
- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - Найти события.
    - Найти алерты.
    - **Скопировать значение в буфер**.

Выполнить задачи:

- Завершить процесс.
- Завершить по уникальному PID.
- Удалить файл.
- Получить файл.
- Собрать форензику.
- Поместить файл на карантин.

- **MD5** – MD5-хеш файла родительского процесса.
  По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:
  - **Найти события**.
  - **Найти алерты**.
  - Найти на Kaspersky TIP.
  - **Найти в Хранилище**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- **SHA256** – SHA256-хеш файла родительского процесса.
  По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:
  - **Найти события**.
  - **Найти алерты**.
  - Найти на Kaspersky TIP.
  - **Найти в Хранилище**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, порт которого был прослушан.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

Выполнить задачи:

- **Собрать данные** → **Файл**, **Форензика**, **Образ диска**, **Дамп памяти**.
- **Завершить процесс**.
- **Удалить файл**.
- **Поместить файл на карантин**.
- **Запустить программу**.

- **IP хоста** – IP-адрес хоста, порт которого был прослушан.

  Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

  Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – имя пользователя, от имени которого было совершено прослушивание порта.
- **Версия ОС** – версия операционной системы, используемой на хосте.

Информация о событии Загружен драйвер

В окне с информацией о событиях типа **Загружен драйвер** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- Раздел **Загружен драйвер**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).

- **Файл** – имя файла загруженного драйвера.
- **MD5** – MD5-хеш файла загруженного драйвера.
- **SHA256** – SHA256-хеш файла загруженного драйвера.
- **Размер** – размер загруженного драйвера.
- **Время события** – время загрузки драйвера.

- Раздел **Сведения**:
  - **Название приложения** – например, название операционной системы.
  - **Производитель** – например, производитель операционной системы.
  - **Описание файла** – например, Example File.
  - **Исходное имя файла** – например, ExampleFile.exe.
  - **Получатель сертификата** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи** – например, "Подпись недействительна" или "Подпись OK".
  - **Время создания** – время создания загруженного драйвера.
  - **Время изменения** – время последнего изменения загруженного драйвера.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на который был загружен драйвер.
  - **IP хоста** – IP-адрес хоста, на который был загружен драйвер.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, загрузившего драйвер.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.

- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Запустить программу**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Найти на Kaspersky TIP.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.

- Найти на Kaspersky TIP.
- **Найти на virustotal.com**.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

Информация о событии DNS

В окне с информацией о событиях типа **DNS** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- Раздел **DNS**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **IP сервера** – IP-адрес запрашиваемого DNS-сервера в формате IPv4.
  - **Параметры запроса** – параметры DNS-запроса.
  - **Статус запроса** – статус DNS-запроса.
  - **Имя домена** – имя домена, для которого требуется разрешить запись DNS.
  - **ID типа записи** – тип ресурсной записи.
  - **Данные ответа** – содержание ответа DNS-сервера на запрос.
  - **Время события** – время отправки DNS-запроса.
- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.

    Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux, в разделе **Инициатор события** также отображаются следующие поля:

- **Переменные окружения** – переменные окружения процесса.
- **Настоящее имя пользователя** – имя пользователя, назначенное при регистрации в системе.
- **Настоящее имя группы** – группа, к которой принадлежит пользователь.
- **Действующее имя пользователя** – имя пользователя, которое использовалось для входа в систему.
- **Действующее имя группы** – группа, к которой принадлежит пользователь, чье имя использовалось для входа в систему.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, от которого поступил запрос к DNS-серверу.
  - **IP хоста** – IP-адрес хоста, от которого поступил запрос к DNS-серверу.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Вход с удаленного хоста** – имя хоста, с которого был совершен удаленный вход в систему.
  - **Имя пользователя** – имя пользователя, под учетной записью которого был отправлен запрос к DNS-серверу.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылкам с IP-адресом сервера, ID типа записи и именем пользователя раскрывается список, в котором вы можете выполнить одно из следующих действий:

- Найти алерты.
- **Скопировать значение в буфер**.

По ссылке с именем домена раскрывается список, в котором вы можете выполнить одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP**.
- **Скопировать значение в буфер**.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Найти на Kaspersky TIP.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Найти на Kaspersky TIP.
- **Найти на virustotal.com**.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачи:
  - **Собрать данные** → **Файл**, **Форензика**, **Образ диска**, **Дамп памяти**.
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Запустить программу**.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Завершить процесс.
  - **Удалить файл**.
  - Получить файл.
  - **Поместить файл на карантин.**
  - Запустить программу.
- **Скопировать значение в буфер**.

По ссылке с IP-адресом хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- **Скопировать значение в буфер**.

Информация о событии LDAP

В окне с информацией о событиях типа **LDAP** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- Раздел **LDAP**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Область поиска** – область поиска LDAP. Может иметь одно из следующих значений: ADS_SCOPE_BASE, ADS_SCOPE_ONELEVEL, ADS_SCOPE_SUBTREE.
  - **Фильтр поиска** – фильтр поиска LDAP.
  - **Уникальное имя** – имя записи в каталоге LDAP.
  - **Список атрибутов поиска** – атрибуты, заданные в поисковом запросе в качестве возвращаемых.
  - **Параметры запуска** – параметры запуска процесса.
- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был выполнен поисковый запрос LDAP.
  - **Имя пользователя** – имя пользователя, под учетной записью которого был выполнен поисковый запрос LDAP.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

Информация о событии Именованный канал

В окне с информацией о событиях типа **Именованный канал** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.

  В зависимости от типа операции с именованным каналом в информации о событии отображается одно из следующих названий раздела:

  - **Канал создан**.
  - **Канал подключен**.

  В разделе отображается следующая информация:

  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – файл процесса, создавшего именованный канал или подключившегося к нему.
  - **Время события** – время создания именованного канала или подключившегося к нему.
- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был создан именованный канал или произошло подключение к нему.
  - **Имя пользователя** – имя пользователя, под учетной записью которого был создан именованный канал или произошло подключение к нему.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем канала раскрывается список, в котором вы можете выполнить одно из следующих действий:

- Найти алерты.
- **Скопировать значение в буфер**.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Найти на Kaspersky TIP.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Найти на Kaspersky TIP.
- **Найти на virustotal.com**.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачи:
  - **Собрать данные** → **Файл**, **Форензика**, **Образ диска**, **Дамп памяти**.
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Запустить программу**.
- **Скопировать значение в буфер**.

По ссылке с IP-адресом хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

По ссылке с именем пользователя раскрывается список, в котором вы можете выполнить одно из следующих действий:

- **Найти алерты**.
- **Скопировать значение в буфер**.

Информация о событии WMI

В окне с информацией о событиях типа **WMI** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.

  В зависимости от типа операции в информации о событии отображается одно из следующих названий раздела:

  - **Активность WMI**.
  - **Имя потребителя событий WMI**.

В разделе **Активность WMI** отображается следующая информация:

- **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

  По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

  Поле отображается, если при создании события сработало правило TAA (IOA).

- **Удаленное соединение** – удаленный запуск службы WMI. Если служба была запущена удаленно, в поле отображается **Да**.

- **Имя машины** – имя хоста, на котором была запущена служба WMI.

- **Имя пользователя** – имя пользователя, под учетной записью которого была запущена служба WMI.

- **Пространство имен** – пространство имен WMI.

- **Запрос** – команда, с которой была запущена служба WMI.

В разделе **Активность WMI** отображается следующая информация:

- **Удаленное соединение** – удаленный запуск службы WMI. Если служба была запущена удаленно, в поле отображается **Да**.

- **Пространство имен** – пространство имен потребителя событий.

- **Имя фильтра событий** – имя фильтра потребителя событий. Поле отображается для типа события **Активность WMI**.

- **Имя потребителя событий** – имя созданного потребителя событий.

- **Описание потребителя событий** – описание созданного потребителя событий. Поле отображается для типа события **Имя потребителя событий WMI**.

- Раздел **Инициатор события**:

  - **Файл** – имя файла родительского процесса.

  - **Параметры запуска** – параметры запуска родительского процесса.

  - **MD5** – MD5-хеш файла родительского процесса.

  - **SHA256** – SHA256-хеш файла родительского процесса.

- Раздел **Сведения о системе**:

  - **Имя хоста** – IP-адрес хоста, на котором была запущена служба WMI или создан потребитель событий.

  - **IP хоста** – IP-адрес хоста, на котором была запущена служба WMI или создан потребитель событий.

  - **Имя пользователя** – имя пользователя, под учетной записью которого была запущена служба WMI или создан потребитель событий.

  - **Версия ОС** – версия операционной системы, используемой на хосте.

Информация о событии Обнаружение

В окне с информацией о событии типа **Обнаружение** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- На закладке **Сведения** в разделе **Обнаружение**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Обнаружено** – имя обнаруженного объекта.

    По ссылке с именем объекта раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - **Найти события**.
    - **Просмотреть на Kaspersky Threats**.
    - **Скопировать значение в буфер**.
  - **Последнее действие** – последнее действие над обнаруженным объектом.
  - **Имя объекта** – полное имя файла, в котором обнаружен объект.
  - **MD5** – MD5-хеш файла, в котором обнаружен объект.
  - **SHA256** – SHA256-хеш файла, в котором обнаружен объект.
  - **Тип объекта** – тип объекта (например, файл).
  - **Режим обнаружения** – режим проверки, в котором создан алерт.
  - **Время события** – дата и время события.
  - **ID записи** – идентификатор записи об обнаружении в базе.
  - **Версия баз** – версия баз, с помощью которых создан алерт.
  - **Содержание** – содержание скрипта, переданного на проверку.

    Вы можете скачать эти данные, нажав на кнопку **Сохранить в файл**.
- На закладке **Сведения** в разделе **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- **Скопировать значение в буфер**.

Выполнить задачи:

- Завершить процесс.
- Завершить по уникальному PID.
- Удалить файл.
- Получить файл.
- Собрать форензику.
- Поместить файл на карантин.

- **ID процесса** – идентификатор родительского процесса.
- **Параметры запуска** – параметры запуска родительского процесса.
- **MD5** – MD5-хеш файла родительского процесса.
- **SHA256** – SHA256-хеш файла родительского процесса.

- На закладке **Сведения** в разделе **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором создан алерт.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - Найти события.
    - Найти алерты.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
    - Завершить процесс.
    - Удалить файл.
    - Поместить файл на карантин.
    - Запустить программу.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи: Получить файл, **Удалить файл**, **Поместить файл на карантин**, Запустить программу.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Mac, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачу Получить файл.
- **Скопировать значение в буфер**.

- **IP хоста** – IP-адрес хоста, на котором создан алерт.

  Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

  Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – учетная запись пользователя, от имени которой было совершено действие над обнаруженным объектом.
- **Версия ОС** – версия операционной системы, используемой на хосте.

- На закладке **История** в таблице:
  - **Тип** – тип события: **Обнаружение** или **Результат обработки обнаружения**.
  - **Описание** – описание события.
  - **Время** – дата и время обнаружения и результата обработки обнаружения.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Найти на Kaspersky TIP.

- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Результат обработки обнаружения

В окне с информацией о событии типа **Результат обработки обнаружения** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- На закладке **Сведения** в блоке параметров **Результат обработки обнаружения**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Обнаружено** – имя обнаруженного объекта.

    По ссылке с именем объекта раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - **Найти события**.
    - **Просмотреть на Kaspersky Threats**.
    - **Скопировать значение в буфер**.
  - **Последнее действие** – последнее действие над обнаруженным объектом.
  - **MD5** – MD5-хеш файла, в котором обнаружен объект.

- **SHA256** – SHA256-хеш файла, в котором обнаружен объект.
- **Тип объекта** – тип объекта (например, файл).
- **Имя объекта** – полное имя файла, в котором обнаружен объект.
- **Режим обнаружения** – режим проверки, в котором создан алерт.
- **Время события** – дата и время события.
- **ID записи** – идентификатор записи об обнаружении в базе.
- **Версия баз** – версия баз, с помощью которых создан алерт.

- На закладке **Сведения** в блоке параметров **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - Найти события.
    - Найти алерты.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - Завершить процесс.
    - Завершить по уникальному PID.
    - Удалить файл.
    - Получить файл.
    - Собрать форензику.
    - Поместить файл на карантин.
  - **ID процесса** – идентификатор родительского процесса.
  - **Параметры запуска** – параметры запуска родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- На закладке **Сведения** в блоке параметров **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором создан алерт.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- **Скопировать значение в буфер**.

Выполнить задачи:

- **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
- Завершить процесс.
- Удалить файл.
- Поместить файл на карантин.

Запустить программу.

- **IP хоста** – IP-адрес хоста, на котором создан алерт.

  Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

  Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – учетная запись пользователя, от имени которой было совершено действие над обнаруженным объектом.
- **Версия ОС** – версия операционной системы, используемой на хосте.

- На закладке **История** в таблице:
  - **Тип** – тип события **Результат обработки обнаружения**.
  - **Описание** – описание события.
  - **Время** – дата и время результата обработки алерта.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Найти на Kaspersky TIP.
- **Найти в Хранилище**.

- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Интерпретированный запуск файла

В окне с информацией о событиях типа **Интерпретированный запуск файла** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- Раздел **Интерпретированный запуск файла**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла.
  - **MD5** – MD5-хеш файла.
  - **SHA256** – SHA256-хеш файла.
  - **Размер** – размер файла.
  - **Время создания** – время создания файла.
  - **Время изменения** – время последнего изменения файла.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был запущен файл.
  - **IP хоста** – IP-адрес хоста, на котором был запущен файл.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, под учетной записью которого был запущен файл.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу в разделе **Интерпретированный запуск файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем файла или путем к файлу в разделе **Инициатор события** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.

- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Запустить программу**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- Найти на Kaspersky TIP.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.

- Найти на Kaspersky TIP.
- **Найти на virustotal.com**.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

Информация о событии AMSI-проверка

В окне с информацией о событии типа **AMSI-проверка** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- В разделе **AMSI-проверка**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Имя объекта** – имя проверенного объекта.
  - **MD5** – MD5-хеш проверенного объекта.
  - **SHA256** – SHA256-хеш проверенного объекта.
  - **Время события** – дата и время события.
  - **Тип содержимого** – тип скрипта.

    В приложении предусмотрено два типа скриптов:

    - Если скрипт представлен в виде текста, в поле **Тип содержимого** отображается тип скрипта *Текст*.
    - Если скрипт представлен в другой форме, в поле **Тип содержимого** отображается тип скрипта *Двоичный код*.
  - **Содержание** – содержание скрипта, переданного на проверку.

    Вы можете скопировать эти данные, нажав на кнопку **Скопировать в буфер**, если данные представлены в виде текста, или скачать файл с данными, нажав на кнопку **Сохранить в файл**, если данные представлены в другой форме.

    Поле **Содержание** отображается в информации о событии, если приложение регистрирует признаки целевых атак.

- В разделе **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - Найти события.
    - Найти алерты.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - Завершить процесс.
    - Завершить по уникальному PID.
    - Удалить файл.
    - Получить файл.
    - Собрать форензику.
    - Поместить файл на карантин.
  - **MD5** – MD5-хеш файла родительского процесса.

    По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - **Найти алерты**.
    - Найти на Kaspersky TIP.
    - **Найти в Хранилище**.
    - **Создать правило запрета**.
    - **Скопировать значение в буфер**.
  - **SHA256** – SHA256-хеш файла родительского процесса.

    По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - **Найти алерты**.
    - Найти на Kaspersky TIP.
    - **Найти в Хранилище**.

- **Создать правило запрета**.
- **Скопировать значение в буфер**.

- В разделе **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором выполнено обнаружение.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - **Найти алерты**.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Собрать данные** → **Файл**, **Форензика**, **Образ диска**, **Дамп памяти**.
    - **Завершить процесс**.
    - **Удалить файл**.
    - **Поместить файл на карантин**.
    - **Запустить программу**.
  - **IP хоста** – IP-адрес хоста, на котором выполнено обнаружение.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – учетная запись пользователя, от имени которой было совершено изменение в реестре.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

Информация о событии Интерактивный ввод команд в консоли

В окне с информацией о событиях типа **Интерактивный ввод команд в консоли** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.

- Раздел **Интерактивный ввод команд в консоли**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Тип ввода** – тип ввода команд, которые были переданы консольному приложению.

    В приложении предусмотрено два типа ввода команд:
    - Если команды в консольном приложении были введены пользователем, в поле **Тип ввода** отображается тип ввода команд *Консоль*.
    - Если команды были переданы в консольное приложение из другого приложения через коммуникационный шлюз (пайп), в поле **Тип ввода** отображается тип ввода команд *Канал.*
    - **Текст команды** – текст, введенный в командную строку (например, CMD) на хосте с компонентом Endpoint Agent.

    Вы можете скопировать этот текст, нажав на кнопку **Скопировать в буфер**, расположенную в поле **Текст команды**.
  - **Время события** – время обнаружения события.
- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - **Найти события**.
    - **Найти алерты**.
    - **Скопировать значение в буфер**.

    Выполнить задачи:
    - **Завершить процесс**.
    - **Завершить по уникальному PID**.
    - **Удалить файл**.
    - **Получить файл**.
    - **Собрать форензику**.
    - **Поместить файл на карантин**.
  - **MD5** – MD5-хеш файла родительского процесса.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

- **SHA256** – SHA256-хеш файла родительского процесса.

  По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - **Найти алерты**.
  - **Найти на Kaspersky TIP**.
  - **Найти в Хранилище**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

- Раздел **Сведения о системе**:

  - **Имя хоста** – имя хоста, на котором была введена команда.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - **Найти алерты**.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Собрать данные** → **Файл**, **Форензика**, **Образ диска**, **Дамп памяти**.
    - **Завершить процесс**.
    - **Удалить файл**.
    - **Поместить файл на карантин**.
    - **Запустить программу**.

  - **IP хоста** – IP-адрес хоста, на котором была введена команда.

Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – учетная запись пользователя, от имени которой была введена команда.
- **Версия ОС** – версия операционной системы, используемой на хосте.

Информация о событии Внедрение кода

В окне с информацией о событиях типа **Внедрение кода** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- Раздел **Внедрение кода**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – путь к файлу целевого процесса.
  - **ID процесса** – идентификатор целевого процесса.
  - **Параметры запуска** – параметры запуска целевого процесса.
  - **Измененные параметры запуска** – измененные параметры запуска целевого процесса.

    Поле отображается, если внедрение кода произошло с помощью метода ARG_SPOOFING.
  - **MD5** – MD5-хеш файла целевого процесса.
  - **SHA256** – SHA256-хеш файла целевого процесса.
  - **Метод доступа** – метод доступа к целевому процессу.

    В поле могут отображаться следующие значения: WRITE_EXECUTABLE_MEMORY, SET_WINDOWS_HOOK, QUEUE_APC_THREAD, SET_THREAD_CONTEXT – .MAP_VIEW_OF_SECTION, CREATE_REMOTE_THREAD, ARG_SPOOFING.
  - **Адресное пространство** – адрес в адресном пространстве целевого процесса, куда был размещен удаленно запускаемый код.

    Поле не заполняется, если внедрение кода произошло с помощью методов SET_WINDOWS_HOOK и ARG_SPOOFING.

- **Параметры системного вызова** – команда, с которой был запущен целевой процесс.
- **Имя DLL** – имя DLL, содержащей процедуру перехватчика и имя функции, которой передается управление после внедрения.

  Поле заполняется, если внедрение кода произошло с помощью метода SET_WINDOWS_HOOK.
- **Полный путь к DLL** – путь к DLL, содержащей процедуру перехватчика.

  Поле заполняется, если внедрение кода произошло с помощью метода SET_WINDOWS_HOOK.
- **Время события** – время внедрения кода.
- **Трассировка вызова** – стек вызовов API на момент перехвата функции, связанной с внедрением кода.

- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором произошло внедрение кода.
  - **Имя пользователя** – имя пользователя, под учетной записью которого произошло внедрение кода.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

Информация о событии Доступ к процессу

В окне с информацией о событиях типа **Изменен файл** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.
- В зависимости от типа операции, которая была проведена с файлом процесса, в информации о событии отображается одно из следующих названий раздела:
  - **Открыт доступ к процессу**.
  - **Продублированный дескриптор**.

  В разделе **Открыт доступ к процессу** отображается следующая информация:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), в соответствии с которым выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).

- **Файл** – имя процесса-реципиента.
- **ID процесса** – идентификатор процесса-реципиента.
- **Параметры запуска** – параметры запуска процесса-реципиента.
- **MD5** – MD5-хеш файла процесса-реципиента.
- **SHA256** – SHA256-хеш файла процесса-реципиента.
- **Права доступа** – запрошенные права доступа к процессу.
- **Размер** – размер файла процесса-реципиента.
- **Время события** – время обнаружения события.
- Время создания – время создания файла процесса-реципиента.
- **Время изменения** – время последнего изменения файла процесса-реципиента.
- **Время изменения атрибутов** – время изменения атрибутов файла процесса-реципиента.
- **Трассировка вызова** – стек вызовов.

В разделе **Продублированный дескриптор** отображается следующая информация:

- **Файл** – имя продублированного процесса.
- **MD5** – MD5-хеш файла продублированного процесса.
- **SHA256** – SHA256-хеш файла продублированного процесса.
- **Время создания** – время создания файла продублированного процесса.
- **Время изменения** – время последнего изменения файла продублированного процесса.
- **Время изменения атрибутов** – время изменения атрибутов файла продублированного процесса.
- **Размер** – размер файла продублированного процесса.
- **ID процесса** – идентификатор продублированного процесса.
- **Параметры запуска** – параметры запуска продублированного процесса.

Для событий этого типа в информации о событии также отображаются разделы **Информация о процессе, в который был продублирован дескриптор** и **Информация о процессе, из которого был продублирован дескриптор**. В этих разделах содержится следующая информация:

- **Файл** – имя файла процесса.
- **MD5** – MD5-хеш файла процесса.
- **SHA256** – SHA256-хеш файла процесса.
- **ID процесса** – идентификатор процесса.

- **Параметры запуска** – параметры запуска процесса.
- **Размер** – размер файла процесса.
- **Время создания** – время создания файла процесса.
- **Время изменения** – время последнего изменения файла.
- **Время изменения атрибутов** – время изменения атрибутов файла процесса.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **Параметры запуска** – параметры запуска родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был создан файл.
  - **Имя пользователя** – имя пользователя, создавшего файл.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу в разделе со сведениями о файле, с которым была произведена операция, раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.
- Выполнить задачи:
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем файла или путем к файлу в разделе **Инициатор события** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти алерты.

- Выполнить задачи:
  - **Завершить процесс**.
  - **Завершить по уникальному PID**.
  - **Удалить файл**.
  - **Получить файл**.
  - **Собрать форензику**.
  - **Поместить файл на карантин**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Найти на Kaspersky TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии USB-устройство

В окне с информацией о событиях типа **USB-устройство** содержатся следующие сведения:

- Дерево событий.
- Действия, которые можно выполнить для обработки события.

- Раздел **Диск подключен**:
  - **Имя устройства** – имя подключенного устройства.
  - **ID устройства** – идентификатор подключенного устройства.
  - **Тип устройства** – тип подключенного устройства.
  - **Системный диск** – признак системного диска. Возможные значения: **Да**, **Нет**.
  - **Время события** – время подключения устройства.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, к которому подключено устройство.
  - **IP хоста** – IP-адрес хоста, к которому подключено устройство.
  - **Имя пользователя** – имя пользователя, под учетной записью которого подключено устройство.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

Проверка цепочек событий по правилам TAA (IOA) "Лаборатории Касперского"

Существуют кибератаки, которые можно выявить только по определенной последовательности событий. Если функция проверки цепочек событий включена, Kaspersky Anti Targeted Attack Platform отмечает события, поступающие на сервер Central Node, по правилам TAA (IOA) "Лаборатории Касперского" и при обнаружении подозрительной последовательности событий записывает алерт в таблицу алертов.

Вы можете просмотреть события, отмеченные правилом TAA (IOA) "Лаборатории Касперского", одним из следующих способов:

- Создав поисковый запрос по базе событий со следующими критериями: IOATag, IOAImportance, IOAConfidence.
- при просмотре событий и алертов.

Редактирование правил TAA (IOA) "Лаборатории Касперского" не предусмотрено. Если вы хотите, чтобы приложение не создавало алерты для событий, сформированных в результате нормальной для вашей организации активности хоста, вы можете добавить правило TAA (IOA) в исключения. Для одного правила TAA (IOA) "Лаборатории Касперского" можно создать только одно исключение.

В режиме распределенного решения и мультитенантности вам нужно включить проверку цепочек событий на каждом сервере Central Node, на котором вы хотите использовать функцию. Если компонент Central Node развернут в виде кластера, вы можете включить функцию на любом сервере кластера.

Использование правил TAA (IOA), проверяющих цепочки событий, увеличивает использование системных ресурсов. Если в процессе работы приложения возникают проблемы с работоспособностью, рекомендуется выключить эту функцию.

Особенности отображения информации о цепочках событий на виджетах

На виджетах топ 10 отображается информация только о событиях, которые вызвали срабатывание правила TAA (IOA). События, которые произошли ранее и участвуют в построении цепочки событий, но не вызвали срабатывание правила, в виджетах не учитываются. В связи с этим возможно расхождение между количеством событий, указанном в виджете, и количестве событий, которое отображается в выборке при переходе по ссылке с именем хоста и названию правила TAA (IOA).

Включение и выключение проверки цепочек событий по правилам TAA (IOA) "Лаборатории Касперского"

Чтобы включить или выключить проверку цепочек событий по правилам TAA (IOA) "Лаборатории Касперского":

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Endpoint Agents**.
2. В блоке параметров **Использование правил TAA (IOA) для цепочек событий** выполните одно из следующих действий:
   - Если вы хотите включить функцию, переведите переключатель **Использовать правила для цепочек событий** в положение **Включено**.
   - Если вы хотите отключить функцию, переведите переключатель **Использовать правила для цепочек событий** в положение **Выключено**.

   По умолчанию функция выключена.

Проверка цепочек событий по правилам TAA (IOA) "Лаборатории Касперского будет включена или выключена.

Просмотр событий, отмеченных правилом TAA (IOA) "Лаборатории Касперского"

*Чтобы просмотреть все события, отмеченные выбранным правилом TAA (IOA) "Лаборатории Касперского", из раздела **Алерты**:*

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.
2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.
3. В раскрывающемся списке слева выберите **Содержит**.
4. В раскрывающемся списке справа выберите технологию **(TAA) Targeted Attack Analyzer**.
5. Нажмите на кнопку **Применить**.

   В таблице отобразятся алерты, выполненные технологией TAA на основе правил TAA (IOA).

6. Выберите алерт, для которого в столбце **Обнаружено** отображается название нужного правила.

   Откроется окно с информацией об алерте.

7. В блоке **Результаты проверки** по ссылке с названием правила откройте окно с информацией о правиле.

8. В открывшемся окне нажмите на кнопку **События**.

Отобразится таблица событий, соответствующих выбранному правилу TAA (IOA).

*Чтобы просмотреть все события, отмеченные выбранным правилом TAA (IOA) "Лаборатории Касперского", из раздела **Поиск угроз**:*

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.

2. Задайте условия поиска и нажмите на кнопку **Найти**. Например, вы можете выбрать критерии для поиска событий в группе **Свойства TAA** в режиме конструктора.

   Отобразится таблица событий, удовлетворяющих условиям поиска.

3. Выберите событие.

4. Справа от названия параметра **Теги IOA** нажмите на имя правила.

   Откроется окно с информацией о правиле.

5. В открывшемся окне нажмите на кнопку **События**.

Отобразится таблица событий, соответствующих выбранному правилу TAA (IOA).

Управление активами

Активы – это все устройства, присутствующие в локальной и внутренней сети организации. Для управления активами вы можете просматривать таблицу устройств в разделе **Активы** веб-интерфейса Kaspersky Anti Targeted Attack Platform. Также вы можете просматривать информацию о взаимодействиях устройств и выполнять различные действия с устройствами при работе с картой сетевых взаимодействий и с топологической картой.

Просмотр таблицы устройств

Для контроля устройств в приложении формируется таблица устройств. Все устройства, присутствующие в таблице, считаются известными приложению.

Чтобы просмотреть таблицу устройств:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.

2. Перейдите на вкладку **Устройства**.

   Отобразится таблица устройств.

В таблице отображаются следующие данные:

- **Имя** – имя, под которым устройство представлено в приложении.
- **ID устройства** – идентификатор устройства, присвоенный в Kaspersky Anti Targeted Attack Platform.
- **Статус** – статус устройства, определяющий разрешение активности устройства в корпоративной сети. Устройство может иметь один из следующих статусов:
  - **Разрешенное**. Этот статус присваивается устройству, которому разрешена активность в сети.
  - **Неразрешенное**. Этот статус присваивается устройству, которому не разрешена активность в сети.
  - **Неиспользуемое**. Этот статус присваивается устройству, если оно больше не используется или не должно использоваться в сети, либо если устройство длительное время не проявляло активность и не изменялись сведения об этом устройстве (30 дней и более).
- **Адресная информация** – MAC- и/или IP-адреса устройства. Если устройство имеет несколько сетевых интерфейсов, для него могут быть указаны различные MAC- и/или IP-адреса устройства на различных сетевых интерфейсах.
- **Категория** – название категории, определяющей функциональное назначение устройства. В Kaspersky Anti Targeted Attack Platform предусмотрены следующие категории устройств:
  - **Сервер** – компьютер, на котором развернуто серверное ПО.
  - **Сетевое устройство**– устройства, относящиеся к сетевому оборудованию (например, маршрутизаторы, коммутаторы).
  - **Рабочая станция** – стационарные персональные компьютеры или рабочие станции операторов.
  - **Мобильное устройство** – портативные электронные устройства с функциями компьютера.
  - **Ноутбук** – переносные персональные компьютеры.
  - **Принтер** – печатающие устройства.
  - **ИБП** – блоки бесперебойного питания, подключаемые к вычислительной сети.
  - **Сетевая камера** – устройства, выполняющие функции видеонаблюдения и передачи изображения в цифровом виде.
  - **Шлюз** – устройства для сопряжения сетей, преобразующие различные интерфейсы (например, Serial/Ethernet) в сетях с разнородной средой передачи данных и разными протоколами.
  - **Система хранения** – устройства для хранения информации внутри систем памяти.
  - **Брандмауэр** – устройства, выполняющие функции сетевого экрана для проверки и блокировки нежелательного трафика.
  - **Коммутатор** – устройства для физического соединения узлов локальной сети.
  - **Виртуальный коммутатор** – устройства, логически объединяющие физические коммутаторы, или программно реализованные коммутаторы для систем виртуализации.

- **Маршрутизатор** – устройства, выполняющие функции перенаправления сетевых пакетов между сегментами вычислительной сети.
- **Виртуальный маршрутизатор** – устройства, логически объединяющие физические маршрутизаторы, или маршрутизаторы, использующие несколько независимых таблиц маршрутизации.
- **Wi-Fi** – точки доступа, обеспечивающие беспроводное подключение устройств из сетей Wi-Fi.
- **Сервер Historian** – серверы архивных данных.
- **Другое** – устройства, не относящиеся к вышеперечисленным категориям.

- **Группа** – имя группы, в которую помещено устройство в дереве групп устройств (содержит имя самой группы и имена всех ее родительских групп).
- **Состояние безопасности** – состояние безопасности устройства, определяемое по наличию связанных с устройством событий. Предусмотрены следующие состояния безопасности:
  - **Критическое**. С устройством связаны события со значением оценки критичности в диапазоне 8.0–10.0.
  - **Важное**. С устройством связаны события со значением оценки критичности в диапазоне 4.0–7.9.
  - **ОК**. С устройством связаны события со значением оценки критичности в диапазоне 0.0–3.9, или у устройства нет связанных событий.
- **Значимость** – значимость устройства. Значимость присваивается устройству в соответствии с его категорией. Предусмотрены следующие значимости устройств:
  - **Высокая**. Присваивается устройствам категории **Сервер**.
  - **Средняя**. Присваивается устройствам категории **Сетевое устройство**, **Рабочая станция**, **Шлюз**, **Система хранения**, **Брандмауэр**, **Коммутатор**, **Виртуальный коммутатор**, **Маршрутизатор**, **Виртуальный маршрутизатор**, **Wi-Fi** или **Сервер Historian**.
  - **Низкая**. Присваивается устройствам категории **Мобильное устройство**, **Ноутбук**, **Принтер**, **ИБП**, **Сетевая камера** или **Другое**.
- **Последнее появление** – дата и время последней зафиксированной активности устройства.
- **Риски** – категории рисков, обнаруженных для устройства. По умолчанию в таблице устройств отображается информация только по актуальным рискам. Для отображения информации по всем рискам можно установить флажок **Отображать устраненные и принятые риски** при настройке таблицы устройств.
- **Последнее изменение** – дата и время последнего изменения сведений об устройстве.
- **Создано** – дата и время добавления устройства в таблицу устройств.
- **ОС** – название операционной системы, установленной на устройстве.
- **Производитель аппаратной части** – название производителя аппаратного обеспечения устройства. В области деталей этот параметр называется **Производитель** и отображается на вкладке **Общие** в блоке параметров **Аппаратное обеспечение**.
- **Модель аппаратной части** – название модели устройства. В области деталей этот параметр называется **Модель** и отображается на вкладке **Общие** в блоке параметров **Аппаратное обеспечение**.

- **Версия аппаратной части** – номер версии аппаратного обеспечения устройства. В области деталей этот параметр называется **Версия** и отображается на вкладке **Общие** в блоке параметров **Аппаратное обеспечение**.
- **Производитель ПО** – название производителя программного обеспечения устройства. В области деталей этот параметр называется **Производитель** и отображается на вкладке **Общие** в блоке параметров **Программное обеспечение**.
- **Название ПО** – название программного обеспечения устройства. В области деталей этот параметр называется **Название** и отображается на вкладке **Общие** в блоке параметров **Программное обеспечение**.
- **Версия ПО** – номер версии программного обеспечения устройства. В области деталей этот параметр называется **Версия** и отображается на вкладке **Общие** в блоке параметров **Программное обеспечение**.
- **Сетевое имя** – имя, под которым устройство представлено в сети.
- **Метки** – список меток, назначенных устройству.
- **Приложение EPP** – краткое название EPP-приложения, установленного на устройстве (если данные от этого приложения поступали в Kaspersky Anti Targeted Attack Platform).
- **Подключение EPP** – статус подключения компонента Endpoint Agent, установленного на устройстве, к серверу интеграции. Предусмотрены следующие статусы:
  - **Активное**. Со времени последнего соединения приложения с сервером интеграции прошло менее суток.
  - **Неактивное**. Со времени последнего соединения приложения с сервером интеграции прошло более суток.
  - **Отсутствует**. Статус подключения неизвестен.
- **Последнее соединение с EPP** – дата последнего подключения компонента Endpoint Agent к серверу интеграции.

Просмотр информации об устройстве

Чтобы просмотреть информацию об устройстве:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Устройства**.
3. Выберите устройство, информацию о котором вы хотите просмотреть.

Откроется окно с информацией об устройстве.

Окно может содержать следующую информацию:

- Сведения об устройстве:
  - **Состояние безопасности** – состояние безопасности устройства, определяемое по наличию связанных с устройством событий. Предусмотрены следующие состояния безопасности:
    - **Критическое**. С устройством связаны события со значением оценки критичности в диапазоне 8.0–10.0.
    - **Важное**. С устройством связаны события со значением оценки критичности в диапазоне 4.0–7.9.
    - **OK**. С устройством связаны события со значением оценки критичности в диапазоне 0.0–3.9, или у устройства нет связанных событий.
  - **Значимость** – значимость устройства для предприятия. Значимость присваивается устройству в соответствии с его категорией. Предусмотрены следующие значимости устройств:
    - **Высокая**. Присваивается устройствам категории **Сервер**.
    - **Средняя**. Присваивается устройствам категории **Сетевое устройство**, **Рабочая станция**, **Шлюз**, **Система хранения**, **Брандмауэр**, **Коммутатор**, **Виртуальный коммутатор**, **Маршрутизатор**, **Виртуальный маршрутизатор**, **Wi-Fi** или **Сервер Historian**.
    - **Низкая**. Присваивается устройствам категории **Мобильное устройство**, **Ноутбук**, **Принтер**, **ИБП**, **Сетевая камера** или **Другое**.
  - **Статус** – статус устройства, определяющий разрешение активности устройства в корпоративной сети. Устройство может иметь один из следующих статусов:
    - **Разрешенное**. Этот статус присваивается устройству, которому разрешена активность в сети.
    - **Неразрешенное**. Этот статус присваивается устройству, которому не разрешена активность в сети.
    - **Неиспользуемое**. Этот статус присваивается устройству, если оно больше не используется или не должно использоваться в сети, либо если устройство длительное время не проявляло активность и не изменялись сведения об этом устройстве (30 дней и более).
  - **Категория** – название категории, определяющей функциональное назначение устройства.
  - **Сетевое имя** – имя, под которым устройство представлено в сети.
  - **Группа** – имя группы, в которую помещено устройство в дереве групп устройств (содержит имя самой группы и имена всех ее родительских групп).
- Вкладка **Основное**:
  - **Создано** – дата и время добавления устройства в таблицу устройств.
  - **Последнее изменение** – дата и время последнего изменения сведений об устройстве.
  - **Последнее появление** – дата и время последней зафиксированной активности устройства.

- **Адресная информация** – MAC- и/или IP-адреса устройства. Если устройство имеет несколько сетевых интерфейсов, для него могут быть указаны различные MAC- и/или IP-адреса устройства на различных сетевых интерфейсах.

- **Аппаратное обеспечение** – сведения об аппаратных характеристиках устройства.

- **Программное обеспечение** – сведения о программном обеспечении устройства.

- **Endpoint Agent** – сведения о работе компонента Endpoint Agent. Раздел отображается, если на устройстве установлен компонент Endpoint Agent.

- **Приложение EPP** – сведения о приложении, которое выступает в роли компонента Endpoint Agent.

- **Маршрутизирующее устройство** – признак маршрутизирующего устройства.

  Если признак маршрутизирующего устройства не был определен приложением автоматически, то его требуется выставить вручную. Этот признак позволяет приложению использовать дополнительные алгоритмы обнаружения устройств, взаимодействующих между собой через маршрутизирующее устройство.

- **Открытый ключ** – открытый ключ для проверки устройства перед установкой SSH-соединения и сканирования устройства в рамках заданий аудита безопасности.

- **Доп. сведения** – дополнительные сведения об устройстве, заданные пользователем приложения (например, описание размещения устройства).

- **Пользовательские поля** – набор нестандартных сведений об устройстве, заданных пользователем приложения (например, категории и классы защиты устройства). Для устройства может быть указано до 16 пользовательских полей.

- **Динамические поля** – набор расширенных сведений об устройстве, обнаруженных в трафике при работе метода обнаружения сведений об устройствах. Поле отображается, если расширенные сведения были обнаружены приложением.

- Вкладка **Адреса**:

  - **DHCP-сервер** – признак DHCP-сервера.

    В поле отображается **Да**, если устройству присвоен признак DHCP-сервера.

  - **DHCP-ретранслятор** – признак DHCP-ретранслятора.

    В поле отображается **Да**, если устройству присвоен признак DHCP-ретранслятора.

  - **Сетевой интерфейс <номер>** – сведения о сетевом интерфейсе устройства.

- **Параметры топологии** – вкладка, содержащая сведения о последнем активном опросе устройства, а также сведения о соединениях устройства с другими узлами.

- **Оборудование** – вкладка, содержащая сведения о BIOS-программах и процессорах устройства, сведения об объемах свободной оперативной памяти и памяти на локальных дисках устройства, а также сведения об используемых USB-устройствах и оптических приводах. Сведения отображаются, если они были получены при использовании функциональности контроля оборудования.

- **Конфигурации** – вкладка, содержащая сведения о полученных конфигурациях устройства. Сведения отображаются, если они были получены по результатам выполнения заданий контроля конфигураций.

Автоматическое добавление и обновление устройств

Приложение может автоматически добавлять устройства в таблицу и обновлять сведения об устройствах. Для автоматического добавления и обновления устройств в Kaspersky Anti Targeted Attack Platform требуется включить и настроить технологию Обнаружение активов (AM). Если технология включена, приложение добавляет и обновляет сведения об устройствах за счет данных, полученных из трафика сети и при интеграции с компонентом Endpoint Agent.

При добавлении устройства приложение по умолчанию задает имя устройства по шаблону: **Устройство <значение внутреннего счетчика устройств>**. При этом значение внутреннего счетчика в имени устройства может не совпадать с идентификатором устройства, который отображается в столбце **ID устройства**.

Приложение может автоматически обновлять сведения, относящиеся к производителям сетевого оборудования устройств, на основе MAC-адресов устройств. Для определения производителей по MAC-адресам приложение сверяет MAC-адреса устройств с диапазонами адресов, которые были зарегистрированы в открытой базе данных международной организации Institute of Electrical and Electronics Engineers (IEEE). Если производитель сетевого оборудования определен по MAC-адресу, то в качестве названия производителя приложение сохраняет такое же название, какое представлено в базе данных IEEE.

После установки приложения используется копия базы данных IEEE, содержащая сведения о MAC-адресах и производителях на момент выпуска текущей версии приложения. Вы можете поддерживать локальную копию базы данных IEEE в актуальном состоянии, устанавливая обновления.

Добавление устройств вручную

Этот раздел содержит инструкции по добавлению устройств вручную. Вы можете вручную добавить новое устройство в таблицу устройств. Для добавляемого устройства требуется указать MAC- и/или IP-адрес.

MAC- и IP-адреса добавленного устройства должны быть уникальны в пределах адресного пространства, к которому относятся эти адреса. Если в приложение добавлены дополнительные адресные пространства, вы можете добавлять устройства с одинаковыми адресами в разные адресные пространства.

Добавлять устройства вручную могут только пользователи с ролью **Старший сотрудник службы безопасности**.

После добавления устройства вы можете добавить параметры контроля процесса для устройства.

Добавление устройства при работе с таблицей устройств

Чтобы добавить устройство при работе с таблицей устройств:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.

2. В таблице устройств на вкладке **Устройства** выберите устройство, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об устройстве.

3. Нажмите на кнопку **Добавить устройство**.

4. На вкладке **Параметры** в области деталей укажите нужные значения в полях, определяющих сведения об устройстве.

5. На вкладке **Адресная информация** в области деталей выполните следующие действия:

   a. В раскрывающемся списке **DHCP-сервер** выберите значение **Да**, если устройство является DHCP-сервером.

   b. В раскрывающемся списке **DHCP-ретранслятор** выберите значение **Да**, если устройство является DHCP-ретранслятором.

      В режиме обучения для устройств, которые являются DHCP-серверами и DHCP-ретрансляторами эти признаки проставляются автоматически. Вы можете отключить автоматическое обновление признаков (см. шаг 6 этой инструкции).

      В режиме наблюдения редактирование признаков доступно только пользователям с ролью **Старший сотрудник службы безопасности**.

   c. В раскрывающемся списке **Адресное пространство** выберите адресное пространство, которому будет принадлежать устройство.

   d. В поле **MAC-адрес** введите MAC-адрес устройства.

   e. В поле **IP-адрес** в раскрывающемся списке выберите тип назначения IP-адреса: статический или динамический, и введите IP-адрес устройства.

      Вы можете указать несколько IP-адресов для одного сетевого интерфейса устройства. Для формирования списка IP-адресов выполните одно из следующих действий:

      - Если вы хотите добавить IP-адрес, нажмите на кнопку **Добавить IP-адрес**.
      - Если вы хотите удалить IP-адрес, нажмите на значок , который расположен справа от поля со значением IP-адреса.

Если устройство имеет несколько сетевых интерфейсов, сформируйте список сетевых интерфейсов устройства:

- Если вы хотите добавить сетевой интерфейс, нажмите на кнопку **Добавить интерфейс**, которая расположена под группой параметров последнего сетевого интерфейса устройства.
- Если вы хотите удалить сетевой интерфейс, нажмите на значок ×, который расположен справа от названия сетевого интерфейса устройства (при наличии двух и более сетевых интерфейсов).
- Если вы хотите задать другое имя для сетевого интерфейса, нажмите на значок ✎, который расположен справа от текущего имени, и введите новое имя сетевого интерфейса в появившемся поле.

6. На вкладках **Параметры** и **Адресная информация** в области деталей включите или выключите автоматическое изменение для нужных сведений об устройстве. Для этого используйте значки 🔒 и 🔓.

   При отключении автоматического обновления IP-адреса устройства, также отключается автоматическое обновление типа IP-адреса (статический или динамический) и обновление сведений об адресном пространстве.

7. На вкладке **Пользовательские поля** в области деталей при необходимости сформируйте список пользовательских полей.

8. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком ●.

В таблице устройств появится новое устройство со статусом *Разрешенное*.

Добавление устройства при работе с топологической картой

При работе с топологической картой вы можете добавить новое устройство в таблицу устройств.

Чтобы добавить новое устройство в таблицу устройств при работе с топологической картой:

1. В окне веб-интерфейса приложения выберите раздел **Карта сети**.
2. Перейдите на вкладку **Топологическая карта**.
3. Нажмите на кнопку **Добавить устройство**.
4. На вкладке **Параметры** в области деталей укажите нужные значения в полях, определяющих сведения об устройстве.
5. На вкладке **Адресная информация** в области деталей выполните следующие действия:
   a. В раскрывающемся списке **DHCP-сервер** выберите значение **Да**, если устройство является DHCP-сервером.
   b. В раскрывающемся списке **DHCP-ретранслятор** выберите значение **Да**, если устройство является DHCP-ретранслятором.

В режиме обучения для устройств, которые являются DHCP-серверами и DHCP-ретрансляторами эти признаки проставляются автоматически. Вы можете отключить автоматическое обновление признаков (см. шаг 6 этой инструкции).

В режиме наблюдения редактирование признаков доступно только пользователям с ролью **Старший сотрудник службы безопасности**.

c. В раскрывающемся списке **Адресное пространство** выберите адресное пространство, которому будет принадлежать устройство.

d. В поле **MAC-адрес** введите MAC-адрес устройства.

e. В поле **IP-адрес** в раскрывающемся списке выберите тип назначения IP-адреса: статический или динамический, и введите IP-адрес устройства.

Вы можете указать несколько IP-адресов для одного сетевого интерфейса устройства. Для формирования списка IP-адресов выполните одно из следующих действий:

- Если вы хотите добавить IP-адрес, нажмите на кнопку **Добавить IP-адрес**.
- Если вы хотите удалить IP-адрес, нажмите на значок , который расположен справа от поля со значением IP-адреса.

Если устройство имеет несколько сетевых интерфейсов, сформируйте список сетевых интерфейсов устройства:

- Если вы хотите добавить сетевой интерфейс, нажмите на кнопку **Добавить интерфейс**, которая расположена под группой параметров последнего сетевого интерфейса устройства.
- Если вы хотите удалить сетевой интерфейс, нажмите на значок , который расположен справа от названия сетевого интерфейса устройства (при наличии двух и более сетевых интерфейсов).
- Если вы хотите задать другое имя для сетевого интерфейса, нажмите на значок , который расположен справа от текущего имени, и введите новое имя сетевого интерфейса в появившемся поле.

6. На вкладках **Параметры** и **Адресная информация** в области деталей включите или выключите автоматическое изменение для нужных сведений об устройстве. Для этого используйте значки и .

> При отключении автоматического обновления IP-адреса устройства, также отключается автоматическое обновление типа IP-адреса (статический или динамический) и обновление сведений об адресном пространстве.

7. На вкладке **Пользовательские поля** в области деталей при необходимости сформируйте список пользовательских полей.

8. Нажмите на кнопку **Сохранить**.

Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком .

В таблице устройств появится новое устройство со статусом *Разрешенное*.

Добавление устройства на основе узла неизвестного устройства на карте сетевых взаимодействий

При работе с картой сетевых взаимодействий вы можете добавить новое устройство в таблицу устройств на основе узла, который представляет неизвестное приложению устройство.

Чтобы добавить узел неизвестного устройства в таблицу устройств:

1. В окне веб-интерфейса приложения выберите раздел **Карта сети.**

2. На вкладке **Карта сетевых взаимодействий** выберите узел, представляющий неизвестное приложению устройство.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Добавить в таблицу устройств**.

4. На вкладке **Параметры** в области деталей укажите нужные значения в полях, определяющих сведения об устройстве.

5. На вкладке **Адресная информация** в области деталей выполните следующие действия:

   a. В раскрывающемся списке **DHCP-сервер** выберите значение **Да**, если устройство является DHCP-сервером.

   b. В раскрывающемся списке **DHCP-ретранслятор** выберите значение **Да**, если устройство является DHCP-ретранслятором.

      В режиме обучения для устройств, которые являются DHCP-серверами и DHCP-ретрансляторами эти признаки проставляются автоматически. Вы можете отключить автоматическое обновление признаков (см. шаг 6 этой инструкции).

      В режиме наблюдения редактирование признаков доступно только пользователям с ролью **Старший сотрудник службы безопасности**.

   c. В раскрывающемся списке **Адресное пространство** выберите адресное пространство, которому будет принадлежать устройство.

   d. Поля **IP-адрес** и **MAC-адрес** заполняются автоматически, менять их значение не рекомендуется.

      Вы можете указать несколько IP-адресов для одного сетевого интерфейса устройства. Для формирования списка IP-адресов выполните одно из следующих действий:

      - Если вы хотите добавить IP-адрес, нажмите на кнопку **Добавить IP-адрес**.

      - Если вы хотите удалить IP-адрес, нажмите на значок , который расположен справа от поля со значением IP-адреса.

Если устройство имеет несколько сетевых интерфейсов, сформируйте список сетевых интерфейсов устройства:

- Если вы хотите добавить сетевой интерфейс, нажмите на кнопку **Добавить интерфейс**, которая расположена под группой параметров последнего сетевого интерфейса устройства.
- Если вы хотите удалить сетевой интерфейс, нажмите на значок ×, который расположен справа от названия сетевого интерфейса устройства (при наличии двух и более сетевых интерфейсов).
- Если вы хотите задать другое имя для сетевого интерфейса, нажмите на значок ✎, который расположен справа от текущего имени, и введите новое имя сетевого интерфейса в появившемся поле.

6. На вкладках **Параметры** и **Адресная информация** в области деталей включите или выключите автоматическое изменение для нужных сведений об устройстве. Для этого используйте значки 🔒 и 🔓.

   При отключении автоматического обновления IP-адреса устройства, также отключается автоматическое обновление типа IP-адреса (статический или динамический) и обновление сведений об адресном пространстве.

7. На вкладке **Пользовательские поля** в области деталей при необходимости сформируйте список пользовательских полей.

8. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком ●.

В таблице устройств появится новое устройство со статусом *Разрешенное*. Узел на карте сетевых взаимодействий, который ранее представлял неизвестное приложению устройство, будет представлять известное приложению устройство.

Добавление устройства на основе неуправляемого коммутатора на топологической карте

При работе с топологической картой вы можете добавить новое устройство в таблицу устройств на основе узла, который представляет неуправляемый коммутатор.

Чтобы добавить узел неуправляемого коммутатора в таблицу устройств:

1. В окне веб-интерфейса приложения выберите раздел **Карта сети.**

2. На вкладке **Карта сетевых взаимодействий** выберите узел, представляющий неуправляемый коммутатор.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Добавить в таблицу устройств**.

4. На вкладке **Параметры** в области деталей укажите нужные значения в полях, определяющих сведения об устройстве.

5. На вкладке **Адресная информация** в области деталей выполните следующие действия:

   a. В раскрывающемся списке **DHCP-сервер** выберите значение **Да**, если устройство является DHCP-сервером.

   b. В раскрывающемся списке **DHCP-ретранслятор** выберите значение **Да**, если устройство является DHCP-ретранслятором.

      В режиме обучения для устройств, которые являются DHCP-серверами и DHCP-ретрансляторами эти признаки проставляются автоматически. Вы можете отключить автоматическое обновление признаков (см. шаг 6 этой инструкции).

      В режиме наблюдения редактирование признаков доступно только пользователям с ролью **Старший сотрудник службы безопасности**.

   c. В раскрывающемся списке **Адресное пространство** выберите адресное пространство, которому будет принадлежать устройство.

   d. В поле **MAC-адрес** введите MAC-адрес устройства.

   e. В поле **IP-адрес** в раскрывающемся списке выберите тип назначения IP-адреса: статический или динамический, и введите IP-адрес устройства.

      Вы можете указать несколько IP-адресов для одного сетевого интерфейса устройства. Для формирования списка IP-адресов выполните одно из следующих действий:

      - Если вы хотите добавить IP-адрес, нажмите на кнопку **Добавить IP-адрес**.
      - Если вы хотите удалить IP-адрес, нажмите на значок , который расположен справа от поля со значением IP-адреса.

      Если устройство имеет несколько сетевых интерфейсов, сформируйте список сетевых интерфейсов устройства:

      - Если вы хотите добавить сетевой интерфейс, нажмите на кнопку **Добавить интерфейс**, которая расположена под группой параметров последнего сетевого интерфейса устройства.
      - Если вы хотите удалить сетевой интерфейс, нажмите на значок , который расположен справа от названия сетевого интерфейса устройства (при наличии двух и более сетевых интерфейсов).
      - Если вы хотите задать другое имя для сетевого интерфейса, нажмите на значок , который расположен справа от текущего имени, и введите новое имя сетевого интерфейса в появившемся поле.

6. На вкладках **Параметры** и **Адресная информация** в области деталей включите или выключите автоматическое изменение для нужных сведений об устройстве. Для этого используйте значки и .

   При отключении автоматического обновления IP-адреса устройства, также отключается автоматическое обновление типа IP-адреса (статический или динамический) и обновление сведений об адресном пространстве.

7. На вкладке **Пользовательские поля** в области деталей при необходимости сформируйте список пользовательских полей.

8. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком .

В таблице устройств появится новое устройство со статусом *Разрешенное*. Узел на топологической карте, который ранее представлял неуправляемый коммутатор, будет представлять известное приложению устройство.

Автоматическое присвоение статусов устройств

При отслеживании активности устройств приложение может автоматически присваивать статусы обнаруженным устройствам по полученным MAC- и/или IP-адресам устройств. Статусы присваиваются в зависимости от текущего режима контроля активов.

В режиме обучения приложение присваивает статус *Разрешенное* всем устройствам (как новым, так и ранее добавленным в таблицу), кроме тех устройств, которым ранее был присвоен статус *Неразрешенное*.

В режиме наблюдения присваиваемый статус зависит от того, является ли устройство, проявившее активность, известным или неизвестным приложению. В этом режиме присвоение статусов происходит по следующим правилам:

- Если устройство является новым (отсутствовало в таблице устройств на момент обнаружения), этому устройству присваивается статус *Неразрешенное*.
- Если устройство присутствует в таблице устройств со статусом *Разрешенное* или *Неразрешенное*, статус не меняется.
- Если устройство присутствует в таблице устройств со статусом *Неиспользуемое*, этому устройству присваивается статус *Неразрешенное*.

По умолчанию если устройство со статусом *Разрешенное* не проявляет активность более 30 дней и за это время не изменялись сведения об устройстве, этому устройству автоматически присваивается статус *Неиспользуемое*. Вы можете выключить автоматическое изменение статуса устройства на статус *Неиспользуемое* при изменении статуса устройства вручную (например, чтобы статус *Разрешенное* не изменялся на статус *Неразрешенное* для редко подключаемого устройства).

При использовании коннекторов типа **Cisco Switch** может происходить автоматическое ограничение сетевого доступа устройств после присвоения этим устройствам статуса *Неразрешенное* вам нужно учитывать заданные параметры коннекторов этого типа, чтобы не допустить блокировку нужных устройств из-за изменения их статуса.

Автоматическая группировка устройств по заданному критерию

Этот раздел содержит инструкции по автоматической группировке устройств по заданному критерию. Вы можете автоматически группировать устройства в дереве групп устройств по одному из следующих критериев:

- принадлежность IP-адресов известным приложению подсетям;
- категории устройств;
- производители устройств.

Выполнять автоматическую группировку устройств могут только пользователи с ролью **Старший сотрудник службы безопасности**.

Автоматическая группировка устройств по заданному критерию, начиная с верхнего уровня иерархии в дереве групп

Чтобы сгруппировать устройства автоматически по заданному критерию, начиная с верхнего уровня иерархии в дереве групп:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** нажмите на одну из следующих кнопок выбора критерия группировки в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий:
   - – для группировки устройств по подсетям;
   - – для группировки устройств по категориям;
   - – для группировки устройств по производителям.

   Откроется окно запроса для выбора варианта группировки.
3. Если требуется группировать устройства по категориям и производителям с учетом адресных пространств, в окне запроса установите флажок **Учитывать адресные пространства**.

4. Нажмите на одну из следующих кнопок в зависимости от нужного результата:

   - Если вы хотите сгруппировать устройства по подсетям, нажмите на кнопку **Сгруппировать**.
   - Если вы хотите сгруппировать устройства с учетом адресных пространств по категориям или производителям во всех группах дерева групп устройств, нажмите на кнопку **Вместе с дочерними**.
   - Если вы хотите сгруппировать устройства с учетом адресных пространств по категориям или производителям только на верхнем уровне иерархии дерева групп устройств, нажмите на кнопку **Только выбранную группу**.

   Приложение определит устройства, подходящие под выбранный критерий группировки, создаст группы для этих устройств и поместит устройства в эти группы.

Автоматическая группировка устройств в выбранной группе устройств

Чтобы сгруппировать устройства автоматически в выбранной группе устройств:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** выберите группу, в которой вы хотите автоматически сгруппировать устройства.
3. По правой кнопке мыши откройте контекстное меню.
4. В контекстном меню выберите один из следующих пунктов:

   - **Сгруппировать по подсетям**.
   - **Сгруппировать по категориям**.
   - **Сгруппировать по производителям**.

   Откроется окно запроса для выбора варианта группировки.

5. Если требуется группировать устройства по категориям и производителям с учетом адресных пространств, в окне запроса установите флажок **Учитывать адресные пространства**.
6. В окне запроса нажмите на одну из следующих кнопок в зависимости от нужного результата:

   - Если вы хотите сгруппировать устройства по подсетям, нажмите на кнопку **Сгруппировать**.
   - Если вы хотите сгруппировать устройства по категориям или производителям во всех дочерних группах выбранной группы, нажмите на кнопку **Вместе с дочерними**.
   - Если вы хотите сгруппировать устройства по категориям или производителям только в выбранной группе, нажмите на кнопку **Только выбранную группу**.

   Приложение определит устройства, подходящие под выбранный критерий группировки, создаст группы для этих устройств и поместит устройства в эти группы (при этом устройства в других группах не будут распределены по новым группам).

Распределение устройств по группам вручную

Этот раздел содержит инструкции по управлению размещением устройств в дереве групп вручную. Управлять размещением устройств в дереве групп могут только пользователи с ролью Старший сотрудник службы безопасности.

Включение одного устройства в группу

Чтобы включить одно устройство в группу при работе с таблицей:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите устройство в разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети**.

   В разделе **Карта сети** вы можете выбрать устройство для добавления в группу как на карте сетевых взаимодействий, так и на топологической карте.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.
4. В области деталей перейдите на вкладку **Параметры**.
5. Нажмите на значок в правой части поля **Группа**.

   Появится окно **Выбор группы в дереве**.
6. В дереве групп устройств выберите нужную группу.

   Если нужная группа отсутствует в дереве, вы можете ее добавить в текущем открытом окне **Выбор группы в дереве**.
7. Нажмите на кнопку **Выбрать**.

   Путь к выбранной группе появится в поле **Группа**.
8. Нажмите на кнопку **Сохранить** в области деталей.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком .

Включение нескольких устройств в группу

Вы можете включить в группу несколько устройств при работе с таблицей устройств.

Также при работе с картой сетевых взаимодействий вы можете включить в группу несколько известных приложению устройств, представленных серверами с компонентами на карте сетевых взаимодействий. Вы можете выбирать нужные серверы с компонентами как по отдельности, так и в составе свернутых групп, включающих нужные устройства. При выборе свернутой группы в выборку устройств также попадают все устройства в дочерних группах любого уровня вложенности.

Чтобы включить несколько устройств в группу при работе с таблицей:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Устройства** выберите устройства, которые вы хотите включить в группу.
4. По правой кнопке мыши откройте контекстное меню.
5. В контекстном меню выберите пункт **Управление группами → Переместить в группу**.

   Появится окно **Выбор группы в дереве**.
6. В дереве групп устройств выберите нужную группу.

   Если нужная группа отсутствует в дереве, вы можете ее добавить в текущем открытом окне **Выбор группы в дереве**.
7. Нажмите на кнопку **Выбрать**.

   Путь к выбранной группе появится в столбце **Группа**.

Чтобы включить несколько устройств в группу при работе с картой сетевых взаимодействий:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Сотрудник службы безопасности или Старший сотрудник службы безопасности.
2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** выберите нужные серверы с компонентами известных приложению устройств и/или свернутые группы.

   Для выбора нескольких серверов с компонентами и/или групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.
3. По правой кнопке мыши откройте контекстное меню.
4. В контекстном меню выберите пункт **Переместить в группу**.

   Появится окно **Выбор группы в дереве**.
5. В дереве групп устройств выберите нужную группу.

   Если нужная группа отсутствует в дереве, вы можете ее добавить в текущем открытом окне **Выбор группы в дереве**.
6. Нажмите на кнопку **Выбрать**.

   Выбранные серверы с компонентами, представляющие известные приложению устройства, отобразятся внутри выбранной группы.

Исключение одного устройства из группы

Чтобы исключить одно устройство из группы при работе с таблицей:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите устройство в разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети**.

   В разделе **Карта сети** вы можете выбрать устройства для исключения из группы как на карте сетевых взаимодействий, так и на топологической карте.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.
4. В области деталей перейдите на вкладку **Параметры**.
5. В поле **Группа** удалите путь к группе с помощью значка × в поле (значок отображается, если группа задана).
6. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком .

После сохранения изменений для устройства очистится параметр **Группа** и устройство будет относиться к верхнему уровню иерархии в дереве групп.

Исключение нескольких устройств из групп

Вы можете исключить из групп несколько устройств при работе с таблицей устройств. Устройства, выбранные для исключения из групп, могут быть включены как в одну и ту же группу, так и в разные группы.

Также при работе с картой сетевых взаимодействий вы можете исключить из групп несколько известных приложению устройств, представленных серверами с компонентами на карте сетевых взаимодействий. Вы можете выбирать нужные серверы с компонентами как по отдельности, так и в составе свернутых групп, включающих нужные устройства. При выборе свернутой группы в выборку устройств также попадают все устройства в дочерних группах любого уровня вложенности.

Чтобы исключить несколько устройств из групп при работе с таблицей:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Устройства** выберите устройства, которые вы хотите исключить из групп.
4. По правой кнопке мыши откройте контекстное меню.

5. В контекстном меню выберите пункт **Управление группами → Исключить из групп**.

   Откроется окно с запросом подтверждения.

6. В окне запроса подтвердите исключение устройств из групп.

Для всех выбранных устройств очистится параметр **Группа** и эти устройства будут относиться к верхнему уровню иерархии в дереве групп.

Чтобы исключить несколько устройств из групп при работе с картой сетевых взаимодействий:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Сотрудник службы безопасности или Старший сотрудник службы безопасности.
2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** выберите серверы с компонентами в развернутых группах и/или свернутые группы.

   Для выбора нескольких серверов с компонентами и/или групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

3. По правой кнопке мыши откройте контекстное меню.
4. В контекстном меню выберите пункт **Исключить из групп**.

   Откроется окно с запросом подтверждения.

5. В окне запроса подтвердите исключение устройств из групп.

Для всех выбранных устройств очистится параметр **Группа** и эти устройства отобразятся вне групп.

Перемещение серверов с компонентами и групп в другие группы на карте сетевых взаимодействий

Вы можете изменять размещение серверов с компонентами и групп в дереве групп устройств, перетаскивая объекты на карте сетевых взаимодействий. После перемещения серверы с компонентами и группы изменяют свое размещение в дереве групп устройств так же, как при включении устройств в группу и исключении устройств из групп.

Перемещать серверы с компонентами и группы в другие группы могут только пользователи с ролью Старший сотрудник службы безопасности.

Чтобы переместить серверы с компонентами и/или группы в другие группы:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** выберите нужные серверы с компонентами известных приложению устройств и/или свернутые группы.

Для выбора нескольких серверов с компонентами и/или групп выполните одно из следующих действий:

- Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
- Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

3. Наведите курсор на один из выбранных объектов (группу или сервер с компонентом, представляющий известное приложению устройство).
4. Нажмите на клавишу **CTRL** и, удерживая ее нажатой, перетащите выбранные объекты в нужную группу (или в любое место вне групп, если вы хотите переместить выбранные объекты на верхний уровень иерархии в дереве групп).

   Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите перемещение выбранных объектов.

Дерево групп устройств

Дерево групп устройств предназначено для распределения устройств в соответствии с их назначением, размещением или по каким-либо другим произвольным признакам. Устройства могут быть распределены по группам вручную или автоматически (по принадлежности IP-адресов устройств подсетям, по категориям устройств или по производителям).

Если устройство не включено ни в одну из групп, это устройство считается относящимся к верхнему уровню иерархии в дереве групп. Устройства, автоматически добавленные в таблицу, по умолчанию не включаются в группы.

Узнать, в какие группы входят устройства, вы можете при просмотре таблицы устройств. Пути к группам указаны в столбце **Группа**. Группы устройств также отображаются и на карте сетевых взаимодействий, однако входящие в эти группы устройства могут не отображаться, если они не удовлетворяют параметрам фильтрации объектов на карте сетевых взаимодействий.

Формирование дерева групп устройств вручную

Вы можете формировать дерево групп устройств при работе с таблицей устройств, с картой сетевых взаимодействий и топологической картой. Функции для формирования дерева доступны в окне **Формирование дерева групп** или **Выбор группы в дереве**.

Формировать дерево групп устройств могут только пользователи с ролью Старший сотрудник службы безопасности.

Чтобы использовать функции для формирования дерева групп устройств:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. В разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети** выполните одно из следующих действий:

   - Откройте окно **Формирование дерева групп** по кнопке **Настроить группы**.

Кнопка **Настроить группы** в разделе **Активы** доступна в раскрывающемся списке **Управление группами** в панели инструментов.

Кнопка **Настроить группы** в разделе **Карта сети** доступна только на вкладке **Карта сетевых взаимодействий**.

- Откройте окно **Выбор группы в дереве**, выполняя добавление устройств в группы. Вы также можете открыть это окно при фильтрации таблицы устройств по столбцу **Группа**.

Изменения, сделанные в дереве групп устройств в окне **Формирование дерева групп** или **Выбор группы в дереве**, применяются сразу.

Этот раздел содержит инструкции по использовании функций для формирования дерева групп устройств.

Добавление группы

Чтобы добавить группу в дерево групп устройств:

1. В окне **Формирование дерева групп** или **Выбор группы в дереве** добавьте новую группу одним из следующих способов:

   - Если дерево пустое и вы хотите добавить первую группу, нажмите на кнопку **Добавить** или на любую из клавиш **INSERT** или **ENTER**.

   - Если вы хотите добавить группу на одном уровне иерархии с имеющейся группой, выберите эту группу и нажмите на клавишу **ENTER**.

   - Если вы хотите добавить дочернюю группу к имеющейся группе, выберите эту группу и нажмите на кнопку **Добавить** или на клавишу **INSERT**.

2. В поле ввода введите имя группы.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /`.

   Имя группы должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;

   - содержит до 255 символов;

   - не совпадает с именем другой группы из числа включенных в ту же родительскую группу (регистр символов не учитывается).

3. Нажмите на значок ✓ справа от поля ввода.

Переименование группы

Чтобы переименовать группу в дереве групп устройств:

1. В окне **Формирование дерева групп** или **Выбор группы в дереве** выберите группу, которую вы хотите переименовать.

2. Нажмите на кнопку **Переименовать** или на клавишу **F2**.

3. В поле ввода введите новое имя группы.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /`.

   Имя группы должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 255 символов;
   - не совпадает с именем другой группы из числа включенных в ту же родительскую группу (регистр символов не учитывается).

4. Нажмите на значок ✓ справа от поля ввода.

Новое имя группы появится в сведениях об устройствах, которые добавлены в эту группу или в ее дочерние группы.

Удаление групп

При удалении группы не удаляются устройства, добавленные в эту группу. Устройства из удаленной группы переводятся на тот же уровень иерархии в дереве устройств, на котором была удаленная группа.

Чтобы удалить группу в дереве групп устройств:

1. В окне **Формирование дерева групп** или **Выбор группы в дереве** выберите группу, которую вы хотите удалить.
2. Нажмите на значок 🗑.

   Откроется окно запроса для выбора варианта удаления.

3. В окне запроса нажмите на одну из следующих кнопок в зависимости от нужного результата:

   - Если вы хотите удалить только выбранную группу и оставить ее дочерние группы, нажмите на кнопку **Только выбранную**.
   - Если вы хотите удалить выбранную группу вместе со всеми ее дочерними группами, нажмите на кнопку **Вместе с дочерними**.

   Откроется окно с запросом подтверждения.

4. В окне запроса нажмите на кнопку **ОК**.

Перемещение группы

Чтобы переместить группу в дереве групп устройств:

1. В окне **Формирование дерева групп** или **Выбор группы в дереве** выберите группу, которую вы хотите переместить.

2. Используйте значки с изображением стрелок или соответствующие им комбинации клавиш **ALT+**↓, **ALT+**↑, **ALT+**←, **ALT+**→ для перемещения группы относительно других элементов дерева. Если невозможно выполнить какую-либо операцию, значок этой операции недоступен.

Поиск групп

Вы можете найти нужные группы в дереве групп устройств с помощью поля **Поиск групп** в окне **Формирование дерева групп** или **Выбор группы в дереве**. Группы, которые удовлетворяют условиям поиска, отобразятся в дереве групп устройств. Для групп, являющихся дочерними, также отображаются их родительские группы.

Обновление дерева

Состав групп в дереве групп устройств может быть изменен на Central Node в то время, когда вы работаете с деревом (например, другим пользователем, который выполнил подключение к Central Node).

Вы можете вручную обновлять дерево с помощью значка в окне **Формирование дерева групп** или **Выбор группы в дереве**.

Установка и удаление меток для устройств

Этот раздел содержит инструкции по установке и удалению меток для устройств. Вы можете присваивать устройствам произвольные метки.

Метка устройства содержит текстовое описание, которое позволяет быстро находить или фильтровать устройства в таблице. В качестве меток вы можете сохранять любые удобные вам текстовые описания. Для устройства можно назначить до 16 меток. При этом каждое устройство может иметь свой набор меток.

Списки меток устройств отображаются в таблице устройств в столбце **Метки**. Метки сортируются в ячейке в алфавитном порядке.

Устанавливать и удалять метки для устройств могут только пользователи с ролью Старший сотрудник службы безопасности.

Установка меток для одного устройства

Чтобы установить метку для одного устройства:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.

2. Выберите устройство в разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети**.

   В разделе **Карта сети** вы можете выбрать устройства для установки его метки как на карте сетевых взаимодействий, так и на топологической карте.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Изменить**.

   В области деталей перейдите на вкладку **Параметры**.

4. В поле **Метки** введите текстовые описания, которые вы хотите использовать в качестве меток. Для разделения меток вы можете использовать клавишу **ENTER** или символ **;**.

   Вы можете использовать прописные и строчные буквы, цифры, пробел, а также следующие специальные символы: **! @ # № $ % ^ & ( ) [ ] { } ' , . - _**.

   Имя метки должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - является уникальным в списке меток устройства (регистр символов не учитывается);
   - содержит от 1 до 255 символов.

5. При необходимости скопируйте список меток с помощью ссылки **Копировать метки**. Ссылка отображается, если список меток не пустой.

6. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком **.**.

Установка меток для нескольких устройств

Вы можете установить метки для нескольких устройств при работе с таблицей устройств.

Также при работе с картой сетевых взаимодействий и с топологической картой вы можете установить метки для известных приложению устройств, представленных узлами на картах. Вы можете выбирать нужные узлы как по отдельности, так и в составе свернутых групп, включающих нужные устройства. При выборе свернутой группы в выборку устройств также попадают все устройства в дочерних группах любого уровня вложенности.

Чтобы установить метки для нескольких устройств при работе с таблицей:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Устройства** выберите устройства, для которых вы хотите установить метки.
4. По правой кнопке мыши откройте контекстное меню одного из выбранных устройств.
5. В контекстном меню выберите пункт **Установить метки**.

   Появится окно **Добавление меток**.
6. В поле **Метки** введите текстовые описания, которые вы хотите использовать в качестве меток. Для разделения меток вы можете использовать клавишу **ENTER** или символ `;`.

   Вы можете использовать прописные и строчные буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   Имя метки должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - является уникальным в списке меток устройства (регистр символов не учитывается);
   - содержит от 1 до 255 символов.
7. При необходимости скопируйте список меток с помощью ссылки **Копировать метки**. Ссылка отображается, если список меток не пустой.
8. Если вы хотите очистить текущие списки меток для выбранных устройств и указать для этих устройств только новые метки, установите флажок **Удалить существующие**.

   Если снят флажок **Удалить существующие**, на каждом устройстве останется его текущий список меток. Списки меток на всех выбранных устройствах дополнятся новыми метками. В этом случае для некоторых из выбранных устройств суммарное количество меток может превысить ограничение (до 16 меток для каждого устройства). Приложение проверяет это ограничение перед добавлением новых меток.
9. Нажмите на кнопку **ОК**.

   Кнопка недоступна, если имена введенных меток не удовлетворяют требованиям или если список меток пустой и при этом снят флажок **Удалить существующие**.

Чтобы установить метки для нескольких устройств при работе с картами:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Карта сети**.
3. На вкладке **Карта сетевых взаимодействий** или **Топологическая карта** выберите нужные узлы известных приложению устройств и/или свернутые группы.

Для выбора нескольких узлов и/или групп выполните одно из следующих действий:

- Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
- Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

4. По правой кнопке мыши откройте контекстное меню одного из выбранных объектов.
5. В контекстном меню выберите пункт **Установить метки**.

   Появится окно **Добавление меток**.
6. В поле **Метки** введите текстовые описания, которые вы хотите использовать в качестве меток. Для разделения меток вы можете использовать клавишу **ENTER** или символ **;**.

   Вы можете использовать прописные и строчные буквы, цифры, пробел, а также следующие специальные символы: **! @ # № $ % ^ & ( ) [ ] { } ' , . - _**.

   Имя метки должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - является уникальным в списке меток устройства (регистр символов не учитывается);
   - содержит от 1 до 255 символов.
7. При необходимости скопируйте список меток с помощью ссылки **Копировать метки**. Ссылка отображается, если список меток не пустой.
8. Если вы хотите очистить текущие списки меток для выбранных устройств и указать для этих устройств только новые метки, установите флажок **Удалить существующие**.

   Если снят флажок **Удалить существующие**, на каждом устройстве останется его текущий список меток. Списки меток на всех выбранных устройствах дополнятся новыми метками. В этом случае для некоторых из выбранных устройств суммарное количество меток может превысить ограничение (до 16 меток для каждого устройства). Приложение проверяет это ограничение перед добавлением новых меток.
9. Нажмите на кнопку**OK**.

   Кнопка недоступна, если имена введенных меток не удовлетворяют требованиям или если список меток пустой и при этом снят флажок **Удалить существующие**.

Удаление меток для одного устройства

Чтобы удалить метку для одного устройства:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите устройство в разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети**.

   В разделе **Карта сети** вы можете выбрать устройства для удаления его метки как на карте сетевых взаимодействий, так и на топологической карте.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Изменить**.

   В области деталей перейдите на вкладку **Параметры**.

4. В поле **Метки** удалите лишние метки:

   - с помощью значка × рядом с названиями меток, если вы хотите удалить определенные метки;
   - с помощью значка × в правой части поля **Метки**, если вы хотите удалить все метки.

5. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком .

Очистка списков меток для нескольких устройств

Вы можете очистить списки меток для нескольких устройств при работе с таблицей устройств.

Также при работе с картой сетевых взаимодействий и с топологической картой вы можете очистить списки меток для известных приложению устройств, представленных узлами на картах. Вы можете выбирать нужные узлы как по отдельности, так и в составе свернутых групп, включающих нужные устройства. При выборе свернутой группы в выборку устройств также попадают все устройства в дочерних группах любого уровня вложенности.

Чтобы очистить списки меток для нескольких устройств при работе с таблицей:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Устройства** выберите устройства, для которых вы хотите очистить списки меток.
4. По правой кнопке мыши откройте контекстное меню одного из выбранных устройств.
5. В контекстном меню выберите пункт **Установить метки**.

   Появится окно **Добавление меток**.

6. Установите флажок **Удалить существующие**.
7. Нажмите на кнопку **ОК**.

Чтобы очистить списки меток для нескольких устройств при работе с картами:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Карта сети**.
3. На вкладке **Карта сетевых взаимодействий** или **Топологическая карта** выберите нужные узлы известных приложению устройств и/или свернутые группы.

Для выбора нескольких узлов и/или групп выполните одно из следующих действий:

- Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
- Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

4. По правой кнопке мыши откройте контекстное меню одного из выбранных объектов.
5. В контекстном меню выберите пункт **Установить метки**.

   Появится окно **Добавление меток**.
6. Установите флажок **Удалить существующие**.
7. Нажмите на кнопку **OK**.

Реагирование

Если вы используете функциональный блок KEDR, вы можете применять к устройствам действия по реагированию на обнаруженные угрозы путем создания задач. Список доступных в приложении действий по реагированию, а также параметры, необходимые для создания задач, приведены в таблице ниже.

Чтобы создать задачу для выполнения действия по реагированию:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Устройства**.
3. Установите флажок слева от имени устройства, на которое требуется назначить задачу.

   Если в списке очень много устройств, вы можете предварительно применить фильтры, чтобы отобразились устройства с нужными вам параметрами. Например, можно найти устройства с определенными метками или входящие в определенные группы.
4. В меню **Реагирование** выберите нужный вам тип задач.

   Откроется окно создания задачи.
5. Укажите параметры задачи в зависимости от ее типа.

   Список параметров приведен в таблице ниже.
6. Нажмите на кнопку **Сохранить**.

Задача будет создана. Задача запускается автоматически после создания.

Описание действий по реагированию и параметры для создания задач

Действие по реагированию	Параметры для создания задачи
Завершить процесс Завершение процесса, который может угрожать безопасности устройств или локальной сети организации.	• **Путь к файлу** – в зависимости от типа задачи, путь к файлу процесса, который вы хотите завершить или путь к файлу, который вы хотите удалить. Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае, в зависимости от типа задачи, для указанного потока данных будут завершены процессы или удалены файлы. Остальные потоки данных этого файла останутся без изменений. • **MD5/SHA256** – MD5-, SHA256-хеш файла процесса, который вы хотите остановить или файла, который вы хотите удалить. Поле не является обязательным. • **Описание** – описание задачи. Поле не является обязательным.

Действие по реагированию	Параметры для создания задачи
Удалить файл Удаление файла на указанных устройствах. Действие необратимо.	
Получить файл Копирование файла с устройства в Хранилище Kaspersky Anti Targeted Attack Platform с возможностью скачать файл на локальный компьютер. Задачу можно назначить только одному устройству.	• **Путь к файлу** – путь к файлу, который вы хотите получить. Если запрашиваемый файл связан с дополнительными потоками данных NTFS, в результате выполнения задачи вы получите все файлы потоков данных NTFS, с которыми связан запрашиваемый файл. Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае вы получите только файлы указанного потока. • **MD5/SHA256** – MD5-, SHA256-хеш файла, который вы хотите получить. Поле не является обязательным. • **Отправить на проверку** – проверка файла в Kaspersky Anti Targeted Attack Platform. • **Описание** – описание задачи. Поле не является обязательным.
Собрать форензику Получение списка файлов, процессов или точек автозапуска с указанных устройств в Хранилище Kaspersky Anti Targeted Attack Platform с возможностью скачать данные на локальный компьютер.	• **Тип информации** – тип собираемых данных. Доступны следующие типы: • **Список процессов** – список процессов, запущенных на хосте в момент выполнения задачи. • **Список точек автозапуска** – список точек автозапуска. В список точек автозапуска включаются данные о приложениях, добавленных в папку автозагрузки или зарегистрированных в разделах реестра Run, а также о приложениях, которые запускаются автоматически при загрузке хоста с компонентом Endpoint Agent и при входе пользователя в систему на указанных хостах. **Список поддерживаемых точек автозапуска** Kaspersky Endpoint Agent поддерживает сбор следующих точек автозапуска: • Logon. • Run. • Explorer. • Shell. • Office. • Internet Explorer®. • Tasks. • Services. • Drivers. • Telephony. • Cryptography. • Debuggers. • COM. • Session Manager. • Network. • LSA. • Applications. • Codecs. • Shellex.

Действие по реагированию	Параметры для создания задачи
	• WMI. • Unspecified. Kaspersky Endpoint Security поддерживает сбор перечисленных выше точек автозапуска и указанных далее: • BootLog. • Browsers. • DriverLog. • EfiLoader. • GroupPolicy. • Logon. • OsLoader. • OsUpdate. • Printer. • Process. • Scheduler. • **Список файлов** – список файлов, хранящихся в выбранной папке или во всех папках хоста в момент выполнения задачи. • При выборе **Список файлов** доступны следующие типы источника: • **Все локальные диски** – включить в список файлы, хранящиеся во всех папках локальных дисков на момент выполнения задачи. • **Директория** – включить в список файлы, хранящиеся в указанной папке и подпапках. • При выборе **Директория** доступны следующие параметры: • **Начальная директория** – путь к папке, с которой начнется поиск файлов. Вы можете использовать системные или пользовательские переменные окружения. При использовании пользовательских переменных окружения в список файлов будет включена информация о файлах в папках всех пользователей, определивших указанные переменные окружения. Если пользовательские переменные окружения переопределяет системные, в список файлов будет включена информация о файлах в папках по значению системных переменных окружения. • **Маска** – маска файлов, которые должны быть включены в список файлов. • **Альтернативные потоки данных** – включить запись информации об альтернативных потоках данных в список файлов. Если запрашиваемый файл связан с дополнительными потоками данных NTFS, в результате выполнения задачи вы получите все файлы потоков данных NTFS, с которыми связан запрашиваемый файл. • **Максимальный уровень вложенности** – максимальный уровень вложенности папок, в которых приложение будет искать файлы. • **Исключения** – путь к папкам, в которых вы хотите запретить поиск информации о файлах. • **Описание** – описание задачи. Поле не является обязательным.
Собрать ключи реестра Получение списка указанных ключей реестра и их значений в Хранилище Kaspersky Anti Targeted Attack Platform с возможностью скачать данные на локальный компьютер.	• **Путь к ключу реестра** – путь к ключу реестра, который вы хотите получить. Вы можете указать путь к ключу реестра в одном из следующих форматов: • Корневой относительный путь. Например, \REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator. • Относительный путь с указанием полного имени раздела. Например, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.

Действие по реагированию	Параметры для создания задачи
	• Относительный путь с аббревиатурой вместо полного имени раздела. Например, HKLM\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator. Если вы хотите получить данные из ветки HKEY_CURRENT_USER, вам требуется указать ветку HKEY_USERS и SID пользователя: HKEY_USERS\<SID пользователя>. • **Описание** – описание задачи. Поле не является обязательным.
Запустить YARA-проверку Проверка процессов, точек автозапуска и файлов с помощью правил YARA.	• **Выбрать правила** – имя правила. Вы можете ввести название правила или несколько знаков из названия правила и выбрать правило в списке. Вы можете добавить несколько правил. • **Проверить** – область проверки. Доступны следующие области проверки: • **ОЗУ** – проверить процессы, запущенные на момент выполнения задачи. Приложение не проверяет процессы с низким уровнем приоритета. • **Точки автозапуска** – проверить точки автозапуска, полученные в результате выполнения задачи Собрать форензику. Для проверки точек автозапуска вам требуется указать устройства, для которых ранее была выполнена задача **Собрать форензику**. • **Указанные директории** – проверить файлы, хранящиеся в указанной папке и во всех вложенных папках на момент выполнения задачи. • **Все локальные диски** – проверить файлы, хранящиеся во всех папках локальных дисков на момент выполнения задачи. Проверка всех локальных дисков может создать повышенную нагрузку на хост. • При выборе **ОЗУ** доступны слеующие параметры: • **Процессы** – короткие имена процессов или маску файлов, которые вы хотите проверить. Приложение проверяет все запущенные на хосте процессы с одинаковыми именами. Если поле **Процессы** не заполнено, приложение проверяет все процессы, запущенные на момент выполнения задачи, кроме процессов с PID ниже 10 и процессов, указанных в поле **Исключения**. • **Исключения** – полные имена процессов или маску файлов, которые хотите исключить из проверки. Если на хосте запущено несколько процессов с одинаковыми именами, приложение исключит из проверки все эти процессы. • При выборе **Точки автозапуска** доступны следующие параметры: • **Быстрая** – проверять все точки автозапуска, кроме COM-объектов. • **Полная** – проверять все точки автозапуска и связанные с ними файлы. Если в качестве компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Security для Windows, вне зависимости от выбранного параметра выполняется полная проверка. • При выборе **Указанные директории** доступны следующие параметры: • **Указанные директории** – путь к директории в формате C:\<имя директории>*. • **Исключения** – путь к директории в формате C:\<имя директории>*.

Действие по реагированию	Параметры для создания задачи
	• **Максимальное время проверки** – максимальное время проверки. По истечении указанного времени проверка завершится, даже если хосты были проверены не по всем правилам. В отчете о выполнении задачи указываются результаты, актуальные на момент завершения проверки. • **Описание** – описание задачи. Поле необязательно для заполнения.
Управление службами Запуск, остановка, приостановка, удаление, продолжение работы службы и изменение типа запуска службы на указанных устройствах.	• **Имя службы** – имя службы. • **MD5/SHA256** – MD5- или SHA256-хеш службы. Поле необязательно для заполнения. Если вы указали хеш службы, которая загружается из DLL, Kaspersky Anti Targeted Attack Platform сравнивает указанный хеш одновременно с хешем библиотеки службы DLL и хешем процесса svchost. • **Действие** – операция, которую вы хотите произвести со службой. Доступны следующие операции со службами: • **Запустить**. • **Остановить**. • **Приостановить**. • **Продолжить**. • **Удалить**. • **Изменить тип запуска**. При удалении службы процессы, которые были запущены этой службой, продолжают работать до перезагрузки системы или завершении работы процесса. • При выборе **Изменить тип запуска** вам нужно выбрать тип запуска службы в поле **Тип запуска**. • **Описание** – описание задачи. Поле необязательно для заполнения.
Поместить файл на карантин Помещение на карантин зараженного или возможно зараженного файла. При необходимости вы можете восстановить файл из карантина.	• **Путь к файлу** – путь к файлу, который вы хотите удалить. • **MD5/SHA256** – MD5-, SHA256-хеш файла, который вы хотите удалить. Поле не является обязательным. • **Описание** – описание задачи. Поле не является обязательным.
Запустить приложение Запуск приложения или выполнение команды. При необходимости вы можете остановить запущенный процесс. Подробнее о задаче остановки процесса см. информацию внутри таблицы выше.	• В полях **Путь к файлу** и **Рабочий каталог** требуется ввести значения одним из следующих способов: • В поле **Путь к файлу** введите полный путь к исполняемому файлу (например, `C:\Windows\System32\ipconfig.exe`). Поле **Рабочий каталог** оставьте пустым. При создании задачи приложение не проверяет на корректность указанный путь к исполняемому файлу. • В поле **Путь к файлу** введите имя и расширение исполняемого файла (например, `ipconfig.exe`). В поле **Рабочий каталог** укажите рабочую директорию (например, `C:\Windows\System32\`). • **Аргументы** – дополнительные параметры запуска файла или выполнения команды (например, аргумент `/all`). • **Описание** – описание задачи. Поле не является обязательным.
Создать правило запрета	• **Состояние** – состояние правила запрета.

Действие по реагированию	Параметры для создания задачи
Запрет запуска файлов и процессов на указанных устройствах. При необходимости вы можете удалить, включить или отключить созданное правило запрета.	• **MD5/SHA256** – MD5- или SHA256-хеш файла или потока данных, запуск которого вы хотите запретить. • **Имя** – имя правила запрета. • **Показывать пользователю уведомление о блокировке запуска файла** – показывать уведомление о срабатывании правила запрета пользователю компьютера, на который распространяется запрет.

Контроль пользователей на устройствах

Kaspersky Anti Targeted Attack Platform может контролировать учетные записи пользователей на устройствах, известных приложению. При контроле пользователей приложение автоматически получает сведения об учетных записях, зарегистрированных в операционных системах устройств. По полученным сведениям приложение формирует таблицы пользователей.

При получении сведений об учетных записях приложение контролирует по этим сведениям все учетные записи пользователей на устройствах, за исключением некоторых локальных системных учетных записей, которые могут использовать только системные службы операционной системы. Например, приложение не контролирует учетные записи LocalSystem и NetworkService, используемые на устройствах под управлением операционных систем семейства Windows.

Для использования функциональности контроля пользователей должны быть включены методы контроля активов для обнаружения активности устройств и обнаружения сведений об устройствах. Эти методы должны быть включены на всех серверах с установленными компонентами приложения, от которых поступают сведения.

Контроль пользователей выполняется на основании данных, поступающих от источников следующих типов:

1. **Телеметрия (Endpoint Agent)**.

   Данные об устройствах и о выполняемых на них процессах поступают при интеграции компонента Endpoint Agent с функциональностью NDR.

2. **Внешний источник**.

   Данные поступают от систем, использующих NDR API и отправляющих в Kaspersky Anti Targeted Attack Platform сведения о пользователях.

Источники перечислены в порядке уменьшения приоритета данных, поступающих от этих источников. Приложение обрабатывает сведения о пользователях в соответствии с приоритетом поступивших данных. Сведения о пользователях, полученные от более приоритетного источника, могут заместить собой сведения от других источников. Также приложение автоматически удаляет из таблиц учетные записи пользователей, сведения о которых ранее были получены от источника **Внешний источник**, но в новых поступивших данных от этих источников такие пользователи отсутствуют.

Вы можете просматривать сведения о пользователях в разделе **Активы** на вкладке **Пользователи**.

При просмотре таблицы пользователей вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.Для таблицы всех пользователей действует ограничение по количеству элементов – не более 200 000.

Приложение отображает следующие сведения о пользователях устройств в таблице и области деталей выбранного пользователя:

- **ID пользователя** – идентификатор пользователя, присвоенный в Kaspersky Anti Targeted Attack Platform.
- **Имя пользователя** – имя учетной записи пользователя без указания домена или сетевого имени устройства.
- **Полное имя** – имя учетной записи пользователя с указанным именем домена или сетевым именем устройства.
- **Группы** – имена групп пользователей, в которые добавлена учетная запись пользователя.
- **Устройство** – имя и адрес устройства.
- **Источник** – тип источника данных о пользователе.
- **SID** – идентификатор безопасности пользователя.
- **Статус учетной записи** – статус, соответствующий полученному значению параметра для включения и выключения использования учетной записи.
- **Блокировка** – статус, соответствующий полученному значению параметра блокировки учетной записи.
- **Смена пароля при следующем входе** – признак включенного или выключенного состояния параметра, определяющего необходимость смены пользователем его пароля при следующем входе в систему.
- **Запрет смены пароля пользователем** – признак включенного или выключенного состояния параметра, определяющего запрет смены пользователем его пароля.
- **Срок действия пароля** – статус, соответствующий полученному значению параметра для включения и выключения ограничения на срок действия пароля пользователя.
- **Данные получены** – дата и время последнего получения сведений об учетной записи.
- **Описание** – описание, заданное для учетной записи.

При контроле пользователей приложение регистрирует события по технологии **Контроль активов**. Для регистрации используется системный тип события, которому присвоен код 4000005600. События регистрируются, если на устройствах автоматически добавлены, изменены или удалены учетные записи пользователей.

Вы можете настроить доступные параметры для типов событий.

Контроль запусков исполняемых файлов на устройствах

Kaspersky Anti Targeted Attack Platform может контролировать запуски исполняемых файлов на устройствах, известных приложению. Контроль запусков исполняемых файлов выполняется на основании данных, которые поступают от EPP-приложений. По полученным сведениям приложение формирует таблицу исполняемых файлов.

Для автоматического получения сведений о запусках исполняемых файлов от EPP-приложений вам необходимо выполнить следующие условия:

- На устройствах должен быть установлен Endpoint Agent.
- Должны быть включены методы контроля активов для обнаружения активности устройств и обнаружения сведений об устройствах.

Для таблицы исполняемых файлов действуют следующие ограничения по количеству и времени хранения элементов:

- Общее количество исполняемых файлов – не более 100 тыс.

  Если достигнуто ограничение максимального количества исполняемых файлов, приложение автоматически удаляет 10% самых старых записей.

- Максимальное время хранения исполняемого файла до следующего получения данных о запуске этого файла – не более 90 дней.

  Если новые данные о запуске исполняемого файла не были получены до истечения максимального времени хранения, приложение автоматически удаляет запись об этом файле.

При необходимости пользователи с ролью Администратор могут удалять исполняемые файлы вручную.

Чтобы просмотреть таблицу исполняемых файлов:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Исполняемые файлы**.

Отобразится таблица исполняемых файлов.

При просмотре таблицы исполняемых файлов вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

В таблице отображаются следующие данные:

- **ID файла** – идентификатор файла, присвоенный в Kaspersky Anti Targeted Attack Platform.
- **Устройство** – имя и адрес устройства.
- **Имя** – название и версия приложения или имя файла.
- **Данные получены** – дата и время последнего получения сведений о файле.
- **Продукт** – название программного продукта, сохраненное в операционной системе устройства.
- **Версия продукта** – версия программного продукта, сохраненная в операционной системе устройства.
- **Поставщик** – название поставщика приложения.
- **Путь** – полный путь к файлу.
- **Размер файла** – объем дискового пространства, занятого файлом.
- **Хеш MD5** – контрольная сумма файла, полученная с помощью алгоритма хеширования MD5.

- **Хеш SHA256** – контрольная сумма файла, полученная с помощью алгоритма хеширования SHA256.
- **Подпись** – результат проверки цифровой подписи файла: **Действительная** (если проверка цифровой подписи пройдена успешно) или **Недействительная** (например, если истек срок годности сертификата).
- **Создан** – дата и время создания файла.
- **Изменен** – дата и время последнего изменения файла.
- **Источник** – тип источника данных о файле.
- **Атрибуты** – список атрибутов файла.
- **Описание** – описание, заданное для файла.

Задания активных опросов устройств

С помощью заданий активного опроса вы можете проводить аудит безопасности контролируемых устройств в части получения точной и полной информации об устройствах и их конфигурациях непосредственно от самих устройств. Активные опросы выполняются с помощью коннекторов. Для проведения активных опросов устройств вам нужно добавить в программу один или несколько коннекторов типа **Active poll**.

Коннекторы предоставляют различные методы проведения активных опросов. *Методы активных опросов* определяют используемые протоколы, а также команды и функции этих протоколов. Встроенный в программу тип коннектора **Active poll** содержит набор методов, поддерживающих активные опросы как по протоколам прикладного уровня, так и по протоколам общего применения. Kaspersky Anti Targeted Attack Platform поддерживает следующие методы для проведения активных опросов устройств:

- опрос по протоколу ARP (только для компьютеров с версией ядра 4.3 и выше);
- опрос по протоколу SMB;
- опрос по протоколу SNMP;
- опрос по протоколу SSH;
- опрос по протоколу WinRM HTTP;
- опрос по протоколу WinRM HTTPS;
- опрос по протоколу взаимодействия WMI.

Методы различаются по составу получаемых сведений об устройствах. Вы можете выбирать нужные вам сведения и используемые методы при настройке параметров проведения активных опросов.

Некоторые методы используют секреты для подключения к устройствам. Подключение к устройствам осуществляется с помощью учетных данных из секретов, добавленных в программу.

При использовании соответствующих методов программа может автоматически обновлять следующие сведения об устройстве по результатам активного опроса:

- имя, под которым устройство представлено в программе;
- имя, под которым устройство представлено в сети (сетевое имя);

- название производителя аппаратного обеспечения устройства;
- название модели устройства;
- номер версии аппаратного обеспечения устройства;
- название производителя программного обеспечения устройства;
- название программного обеспечения устройства;
- номер версии программного обеспечения устройства;
- адресная информация для сетевых интерфейсов устройства;
- название операционной системы, установленной на устройстве (только для устройств под управлением операционных систем семейств Windows и Linux).

Список операционных систем, поддерживаемых программой для проведения активных опросов устройств, см. в Приложении.

Обновление не выполняется для тех сведений, для которых выключено автоматическое изменение с помощью переключателей **Автообновление** при добавлении устройства или при изменении сведений об устройстве. Также программа оценивает достоверность полученных сведений об устройстве и в некоторых случаях может не обновлять ранее полученные сведения.

Некоторые методы активных опросов поддерживают возможность обнаружения рисков и внесения изменений в топологическую карту по полученным данным об устройствах.

Для каждого задания вы можете запускать выполнение вручную или настроить расписание автоматического запуска. Запускать задания активного опроса устройств могут только пользователи с ролью Старший сотрудник службы безопасности.

Для использования функциональности активного опроса вам нужно учитывать следующие особенности и ограничения:

- Функциональность доступна после добавления лицензионного ключа.
- Программные модули коннекторов, с помощью которых выполняются активные опросы устройств, должны иметь сетевой доступ к устройствам для отправки запросов и получения данных от устройств. Если программные модули функционируют на узле с установленными компонентами программы, для обеспечения сетевого доступа к устройствам на этом компьютере должен быть сетевой интерфейс с подключением к сети этих устройств. Для этих целей не могут использоваться сетевые интерфейсы точек мониторинга, если на эти сетевые интерфейсы поступает зеркалированный трафик корпоративной сети (например, от SPAN-портов сетевых коммутаторов).
- При активном опросе возможно возникновение непредвиденных проблем с устройствами из-за неверной интерпретации этими устройствами поступивших команд активного опроса. Проблемы могут быть вызваны неправильной или узкоспецифичной настройкой устройств. Также проблемы могут возникать из-за скрытых ошибок в сетевой конфигурации, которые не проявляются при обычном взаимодействии устройств. В связи с этим при активном опросе устройства имеются следующие риски возможных последствий:
  - выключение устройства;
  - потеря связи с устройством;
  - полная или частичная неработоспособность устройства;

- замедление работы устройства;
- другие потенциальные сбои в работе сети и оборудования.

Добавление задания активного опроса

Для известных программе устройств вы можете добавлять задания, по которым программа будет выполнять активный опрос.

Добавлять задания активного опроса могут только пользователи с ролью Старший сотрудник службы безопасности. Добавление задания активных опросов возможно после добавления лицензионного ключа.

Настройка задания активного опроса выполняется с помощью мастера. Мастер позволяет пошагово выполнить настройку всех нужных параметров задания. После завершения настройки вы можете дождаться запуска сканирований на устройствах по расписанию или запустить задание вручную.

При добавлении задания активного опроса вы можете вызвать мастер настройки следующими способами:

- Добавление задания с изначально пустыми значениями параметров. Для этого:

  1. Выберите раздел **Активы**.
  2. На вкладке **Активный опрос** нажмите на кнопку **Добавить задание**.

  В параметрах мастера настройки не будут заданы значения по умолчанию.

- Добавление задания для выбранных устройств. Для этого:

  1. Выберите раздел **Активы**.
  2. На вкладке **Устройства** выберите устройства, для которых вы хотите добавить задание активного опроса. Вы можете выбрать не более 100 устройств.
  3. В панели инструментов, которая расположена над таблицей устройств, откройте раскрывающийся список **Создать задание** и выберите пункт **Активный опрос**.

  В параметрах мастера настройки по умолчанию будет сформирован список устройств, состоящий из выбранных устройств.

Чтобы настроить параметры задания в окне мастера настройки:

1. В окне с предупреждением об особенностях активных опросов внимательно ознакомьтесь с описанием этих особенностей и подтвердите принятие рисков возможных последствий при использовании модуля активного опроса.
2. В разделе мастера **Выбор устройств** сформируйте список устройств, для которых требуется выполнить активный опрос. Выберите не более 100 устройств.

   Вы можете сформировать список устройств с помощью кнопок **Добавить в задание** и **Удалить из задания**. Для добавления устройств программа открывает окно с таблицей устройств для выбора. Вы можете выполнять фильтрацию и сортировку таблицы для отображения нужных устройств.
3. В разделе мастера **Выбор параметров** установите флажки для тех сведений об устройствах, которые вы хотите обновить с помощью активного опроса. Вы также можете включить обнаружение рисков (флажок **Риски**) и обнаружение параметров топологии для устройств (флажок **Параметры топологии**).

4. В разделе мастера **Выбор методов** выполните следующие действия:

   a. Выберите модуль активного опроса.

   b. Установите флажки для тех методов, которые вы хотите использовать для получения сведений об устройствах, обнаружения рисков и/или параметров топологии.

      Доступные для использования методы сгруппированы по коннекторам, которые предоставляют возможности активного опроса устройств. Список содержит только методы, поддерживающие получение выбранных сведений. Если коннектор невозможно использовать для активного опроса выбранных устройств, доступные методы не отображаются для этого коннектора (например, если коннектор выключен или для коннектора выбрано адресное пространство, не содержащее адресов выбранных устройств).

   c. При необходимости настройте параметры для работы методов каждого коннектора (например, для метода **Опрос по протоколу SSH** требуется указать порт и секрет с учетными данными для подключения).

      Если секрет с нужными учетными данными не добавлен в программу, вы можете, не закрывая окно мастера настройки, открыть в браузере новую вкладку, подключиться к Серверу и добавить секрет, после чего обновить список секретов с помощью кнопки в окне мастера настройки.

      Не рекомендуется использовать один и тот же секрет для активного опроса устройств в сети, так как это негативно влияет на уровень информационной безопасности.

      Методы, для которых требуется настройка параметров, выделены красным. Для уточнения параметров нажмите на кнопку справа от нужного метода.

5. В разделе мастера **Настройка задания** настройте остальные параметры задания:

   a. Введите имя и описание задания.

      Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. Имя задания должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

      Имя задания должно содержать не более 256 символов. Описание задания должно содержать не более 4096 символов.

   b. Если требуется запускать выполнение задания по расписанию, включите переключатель **Запускать задание по расписанию** и настройте параметры расписания:

      - В раскрывающемся списке **Периодичность** выберите, как часто требуется выполнять запуски: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.
      - В зависимости от выбранного варианта задайте значения параметров, чтобы уточнить время запуска.

      Программа выполняет запуск задания по расписанию при условии завершения предыдущего запуска этого задания. Если к моменту запуска задания по расписанию его предыдущий запуск имеет статус *Выполняется*, программа пропускает запуск задания по расписанию.

6. Нажмите на кнопку для завершения работы мастера: **Создать задание** или **Создать и запустить**.

Заданные параметры отобразятся в области деталей задания.

Изменение задания активного опроса

Изменять задания активного опроса могут только пользователи с ролью Старший сотрудник службы безопасности.

Чтобы изменить задание активного опроса:

1. Выберите раздел **Активы**.
2. На вкладке **Активный опрос** выберите задание, для которого вы хотите изменить параметры.
3. Нажмите на кнопку **Изменить**.

   Запустится мастер настроек. В параметрах мастера настройки в качестве значений по умолчанию будут заданы значения параметров выбранного задания.
4. В разделе мастера **Настройка задания** настройте остальные параметры задания:

   a. Введите имя и описание задания.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. Имя задания должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

   Имя задания должно содержать не более 256 символов. Описание задания должно содержать не более 4096 символов.

   b. Если требуется запускать выполнение задания по расписанию, включите переключатель **Запускать задание по расписанию** и настройте параметры расписания:

   - В раскрывающемся списке **Периодичность** выберите, как часто требуется выполнять запуски: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.
   - В зависимости от выбранного варианта задайте значения параметров, чтобы уточнить время запуска.

   > Программа выполняет запуск задания по расписанию при условии завершения предыдущего запуска этого задания. Если к моменту запуска задания по расписанию его предыдущий запуск имеет статус *Выполняется*, программа пропускает запуск задания по расписанию.

5. Нажмите на кнопку **Изменить задание** для завершения работы мастера.

Заданные параметры отобразятся в области деталей задания.

Просмотр таблицы заданий активных опросов

Таблица заданий активного опроса отображается в разделе **Активы** на вкладке **Активный опрос**.

Параметры заданий отображаются в следующих столбцах таблицы:

- **ID задания**.

  Идентификатор задания, присвоенный в Kaspersky Anti Targeted Attack Platform.

- **Имя**.

  Имя, под которым задание представлено в программе.

- **Описание**.

  Описание задания.

- **Создано**.

  Дата и время добавления задания в программу.

- **Изменено**.

  Дата и время последнего изменения в программе.

- **Выбрано устройств**.

  Количество устройств, выбранных для задания.

- **Расписание**.

  Информация о расписании, по которому программа автоматически запускает выполнение задания.

- **Статус последнего запуска**.

  Результирующий статус сканирований всех устройств при последнем запуске задания.

- **Последний запуск**.

  Дата и время последнего запуска задания.

- **Следующий запуск**.

  Дата и время следующего запуска задания по расписанию.

При просмотре таблицы заданий активного опроса вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Запуск и остановка заданий активных опросов

Вы можете запускать и останавливать задания активного опроса вручную. При запуске или остановке задания программа запускает или останавливает выполнение всех сканирований на устройствах, которые выбраны для этого задания.

Действия по остановке или запуску задания доступны при соответствующих статусах последнего запуска задания (например, запуск задания не доступен, если его последний запуск имеет статус *Выполняется*).

Запускать и останавливать задания активного опроса вручную могут только пользователи с ролью Старший сотрудник службы безопасности.

Чтобы запустить задание активного опроса:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Активный опрос** выберите задание, которое вы хотите запустить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Запустить** (кнопка заблокирована, если запуск задания невозможен в текущий момент).

   Kaspersky Anti Targeted Attack Platform запустит выполнение задания. Сведения о выполнении сканирований устройств вы можете просмотреть на вкладке **Запуски** в области деталей задания.

Чтобы остановить выполнение задания активного опроса:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Активный опрос** выберите задание, выполнение которого вы хотите остановить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Остановить** (кнопка заблокирована, если остановка выполнения задания невозможна в текущий момент).

Просмотр общих сведений о выполнении запусков заданий активных опросов

Вы можете просматривать общие сведения о запусках заданий активного опроса при просмотре таблицы заданий. В таблице отображаются сведения о выполнении последних запусков без вывода сведений о сканированиях устройств. Для просмотра общих сведений обо всех запусках задания, включая сведения о сканированиях устройств, вы можете выбрать это задание и перейти на вкладку **Запуски** в области деталей.

К общим сведениям о выполнении запусков заданий активного опроса относятся следующие:

- Статус выполнения запуска задания или сканирования устройства.

  Предусмотрены следующие статусы:

  - **Ожидание** – команда на начало сканирования еще не отправлена.
  - **Выполняется** – сканирование или запуск находится в процессе выполнения.
  - **Отменяется** – сканирование или запуск находится в процессе остановки.
  - **Отменено** – остановлено сканирование или запуск.
  - **Завершено** – сканирование завершено успешно или все сканирования в запуске завершены успешно.

- **Ошибка** – при сканировании произошла ошибка или во всех сканированиях в запуске произошли ошибки.
- **Не все успешно** – запуск задания завершен с частично успешным результатом: есть сканирования со статусом **Завершено** и есть сканирования со статусом **Отменено** или **Ошибка**.

- Дата и время начала.
- Дата и время завершения.
- Длительность выполнения.

Просмотр отчета о выполнении задания активного опроса

Вы можете просматривать отчеты с результатами выполнения сканирований на устройствах при просмотре подробных данных о запуске задания активного опроса. Отчеты формируются программой для заданий, выполнение которых завершилось со статусами **Завершено**, **Не все успешно**, **Отменено** и **Ошибка**.

В отчете отображается следующая информация:

- Имя устройства, для которого было выполнено сканирование.
- Статус обновления параметров устройства.
- Список параметров устройства, сгруппированных по статусу их обновления.
- Список методов, сгруппированных по статусу их выполнения. В случае возникновения ошибки при работе метода, программа отображает ее причину.

Чтобы просмотреть отчет о выполнении задания активного опроса:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Активный опрос** выберите задание, отчет о запуске которого вы хотите просмотреть.

   В правой части окна веб-интерфейса появится область деталей.
4. В области деталей перейдите на вкладку **Запуски** и выберите нужный запуск задания.

   В правой части окна веб-интерфейса появится область деталей. В области деталей отображаются подробные сведения о выбранном запуске задания.

Удаление заданий активных опросов

Вы можете удалять задания активного опроса. При этом невозможно удалять задания со статусом последнего запуска **Выполняется** или **Ожидание**.

Удалять задания активного опроса могут только пользователи с ролью Старший сотрудник службы безопасности.

Чтобы удалить задания активного опроса:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Активный опрос** выберите задания, которое вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление заданий.

   Из выбранных заданий вы можете удалить только такие задания, у которых статус последнего запуска отличается от статусов **Выполняется** и **Ожидание**. Если среди выбранных заданий есть задания со статусом **Выполняется** или **Ожидание**, на экране появится сообщение об этом. Для удаления таких заданий вам нужно предварительно остановить выполнение заданий.

Настройка адресных пространств

Kaspersky Anti Targeted Attack Platform контролирует устройства и их взаимодействия с учетом адресных пространств (далее также "АП"). *Адресные пространства* предназначены для распределения адресов устройств на множества по какому-либо признаку (например, по принадлежности устройств сегментам сети).

Для описания адресных пространств в приложении используются списки правил и подсетей.

Правило адресного пространства – это набор параметров, определяющих условия принадлежности адресов адресному пространству. Для связывания с адресным пространством каждый MAC- или IP-адрес должен удовлетворять хотя бы одному правилу адресного пространства. При этом приложение связывает адрес с тем адресным пространством, правило которого наименее обобщенно определяет условия для принадлежности этого адреса (например, если адрес явно указан в правиле).

Подсети адресного пространства используются для проверки IP-адресов, обнаруженных приложением. В зависимости от типа подсети, которой принадлежит обнаруженный IP-адрес, приложение может выполнять различные действия для контроля активов и контроля взаимодействий устройств.

Вы можете настраивать адресные пространства в разделе **Активы** на вкладке **Адресные пространства**. Каждое адресное пространство представлено в виде блока со сведениями об адресном пространстве. Блок состоит из заголовка и вложенных блоков с таблицами правил и подсетей. При просмотре сведений об адресных пространствах вы можете разворачивать и сворачивать содержимое блоков.

Адресное пространство **Default**

По умолчанию в приложении задано одно общее адресное пространство с именем **Default**. Это адресное пространство содержит единственное правило, параметры которого настроены на связывание любых MAC- и IP-адресов с этим адресным пространством. Список подсетей адресного пространства **Default** по умолчанию содержит стандартный набор подсетей, наиболее часто используемых на предприятиях.

Вы не можете изменить правило адресного пространства **Default** и добавлять другие правила в это адресное пространство. При этом пользователи с ролью Старший сотрудник службы безопасности могут изменять список подсетей в этом адресном пространстве, чтобы сформировать набор подсетей с учетом особенностей IP-адресации устройств в сети вашего предприятия. Если в Kaspersky Anti Targeted Attack Platform поступают данные от EPP-приложений, по этим данным приложение может автоматически добавлять подсети в список подсетей.

Дополнительные адресные пространства

При необходимости вы можете настроить в приложении несколько адресных пространств в дополнение к адресному пространству **Default**. Для добавленных адресных пространств доступны возможности формирования произвольных правил и наборов подсетей. Адреса, удовлетворяющие условиям добавленных адресных пространств, будут связаны с этими адресными пространствами. Остальные адреса останутся связанными с адресным пространством **Default**.

Необходимость в добавлении адресных пространств может возникнуть, например, при использовании устройств с одинаковыми адресами в разных сегментах сети. В этом случае после добавления и настройки адресных пространств приложение сможет различать адресную информацию по дополнительным атрибутам, которые приложение добавляет к адресам в виде имен адресных пространств.

Примеры использования адресных пространств см. в Приложении.

Связи адресов и адресных пространств

При использовании нескольких адресных пространств приложение добавляет атрибуты с именами адресных пространств ко всем адресам, которые указываются в объектах приложения: в устройствах, рисках, правилах, событиях и прочих объектах. Атрибуты с именами адресных пространств перестают отображаться для адресов, если в приложении удалены все добавленные адресные пространства (атрибуты адресных пространств остаются только для адресов в событиях и в некоторых рисках, связанных с устройствами).

Атрибуты с именами адресных пространств обозначают связи адресов и адресных пространств. За счет связей с адресными пространствами адреса становятся зависимыми от этих адресных пространств.

Установленные связи адресов и адресных пространств приводят к следующим особенностям при удалении адресного пространства: приложение автоматически удаляет все адреса, связанные с удаляемым адресным пространством. Такие адреса удаляются из всех объектов приложения, за исключением событий. При удалении адреса из объекта приложение проверяет наличие остающихся других адресов в этом объекте, и если других адресов не остается, приложение удаляет и сам объект (например, устройство).

О правилах адресных пространств

Правила адресных пространств отображаются в блоках **Правила** внутри описаний адресных пространств. Информация о правилах отображается в строке заголовка адресного пространства и в таблице правил.

Параметры правил адресных пространств отображаются в следующих столбцах таблицы:

- **Источник**.

  Тип источника поступления данных об адресной информации и список выбранных источников данных. Предусмотрены следующие типы источников данных:

  - **Точки мониторинга** – выбранные для правила точки мониторинга.
  - **Серверы интеграции** – выбранные для правила серверы интеграции (данные об адресной информации, поступившие от выбранных серверов интеграции, будут удовлетворять правилу адресного пространства).
  - **Модули активного опроса** – выбранные для правила коннекторы модулей активного опроса (данные об адресной информации, поступившие от выбранных модулей активного опроса, будут удовлетворять правилу адресного пространства).

  Конкретные источники данных требуется указывать в правилах адресных пространств после добавления в приложение объектов, которые будут являться источниками. Например, коннекторы для источника данных **Модули активного опроса** нужно указывать после добавления коннекторов типа **Active poll**.

- **Уровни модели OSI**.

  Выбранные уровни сетевой модели стека сетевых протоколов OSI (Open Systems Interconnection) для правила адресного пространства. Правило можно настроить на адреса следующих уровней модели OSI:

  - **Канальный (L2)** – к этому уровню относятся MAC-адреса.
  - **Сетевой (L3)** – к этому уровню относятся IP-адреса.
  - **Канальный и сетевой (L2 и L3)** – к этому уровню относятся и MAC-, и IP-адреса.

- **VLAN ID**.

  Идентификаторы виртуальных локальных сетей (VLAN), применяемые при использовании технологии VLAN в соответствии со стандартом IEEE 802.1q. Для правила адресного пространства параметр **VLAN ID** может принимать следующие значения:

  - **Используются любые** – для сетевых взаимодействий между устройствами используется технология VLAN, при этом идентификаторы VLAN могут быть любыми.
  - **Не используются** – для сетевых взаимодействий между устройствами не используется технология VLAN.
  - **Любые или не используются** – для сетевых взаимодействий между устройствами технология VLAN либо не используется, либо используется с применением любых идентификаторов VLAN.
  - **Фиксированные значения** со списком идентификаторов VLAN – для сетевых взаимодействий между устройствами используется технология VLAN, при этом к адресному пространству относится только такая адресная информация, в которой указан один из перечисленных идентификаторов VLAN.

- **IP-адреса**.

  IP-адреса, входящие в адресное пространство. Адреса могут быть указаны по отдельности, в виде диапазонов или в формате CIDR-адреса подсети.

При просмотре таблицы правил вы можете использовать функции настройки (по значку ⚙), а также поиска.

О подсетях адресных пространств

Подсети адресных пространств отображаются в блоках **Подсети** внутри описаний адресных пространств.

Приложение проверяет обнаруженные IP-адреса по спискам подсетей адресных пространств и в зависимости от принадлежности IP-адресов определенным типам подсетей может выполнять следующие действия:

- добавлять устройство с обнаруженным IP-адресом в таблицу устройств и контролировать активность этого устройства;
- отображать устройство с обнаруженным IP-адресом на карте сетевых взаимодействий и топологической карте в виде узла соответствующего типа (известное приложению устройство, неизвестное или узел WAN);
- отображать соединение на карте сетевых взаимодействий, в котором одной из сторон взаимодействия является устройство с обнаруженным IP-адресом;
- проверять взаимодействия устройства с обнаруженным IP-адресом по заданным правилам (правила контроля взаимодействий, правила обнаружения вторжений и правила корреляции);
- игнорировать активность устройства с обнаруженным IP-адресом.

Параметры подсетей адресных пространств отображаются в следующих столбцах таблицы:

- **Подсеть**.

  Адрес подсети в формате записи по методу бесклассовой адресации (Classless Inter-Domain Routing, CIDR): `<базовый адрес подсети>/<количество бит в маске>`. Адреса подсетей отображаются в виде дерева, которое показывает иерархию вложенности подсетей.

- **Тип**.

  Тип подсети, определяющий ее назначение. Предусмотрены следующие типы:

  - **Частная, IT** – подсеть для устройств, относящихся к ресурсам информационных технологий (IT), например файловых серверов.
  - **Частная, DMZ** – подсеть для устройств, находящихся в сегменте сети демилитаризованной зоны (DMZ), например серверов для запросов из внешних сетей.
  - **Публичная** – подсеть, которая считается внешней (глобальной) сетью для устройств в подсетях других типов. IP-адреса из этой подсети представлены на карте сетевых взаимодействий узлом WAN.
  - **Link-local** – подсеть для сетевых взаимодействий в пределах одного сегмента локальной сети (немаршрутизируемая).

- **Диапазон**.

  Диапазон IP-адресов, входящих в подсеть.

- **Автоматически добавлять подсети**.

  Признак включенного или выключенного режима автоматического добавления вложенных подсетей по данным от EPP-приложений. Если режим включен, приложение добавляет вложенные подсети на основании данных, полученных от EPP-приложений.

При просмотре таблицы подсетей вы можете использовать функции настройки (по значку ⚙), а также фильтрации, поиска и сортировки.

Добавление адресного пространства

Вы можете добавлять в приложение адресные пространства, если требуется распределять адреса устройств на множества по какому-либо признаку (например, по принадлежности устройств сегментам сети).

Максимальное количество адресных пространств в приложении – 100.

Добавлять адресные пространства могут только пользователи с ролью Старший сотрудник службы безопасности.

Чтобы добавить адресное пространство:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Адресные пространства** откройте область деталей по кнопке **Добавить АП**.
4. Введите имя адресного пространства.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   Имя адресного пространства должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 255 символов;
   - не совпадает с именем другого адресного пространства (регистр символов не учитывается).

   > Рекомендуется задавать имя адресного пространства длиной не более 6-8 символов. Если имя содержит большое количество символов, адресная информация может не полностью отображаться в ячейках некоторых таблиц данных (например, в таблице устройств).

5. При необходимости введите текстовое описание адресного пространства.
6. Настройте параметры первого правила адресного пространства.
7. При необходимости добавьте и настройте дополнительные правила адресного пространства по кнопке **Добавить правило**.

   Общее количество правил в адресном пространстве не может превышать 10.

8. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

В нижней части вкладки **Адресные пространства** появится отдельный блок со сведениями о добавленном адресном пространстве.

Формирование списка подсетей для контроля активов

Этот раздел содержит информацию о функциях, доступных для формирования списка подсетей для контроля активов.

Для адресных пространств вы можете формировать списки подсетей с учетом особенностей адресации устройств в сети вашего предприятия. Этот раздел содержит инструкции по использованию функций для формирования списка подсетей.

Если в Kaspersky Anti Targeted Attack Platform поступают данные от EPP-приложений, приложение может использовать эти данные для автоматического добавления подсетей в соответствующих адресных пространствах. Приложение автоматически добавляет обнаруженные подсети, если они являются вложенными в подсети, для которых включен режим автоматического добавления подсетей.

Формировать список подсетей могут только пользователи с ролью Старший сотрудник службы безопасности.

Добавление подсети

Чтобы добавить подсеть:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Адресные пространства** раскройте блок со сведениями об адресном пространстве, в которое вы хотите добавить подсеть.
4. В заголовке блока **Подсети** нажмите на значок `+`.

   В правой части окна веб-интерфейса появится область деталей.
5. В поле **Подсеть** введите адрес подсети в формате CIDR: `<базовый адрес подсети>/<количество бит в маске>`.
6. В раскрывающемся списке **Тип** выберите тип подсети в соответствии с ее назначением.

7. Установите в нужное положение переключатель **Автоматически добавлять подсети**, который включает и выключает автоматическое добавление вложенных подсетей по данным от EPP-приложений.

   Если этот режим включен, приложение добавляет в этой подсети вложенные подсети на основании данных, полученных от EPP-приложений. Для этих вложенных подсетей по умолчанию указывается тип, выбранный для текущей подсети.

8. Нажмите на кнопку **Сохранить**.

В списке подсетей появится новая подсеть на соответствующем уровне иерархии в дереве.

Изменение параметров подсети

Чтобы изменить параметры подсети:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Адресные пространства** раскройте блок со сведениями об адресном пространстве, в котором вы хотите изменить параметры подсети.
4. Раскройте блок **Подсети** и выберите нужную подсеть.

   В правой части окна веб-интерфейса появится область деталей.

5. Нажмите на кнопку **Изменить**.
6. Выполните следующие действия (в зависимости от нужного результата):

   - В поле **Подсеть** введите адрес подсети в формате CIDR: `<базовый адрес подсети>/<количество бит в маске>`.

     Адрес корневой подсети недоступен для изменения.

   - В раскрывающемся списке **Тип** выберите тип подсети в соответствии с ее назначением.

     > При изменении типа подсети учитывайте, что новый тип подсети может повлиять на выполняемые приложением действия с IP-адресами из этой подсети. Например, при выборе типа **Публичная** на карте сетевых взаимодействий перестанут отображаться соединения с устройствами, у которых заданы IP-адреса из этой подсети.

   - Установите в нужное положение переключатель **Автоматически добавлять подсети**, который включает и выключает автоматическое добавление вложенных подсетей по данным от EPP-приложений.

     Если этот режим включен, приложение добавляет в этой подсети вложенные подсети на основании данных, полученных от EPP-приложений. Для этих вложенных подсетей по умолчанию указывается тип, выбранный для текущей подсети.

7. Нажмите на кнопку **Сохранить**.

Если изменен параметр **Подсеть**, для подсети может измениться уровень иерархии в дереве.

Удаление подсетей

В списке подсетей адресного пространства вы можете удалить любую подсеть, кроме корневой подсети в дереве (подсеть 0.0.0.0/0).

Чтобы удалить подсети:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Адресные пространства** раскройте блок со сведениями об адресном пространстве, в котором вы хотите удалить подсети.
4. Раскройте блок **Подсети** и выберите подсети для удаления.

   В правой части окна веб-интерфейса появится область деталей.
5. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
6. В окне запроса подтвердите удаление подсетей.

Удаленные подсети перестанут отображаться в списке подсетей. Если удаленная подсеть содержала вложенные подсети, эти подсети останутся в списке (при этом изменится уровень иерархии этих подсетей в дереве).

Просмотр сведений об устройствах с IP-адресами из выбранных подсетей

Вы можете просмотреть сведения об устройствах, у которых заданы IP-адреса из выбранных подсетей в адресном пространстве. Сведения об устройствах выводятся в таблице устройств. В таблице устройств автоматически применяется фильтрация по адресам подсетей.

Чтобы просмотреть сведения об устройствах в таблице устройств:

1. Выберите раздел **Активы**.
2. На вкладке **Адресные пространства** раскройте блок со сведениями об адресном пространстве с нужными подсетями.
3. Раскройте блок **Подсети** и выберите подсети, для которых вы хотите просмотреть сведения об устройствах.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Показать устройства**.

Откроется вкладка **Устройства** в разделе **Активы**. В таблице устройств будет применена фильтрация по IP-адресам в адресной информации устройств.

Изменение адресного пространства

Для добавленных адресных пространств вы можете изменять имена, текстовые описания и параметры правил адресных пространств. Для адресного пространства **Default** такие изменения недоступны.

Также вы можете формировать списки подсетей для любых адресных пространств (включая список подсетей адресного пространства **Default**).

При изменении параметров правила адресного пространства требуется учитывать установленные связи этого адресного пространства и адресов, которые указаны в объектах приложения: в устройствах, рисках, правилах, событиях и прочих объектах. Если в результате изменения параметров в правилах адресного пространства удаляются связи этого адресного пространства и адресов, приложение автоматически удаляет такие адреса. Это может привести и к удалению самих объектов приложения (например, устройств), если у этих объектов не остается других адресов.

Изменять имена, текстовые описания и параметры правил адресных пространств могут только пользователи с ролью Старший сотрудник службы безопасности.

Чтобы изменить имя, текстовое описание или параметры правил адресного пространства:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.
2. Выберите раздел **Активы**.
3. На вкладке **Адресные пространства** нажмите на значок в блоке со сведениями о нужном адресном пространстве.

   В правой части окна веб-интерфейса появится область деталей.
4. Выполните следующие действия (в зависимости от нужного результата):

   - Введите имя адресного пространства.

     Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

     Имя адресного пространства должно удовлетворять следующим требованиям:

     - начинается и заканчивается любым символом, кроме пробела;
     - содержит до 255 символов;
     - не совпадает с именем другого адресного пространства (регистр символов не учитывается).

     Рекомендуется задавать имя адресного пространства длиной не более 6-8 символов. Если имя содержит большое количество символов, адресная информация может не полностью отображаться в ячейках некоторых таблиц данных (например, в таблице устройств).

   - Введите описание адресного пространства.
   - Настройте параметры правил адресного пространства.

- При необходимости добавьте и настройте дополнительные правила адресного пространства по кнопке **Добавить правило** или удалите ненужные правила с помощью значков ×.

  Общее количество правил в адресном пространстве не может превышать 10.

5. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

6. В окне запроса подтвердите изменение параметров адресного пространства.

Удаление адресного пространства

Вы можете удалять добавленные адресные пространства. Для адресного пространства **Default** возможность удаления недоступна.

При удалении адресного пространства требуется учитывать установленные связи этого адресного пространства и адресов, которые указаны в объектах приложения: в устройствах, рисках, правилах, событиях и прочих объектах. Если в результате удаления адресного пространства удаляются связи этого адресного пространства и адресов, приложение автоматически удаляет такие адреса. Это может привести и к удалению самих объектов приложения (например, устройств), если у этих объектов не остается других адресов.

Удалять адресные пространства могут только пользователи с ролью Старший сотрудник службы безопасности.

Чтобы удалить адресное пространство:

1. Подключитесь к Central Node через веб-интерфейс под учетной записью с ролью Старший сотрудник службы безопасности.

2. Выберите раздел **Активы**.

3. На вкладке **Адресные пространства** нажмите на значок в блоке со сведениями об адресном пространстве, которое вы хотите удалить.

   Откроется окно с запросом подтверждения.

4. В окне запроса подтвердите удаление адресного пространства.

Работа с картой сетевых взаимодействий

Карта сетевых взаимодействий – это визуальное отображение обнаруженных взаимодействий между устройствами. С помощью карты сетевых взаимодействий вы можете просматривать сведения о взаимодействиях устройств в различные периоды времени.

Чтобы просмотреть карту сетевых взаимодействий:

1. В окне веб-интерфейса приложения выберите раздел **Карта сети**.
2. Перейдите на вкладку **Карта сетевых взаимодействий**.

Отобразится карта сетевых взаимодействий.

На ней могут отображаться следующие объекты:

- Узлы. Эти объекты обозначают отправителей и получателей сетевых пакетов.
- Группы устройств. Эти объекты соответствуют группам в дереве групп устройств. Группы содержат узлы, представляющие включенные в эти группы устройства, и дочерние группы.
- Соединения. Эти объекты обозначают взаимодействия между узлами.

Узлы и соединения появляются на карте сетевых взаимодействий на основании данных, полученных из трафика или от Endpoint Agent за определенный промежуток времени. Группы устройств отображаются постоянно.

При необходимости вы можете использовать фильтрацию узлов и соединений. По умолчанию на карте сетевых взаимодействий в онлайн-режиме отображаются объекты с заданным периодом для фильтрации длительностью один час.

Максимальное количество соединений, которые могут отображаться на карте сетевых взаимодействий, составляет 1000.

Объекты, требующие внимания, визуально выделяются на карте сетевых взаимодействий. Приложение считает требующими внимания следующие объекты:

- Узел, если с этим узлом связаны необработанные события со значением оценки 4.0 и выше, либо если этот узел представляет устройство со статусом *Неразрешенное*.
- Соединение, если к нему относятся события со значением оценки 4.0 и выше. Учитываются события, зарегистрированные в течение заданного периода для фильтрации объектов. При этом текущий статус событий не учитывается.
- Группа, если она содержит устройства, требующие внимания, или есть требующие внимания соединения от узлов этой группы. Рассматриваются объекты как в самой группе, так и в любой дочерней группе всех уровней вложенности.

Узлы на карте сетевых взаимодействий

Узлы на карте сетевых взаимодействий могут быть следующих типов:

- Известное приложению устройство. Узел этого типа представляет устройство, входящее в таблицу устройств.
- Неизвестное приложению устройство. Узел этого типа представляет устройство с уникальным IP- или MAC-адресом, не входящее в таблицу устройств. Такой узел может появиться на карте сетевых взаимодействий, например, в случае отправки сетевых пакетов с помощью команды `ping` на адрес несуществующего устройства. Узлы неизвестных приложению устройств отображаются по отдельности, если их общее количество (в соответствии с текущими параметрами фильтрации на карте сетевых взаимодействий) не превышает 100. Если таких узлов больше, отображается один общий узел неизвестных устройств.

Отображаемая информация на узлах, представляющих известные приложению устройства

Для узлов, представляющих известные приложению устройства, при максимальном масштабе карты сетевых взаимодействий отображается следующее:

- Заданное имя устройства.
- Значок категории устройства.
- IP-адрес устройства (если IP-адрес не задан, отображается MAC-адрес).
- Различные значки в зависимости от выполнения следующих условий:
  - если для устройства задан признак маршрутизирующего устройства;
  - если на устройстве установлен Endpoint Agent (цвет значка зависит от состояния подключения);
  - если устройство имеет статус *Неиспользуемое*.
- Утолщенная линия на левой границе узла одного из следующих цветов в зависимости от состояния безопасности устройства:
  - зеленый цвет – состояние безопасности *OK*;
  - желтый цвет – состояние безопасности *Важное*;
  - красный цвет – состояние безопасности *Критическое*.

Если устройство имеет статус *Неразрешенное* или состояние безопасности устройства отличается от состояния *OK*, фон узла закрашен красным цветом.

Отображаемая информация на узлах, представляющих неизвестные приложению устройства

Для узлов, представляющих неизвестные приложению устройства, при максимальном масштабе карты сетевых взаимодействий отображается следующее:

- Если узел представляет одно неизвестное устройство, отображается IP- или MAC-адрес устройства. Если узел является общим узлом неизвестных устройств (узел, объединяющий более 100 неизвестных приложению устройств), отображается **Неизвестные устройства**.
- Значок неизвестного устройства и его статуса  .

Узлы, представляющие неизвестные приложению устройства, имеют серый цвет фона.

Группы устройств на карте сетевых взаимодействий

Группы из дерева групп устройств могут отображаться на карте сетевых взаимодействий в свернутом или развернутом состояниях. Свернутые группы отображаются в виде значков, аналогичных узлам. Развернутые группы отображаются в виде окон с включенными в них узлами и другими группами.

Отображаемая информация на свернутых группах

Если группа свернута, при максимальном масштабе карты сетевых взаимодействий отображается следующее:

- Имя группы.
- Количество устройств, удовлетворяющих текущим параметрам фильтрации на карте сетевых взаимодействий. Учитываются устройства в этой группе и в ее дочерних группах всех уровней вложенности.
- Количество дочерних групп всех уровней вложенности.

Если группа содержит устройства или соединения, требующие внимания, (в том числе в дочерних группах любого уровня вложенности), рамка этой группы окрашивается красным цветом.Отображаемая информация на развернутых группах

Окно развернутой группы содержит заголовок с именем группы и область для отображения объектов. В окне группы отображаются включенные в эту группу устройства, а также дочерние группы следующего уровня вложенности. Из числа устройств, включенных в группу, отображаются только те устройства, которые удовлетворяют текущим параметрам фильтрации на карте сетевых взаимодействий.

Если группа содержит устройства или соединения, требующие внимания, (в том числе в дочерних группах любого уровня вложенности), окно закрашено красным фоном.

Сворачивание и разворачивание групп

Если группа свернута, вы можете ее развернуть двойным щелчком мыши на значке группы. Если группа развернута, вы можете ее свернуть двойным щелчком мыши на заголовке окна этой группы или с помощью кнопки в заголовке.

Чтобы одновременно развернуть несколько свернутых групп:

1. На карте сетевых взаимодействий выберите несколько свернутых групп, выполнив одно из следующих действий:
   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными группами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные свернутые группы с помощью мыши.
2. Нажмите на кнопку в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий (кнопка доступна, если выбрана хотя бы одна свернутая группа).

Чтобы одновременно свернуть все развернутые группы,

нажмите на кнопку в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий (кнопка доступна, если развернута хотя бы одна группа).

Соединения на карте сетевых взаимодействий

Соединения на карте сетевых взаимодействий определяются по обнаруженным сетевым пакетам, в которых адреса отправителей и получателей можно сопоставить с адресами узлов.

Каждое соединение показывает две стороны взаимодействия. Стороной взаимодействия в соединении может быть один из следующих объектов на карте сетевых взаимодействий:

- узел одного из типов:
  - известное приложению устройство;
  - неизвестное приложению устройство;
  - общий узел неизвестных устройств – если соединение показывает взаимодействие с одним или несколькими неизвестными устройствами этого узла.
- свернутая группа, если соединение показывает взаимодействие с одним или несколькими устройствами в этой группе.

В зависимости от значений оценок событий, зарегистрированных при обнаружении взаимодействий, линия соединения может быть окрашена следующими цветами:

- Серый цвет – взаимодействие не вызвало регистрацию событий или зарегистрированы только события со значениями оценок 0.0–3.9.
- Красный цвет – взаимодействие вызвало регистрацию событий со значениями оценок 4.0–10.0.

Для соединений учитываются события, зарегистрированные в течение заданного периода для фильтрации объектов. При этом текущий статус событий не учитывается.

Приложение сохраняет данные о соединениях в базе данных на Central Node. Суммарный объем сохраняемых записей не может превышать заданного ограничения. Если объем превышает заданное ограничение, приложение автоматически удаляет 10% самых старых записей. Вы можете задать ограничение максимального объема для карты сетевых взаимодействий при настройке параметров хранения данных на Central Node.

Просмотр подробных сведений об объектах

Подробные сведения об объектах, представленных на карте сетевых взаимодействий, отображаются в области деталей. Для отображения подробных сведений вы можете выбрать объект с помощью мыши (если вы хотите просмотреть сведения о группе, требуется сначала свернуть группу).

Для узлов отображаются следующие сведения:

- Если узел представляет известное приложению устройство, в области деталей отображаются те же сведения, которые выводятся в таблице устройств.
- Если узел представляет одно неизвестное приложению устройство, в области деталей отображаются MAC- и/или IP-адреса устройства (с именами адресных пространств, если в приложение добавлены дополнительные адресные пространства).
- Если выбран общий узел неизвестных устройств, отображаются следующие сведения:
  - Количество узлов, которые объединяет этот узел с учетом текущих параметров фильтрации.
  - **IP-адреса** – количество IP-адресов неизвестных устройств и первые 100 IP-адресов (с именами адресных пространств, если в приложение добавлены дополнительные адресные пространства). Раздел отображается, если среди узлов неизвестных устройств есть узлы с IP-адресами.
  - **MAC-адреса** – количество MAC-адресов неизвестных устройств и первые 100 MAC-адресов (с именами адресных пространств, если в приложение добавлены дополнительные адресные пространства). Раздел отображается, если среди узлов неизвестных устройств есть узлы с MAC-адресами.

Для групп отображаются следующие сведения:

- **Родительская группа** – путь к группе в дереве групп устройств. Если группа относится к верхнему уровню иерархии, отображается **отсутствует (эта группа верхнего уровня)**.
- Количество устройств и групп в выбранной группе и в ее дочерних группах всех уровней вложенности.
- Сведения о количестве объектов, требующих внимания, в выбранной группе и в ее дочерних группах всех уровней вложенности. Если таких объектов нет, отображается состояние безопасности *OK*.

Для соединений отображаются следующие сведения:

- **Уровень важности** – значок, соответствующий максимальному уровню критичности событий, связанных с соединением. Если с соединением не связано ни одно событие, отображается **Без событий**. Учитываются события, зарегистрированные в течение заданного период для фильтрации объектов. При этом текущий статус событий не учитывается.

- Разделы с основными сведениями о первой и второй сторонах взаимодействия:

  - Если стороной взаимодействия является узел известного устройства или узел неизвестного устройства, в разделе отображается имя или адрес устройства, категория и адресная информация (при этом для известного приложению устройства адресная информация представлена только по тем сетевым интерфейсам, которые использовались при взаимодействии). Для известного устройства также отображается статус устройства.

  - Если стороной взаимодействия является свернутая группа, в разделе отображается имя группы и количество устройств и дочерних групп в ней.

  - Если стороной взаимодействия является общий узел неизвестных устройств, в разделе отображается имя узла **Неизвестные устройства** и количество узлов, объединенных в этом узле.

- **Протоколы** – раздел со списком протоколов, используемых при взаимодействии. Для каждого протокола указан объем переданных данных, вычисленный по обнаруженным сетевым пакетам. Раздел не отображается, если одной из сторон взаимодействия является общий узел неизвестных устройств.

Изменение масштаба карты сетевых взаимодействий

Карта сетевых взаимодействий может отображаться в масштабе 1–100%. Текущее значение масштаба отображается в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий.

Чтобы изменить масштаб карты сетевых взаимодействий,

используйте колесико мыши или кнопки **+** и **–**, расположенные в панели инструментов рядом с текущим значением масштаба.

При уменьшении масштаба карты сетевых взаимодействий сокращается объем выводимой информации в узлах и свернутых группах.

В масштабе отображения менее 25% в узлах и свернутых группах не отображаются значки и текстовая информация. Узлы и свернутые группы видоизменяются следующим образом:

- На узле, представляющем известное приложению устройство, в правом верхнем углу отображается статус устройства в виде треугольника одного из следующих цветов:

  - зеленый цвет – устройство имеет статус *Разрешенное*;

  - красный цвет – устройство имеет статус *Неразрешенное*;

  - серый цвет – устройство имеет статус *Неиспользуемое*.

- На свернутой группе в правом верхнем углу отображается треугольник, который обозначает признак наличия объектов, требующих внимания. Треугольник закрашен одним из следующих цветов:
  - зеленый цвет – группа не содержит объектов, требующих внимания;
  - красный цвет – группа содержит объекты, требующие внимания.

Позиционирование карты сетевых взаимодействий

При необходимости вы можете изменить позиционирование карты сетевых взаимодействий вручную или автоматически. Автоматическое позиционирование позволяет переместить карту сетевых взаимодействий и изменить ее масштаб таким образом, чтобы на экране отображались все узлы, удовлетворяющие заданным параметрам фильтрации, а также все развернутые группы.

Чтобы позиционировать карту сетевых взаимодействий вручную:

1. Наведите курсор мыши на любое место карты сетевых взаимодействий, не занятое объектами.
2. Удерживая нажатой левую кнопку мыши, перетащите изображение карты сетевых взаимодействий.

Чтобы автоматически позиционировать карту сетевых взаимодействий,

нажмите на кнопку  в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий.

Позиционирование и масштаб карты сетевых взаимодействий изменятся для отображения всех узлов и развернутых групп.

Закрепление и открепление узлов и групп

По умолчанию узлы и свернутые группы не закреплены на карте сетевых взаимодействий. Незакрепленные узлы и свернутые группы могут автоматически перемещаться для оптимального отображения остальных объектов.

Закрепление узлов и групп происходит при изменении их местоположения вручную или при автоматическом распределении. Также вы можете закрепить текущее местоположение отображаемых объектов, не перемещая их.

Для закрепления и открепления объектов без их перемещения вы можете использовать следующие элементы интерфейса:

- Кнопки в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий. С помощью кнопок и вы можете закрепить и открепить все узлы и группы, отображаемые на карте сетевых взаимодействий (в том числе узлы в развернутых группах).
- Кнопки в заголовке окна развернутой группы. С помощью кнопок и вы можете закрепить и открепить только узлы и группы в окне развернутой группы (но не в окнах вложенных групп).

Кнопки доступны, если на карте сетевых взаимодействий есть объекты, к которым можно применить соответствующие действия.

После того, как местоположение узла или свернутой группы закреплено, в правом верхнем углу этого элемента отображается значок (если для карты сетевых взаимодействий задан масштаб не менее 25%). Вы также можете использовать этот значок для открепления объекта.

Местоположение закрепленного узла или закрепленной группы сохраняется. Если закрепленный узел перестал отображаться на карте сетевых взаимодействий (например, после применения фильтрации), при следующем появлении этот узел отобразится на том же месте.

Изменение местоположения узлов и групп вручную

Вы можете вручную изменять местоположение узлов и групп на карте сетевых взаимодействий, распределяя их наиболее удобным для вас способом.

После перемещения узлы и группы закрепляются на новом местоположении. При необходимости вы можете откреплять эти объекты.

Объекты, включенные в группы, можно перемещать только в пределах окон этих групп.

Чтобы изменить местоположение узлов и/или свернутых групп:

1. На карте сетевых взаимодействий выберите один или несколько объектов, представляющих узлы и/или свернутые группы.

   Для выбора нескольких узлов и/или свернутых групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

2. С помощью мыши перетащите выбранные объекты в нужное место.

   После перемещения узлы и свернутые группы останутся закрепленными. В этих объектах появится значок .

Чтобы изменить местоположение развернутой группы,

наведите курсор на заголовок окна развернутой группы, нажмите на левую кнопку мыши и перетащите окно в нужное место.

Автоматическое распределение узлов и групп

Для оптимального размещения объектов на карте сетевых взаимодействий вы можете использовать алгоритмы автоматического изменения местоположения (распределения) узлов и групп. Предусмотрены следующие алгоритмы:

- распределение по радиальному принципу;
- распределение с выравниванием по сетке.

Вы можете использовать алгоритмы автоматического распределения для следующих объектов:

- Все отображаемые узлы и группы, относящиеся к верхнему уровню иерархии в дереве групп. Автоматическое распределение выполняется с помощью кнопок (для распределения по радиальному принципу) и (для распределения с выравниванием по сетке) в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий.

- Все отображаемые узлы и группы внутри развернутой группы. Автоматическое распределение выполняется с помощью кнопок (для распределения по радиальному принципу) и (для распределения с выравниванием по сетке) в заголовке окна развернутой группы.

- Только выбранные узлы и свернутые группы. Перед автоматическим распределением вам нужно выбрать не менее трех узлов и/или свернутых групп внутри развернутой группы или на верхнем уровне иерархии. Для выбора нескольких объектов вы можете выделить мышью прямоугольную область с нужными объектами, удерживая нажатой клавишу **SHIFT**, или выбрать нужные объекты с помощью мыши, удерживая нажатой клавишу **CTRL**. Автоматическое распределение выполняется с помощью кнопок (для распределения по радиальному принципу) и (для распределения с выравниванием по сетке) в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий.

После автоматического распределения узлы и группы закрепляются на новом месте. В этих объектах появляется значок . При необходимости вы можете открепить эти объекты.

Поиск узлов на карте сетевых взаимодействий

Вы можете выполнять поиск узлов на карте сетевых взаимодействий по сведениям об этих узлах. В поиске участвуют все узлы, удовлетворяющие текущим параметрам фильтрации, в том числе находящиеся в свернутых группах или за пределами отображаемой части карты сетевых взаимодействий.

Для узлов, представляющих известные приложению устройства, поиск выполняется по всем столбцам таблицы устройств, кроме столбцов **Статус**, **Состояние безопасности**, **Последнее появление**, **Последнее изменение** и **Создано**. Поиск также выполняется по значениям пользовательских полей для устройств.

Если найдены узлы, удовлетворяющие поисковому запросу, контуры этих узлов подсвечиваются желтым цветом. Аналогично подсвечиваются контуры свернутых групп, в которых найдены узлы. При этом в правой части поля **Поиск узлов** появляются следующие элементы:

- Порядковый номер текущего выбранного объекта (узла или свернутой группы с найденными узлами) среди результатов поиска.

- Общее количество найденных объектов (узлов и/или свернутых групп с найденными узлами).

  > В общем количестве найденных объектов не учитывается количество узлов в свернутых группах. Если вы хотите, чтобы узлы в группах также учитывались в результатах поиска, разверните свернутые группы.

- Стрелки для переходов между найденными объектами. Переходы выполняются в алфавитном порядке имен найденных объектов. При переходе к очередному объекту карта сетевых взаимодействий автоматически позиционируется для отображения этого объекта.

Чтобы найти узлы на карте сетевых взаимодействий:

Фильтрация объектов на карте сетевых взаимодействий

Этот раздел содержит инструкции по фильтрации объектов на карте сетевых взаимодействий для ограничения количества отображаемых узлов и соединений.

Комплексная фильтрация узлов и соединений

Этот раздел содержит инструкции по комплексной фильтрации узлов и соединений.

Фильтрация с помощью периода на временной шкале

Для фильтрации узлов и соединений вы можете выбрать нужный период времени на временной шкале. Временная шкала отображается в нижней части окна карты сетевых взаимодействий.

Временная шкала содержит следующие элементы:

- Дата и время начала временной шкалы.
- Периоды, когда были зарегистрированы со значениями оценок 4.0 и выше. Эти периоды отображаются в виде полос красного цвета в нижней части шкалы. Периоды не отображаются, если для временной шкалы задана длительность более семи суток.
- Период для фильтрации. Этот период отображается в виде желтой полосы, по краям которой находятся кнопки для перемещения границ.
- График объема трафика, обработанного приложением. График не отображается, если для временной шкалы задана длительность более семи суток.
- Окончание временной шкалы. В зависимости от размещения периода для фильтрации, окончание временной шкалы отображается в виде даты и времени (если заданы дата и время) или в виде ссылки **Сейчас**.

Предусмотрены следующие типы периодов для фильтрации:

- Период с привязкой к текущему моменту. Правая граница такого периода совпадает с границей временной шкалы, обозначающей текущий момент.
- Период без привязки к текущему моменту. Период этого типа может быть размещен в любой части временной шкалы.

Чтобы настроить фильтрацию объектов по периоду с привязкой к текущему моменту:

1. Нажмите на кнопку **Сейчас** справа от временной шкалы. Кнопка не отображается, если период уже привязан к текущему моменту.

2. Если требуется указать другую длительность периода, выполните одно из следующих действий:

   - Переместите левую границу желтой полосы периода в нужное положение (максимальная длительность периода – 7 дней).

   - Откройте окно настройки с помощью кнопки над желтой полосой периода, установите флажок **Прикреплять к границе**, выберите нужную длительность (**Час**, **День**, **7 дней**) и нажмите на кнопку **OK**.

На карте сетевых взаимодействий отобразятся только те узлы и соединения, для которых были обнаружены взаимодействия от начала заданного периода и до текущего момента.

Чтобы настроить фильтрацию по периоду без привязки к текущему моменту:

1. Если нужный период не входит в пределы временной шкалы, измените значения даты и времени начала и/или окончания временной шкалы:

   a. Для изменения даты и времени начала временной шкалы откройте окно по ссылке в левой части шкалы и выберите один из следующих вариантов:

      - **День**.

      - **7 дней**.

      - **30 дней**.

      - **Задать дату**. Для этого варианта укажите дату и время в открывшемся поле.

   b. Для изменения даты и времени окончания временной шкалы откройте окно по ссылке в правой части шкалы и выберите один из следующих вариантов:

      - **Сейчас**.

      - **Задать дату**. Для этого варианта укажите дату и время в открывшемся поле.

2. Задайте нужный период. Для этого выполните одно из следующих действий:

   - Переместите период в нужную часть временной шкалы с помощью мыши.

   - Переместите одну или обе границы желтой полосы периода в нужную часть временной шкалы (максимальная длительность периода – 7 дней).

   - Откройте окно настройки с помощью кнопки над желтой полосой периода, выберите нужную длительность (**Час**, **День**, **7 дней**) и нажмите на кнопку **OK**.

3. Если для периода автоматически устанавливается привязка к текущему моменту (при перемещении периода в крайнее правое положение перестает отображаться кнопка **Сейчас** справа от временной шкалы), выключите режим автоматического прикрепления периода к границе шкалы. Для этого откройте окно настройки с помощью кнопки над желтой полосой периода, снимите флажок **Прикреплять к границе** и нажмите на кнопку **OK**.

Фильтрация по зарегистрированным событиям

Вы можете отобразить на карте сетевых взаимодействий узлы и соединения, информация о которых сохранена в событиях, связанных с выбранными узлами.

Возможность фильтрации по событиям доступна, если выбрано не более 200 узлов на карте сетевых взаимодействий. Вы можете выбирать нужные узлы как по отдельности, так и в составе свернутых групп, включающих нужные устройства. При выборе свернутой группы в выборку устройств также попадают все устройства в дочерних группах любого уровня вложенности.

Фильтрацию по событиям можно выполнить следующими способами:

- Начальная фильтрация по событиям. Этот способ применяется, если требуется отфильтровать объекты по событиям, связанным только с выбранными узлами.

- Дополнительная фильтрация по событиям. Этот способ применяется, если уже выполнена начальная фильтрация по событиям (например, при переходе на карту сетевых взаимодействий из таблицы событий) и требуется добавить к фильтру события, связанные с дополнительно выбранными узлами из числа отображаемых на карте сетевых взаимодействий.

Чтобы отобразить узлы и соединения с использованием начальной фильтрации по событиям:

1. На карте сетевых взаимодействий выберите один или несколько объектов, представляющих узлы и/или свернутые группы.

   Для выбора нескольких узлов и/или групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.

   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

2. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Фильтр по событиям**.

3. В раскрывающемся списке выберите пункт **Отфильтровать**.

   На карте сетевых взаимодействий отобразятся только те узлы и соединения, информация о которых содержится в событиях, связанных с выбранными узлами. В панели инструментов, которая расположена над картой сетевых взаимодействий, появится список с идентификаторами событий (идентификаторы перечислены в порядке обнаружения связанных событий).

Чтобы добавить к отображаемым объектам узлы и соединения с использованием дополнительной фильтрации по событиям:

1. Убедитесь, что выполнена начальная фильтрация по событиям. Для этого проверьте наличие списка с идентификаторами событий в панели инструментов, которая расположена над картой сетевых взаимодействий.

2. Среди отображаемых узлов на карте сетевых взаимодействий выберите те узлы, для которых вы хотите добавить связанные события к фильтру.

   В правой части окна веб-интерфейса появится область деталей.

3. В панели инструментов. которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Фильтр по событиям**.

4. В раскрывающемся списке выберите пункт **Добавить к фильтру**.

На карте сетевых взаимодействий дополнительно отобразятся те узлы и соединения, информация о которых содержится в событиях, связанных с выбранными узлами. Идентификаторы обнаруженных событий добавятся в список с идентификаторами в панели инструментов.

Фильтрация узлов

Этот раздел содержит инструкции по фильтрации узлов.

Фильтрация узлов по статусам устройств

Чтобы отфильтровать узлы по статусам устройств:

1. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Статусы устройств**.

   Появится список, содержащий названия статусов для известных приложению устройств (*Неразрешенное*, *Разрешенное*, *Неиспользуемое*), а также статус *Неизвестное устройство* для неизвестных приложению устройств.

2. В раскрывающемся списке установите флажки для тех статусов, устройства с которыми нужно отобразить на карте сетевых взаимодействий.

3. Нажмите на кнопку **OK**.

На карте сетевых взаимодействий отобразятся только те узлы, которые представляют устройства с выбранными статусами.

Фильтрация узлов по состояниям безопасности устройств

Чтобы отфильтровать узлы по состояниям безопасности устройств:

1. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Состояния устройств**.

   Появится список, содержащий названия состояний безопасности для устройств (*OK*, *Важное*, *Критическое*).

2. В раскрывающемся списке установите флажки для тех состояний безопасности, узлы с которыми нужно отобразить на карте сетевых взаимодействий.

3. Нажмите на кнопку **OK**.

На карте сетевых взаимодействий отобразятся только те узлы, которые представляют устройства с выбранными состояниями безопасности.

Фильтрация узлов по категориям устройств

Чтобы отфильтровать узлы по категориям устройств:

1. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Категории устройств**.

   Появится список, содержащий названия категорий для известных приложению устройств, а также отдельные категории для неизвестных устройств.

2. В раскрывающемся списке установите флажки для тех категорий, устройства с которыми нужно отобразить на карте сетевых взаимодействий.

3. Нажмите на кнопку **OK**.

   На карте сетевых взаимодействий отобразятся только те узлы, которые представляют устройства выбранных категорий.

Включение и выключение отображения узлов, связанных с отфильтрованными узлами

После фильтрации узлов на карте сетевых взаимодействий отображаются только те узлы, которые удовлетворяют заданным параметрам фильтрации. При этом для отображения узла на карте сетевых взаимодействий требуется, чтобы этот узел имел соединение с другим отображаемым узлом. Если по заданным параметрам фильтрации на карте сетевых взаимодействий не отображаются все узлы, с которыми были обнаружены взаимодействия узла, этот узел также не отображается на карте сетевых взаимодействий. Для узлов, входящих в общий узел неизвестных устройств, фильтрация применяется аналогично: если не отображаются все узлы, с которыми были обнаружены взаимодействия узла неизвестного устройства, этот узел исключается из списка узлов общего узла неизвестных устройств.

При необходимости вы можете включить отображение на карте сетевых взаимодействий всех узлов, связанных с отфильтрованными узлами. Вместе с узлами, удовлетворяющими заданным параметрам фильтрации узлов, на карте сетевых взаимодействий будут отображаться все узлы, с которыми были взаимодействия (независимо от заданных параметров фильтрации).

Чтобы включить или выключить отображение узлов, связанных с отфильтрованными узлами,

используйте переключатель **Связанные устройства** в панели инструментов, которая расположена над картой сетевых взаимодействий.

Фильтрация соединений

Этот раздел содержит инструкции по фильтрации соединений.

Фильтрация соединений по значениям оценок критичности соединений

Чтобы отфильтровать соединения на карте сетевых взаимодействий по значениям оценок критичности соединений:

1. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Оценки соединений**.

   Появится список, содержащий названия уровней критичности событий с диапазонами их значений (Низкий (0.0 – 3.9), Средний (4.0 – 7.9), Высокий (8.0 – 10.0)), а также элемент **Без событий**, позволяющий выполнить фильтрацию соединений, для которых не зарегистрированы события.

2. В раскрывающемся списке установите флажки для тех уровней критичности, по которым вы хотите выполнить фильтрацию.

3. Нажмите на кнопку **OK**.

На карте сетевых взаимодействий отобразятся только те соединения, с которыми связаны события с выбранными уровнями критичности.

Фильтрация соединений по протоколам взаимодействий

Чтобы отфильтровать соединения на карте сетевых взаимодействий по протоколам взаимодействий:

1. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Протоколы**.

   Откроется окно с таблицей поддерживаемых протоколов, отображаемых в виде дерева стека протоколов. Вы можете управлять отображением элементов дерева с помощью кнопок **+** и **-** рядом с названиями протоколов, которые содержат протоколы следующих уровней.

   В столбцах таблицы представлена следующая информация:

   - **Протокол** – название протокола в дереве стека протоколов.
   - **EtherType** – номер протокола следующего уровня внутри протокола Ethernet (если протокол имеет заданный номер). Отображается в десятичном формате.
   - **IP-номер** – номер протокола следующего уровня внутри протокола IP (если протокол имеет заданный номер). Указывается только для протоколов, входящих в структуру протокола IP. Отображается в десятичном формате.

2. При необходимости воспользуйтесь поисковой строкой над таблицей, чтобы найти нужные протоколы.

3. В списке протоколов установите флажки напротив протоколов, по которым вы хотите выполнить фильтрацию.

   Если вы устанавливаете или снимаете флажок для протокола, который содержит вложенные протоколы, то для всех вложенных протоколов также автоматически устанавливаются или снимаются флажки.

4. Нажмите на кнопку **OK**.

На карте сетевых взаимодействий отобразятся только те соединения, в которых использовались выбранные протоколы.

Фильтрация соединений по уровням модели OSI

Вы можете отфильтровать соединения по уровням взаимодействий, соответствующих уровням сетевой модели стека сетевых протоколов OSI (Open Systems Interconnection).

Чтобы отфильтровать соединения на карте сетевых взаимодействий по уровням сетевой модели OSI:

1. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Уровни модели OSI**.

   Появится список, содержащий названия уровней модели OSI:

   - **Канальный**. К этому уровню относятся соединения, в которых для связи с устройствами использовались MAC-адреса.
   - **Сетевой**. К этому уровню относятся соединения, в которых для связи с устройствами использовались IP-адреса.

2. В раскрывающемся списке установите флажки для тех уровней модели OSI, для которых нужно отобразить соединения на карте сетевых взаимодействий.

3. Нажмите на кнопку **OK**.

   На карте сетевых взаимодействий отобразятся только те соединения, которые относятся к выбранному уровню модели OSI.

Сброс параметров фильтрации

Вы можете сбросить заданные параметры фильтрации узлов и соединений в состояние по умолчанию.

Чтобы сбросить заданные параметры фильтрации на карте сетевых взаимодействий,

в панели инструментов, которая расположена над картой сетевых взаимодействий, нажмите на кнопку **Фильтр по умолчанию** (кнопка отображается, если заданы параметры фильтрации).

На карте сетевых взаимодействий отобразятся все узлы и соединения, для которых были обнаружены взаимодействия в течение времени заданного периода.

Сохранение и загрузка параметров отображения карты сетевых взаимодействий

Этот раздел содержит информацию о функциях для работы с параметрами отображения карты сетевых взаимодействий.

Приложение позволяет сохранить текущие параметры отображения карты сетевых взаимодействий. Набор сохраняемых параметров отображения называется *видом*. Вы можете использовать виды для применения сохраненных в них параметров на карте сетевых взаимодействий (например, чтобы быстро восстановить параметры отображения после каких-либо изменений или для работы с картой сетевых взаимодействий на другом компьютере).

При сохранении вида карты сетевых взаимодействий сохраняются следующие параметры отображения:

- масштаб;
- позиционирование карты сетевых взаимодействий;
- местоположение закрепленных узлов и групп;
- фильтрация узлов и соединений.

В приложении можно сохранить и использовать не более 10 наборов параметров, представляющих различные виды карты сетевых взаимодействий.

Управлять списком видов карты сетевых взаимодействий (в том числе сохранять текущие параметры отображения) могут только пользователи с ролью Администратор. При этом просматривать список видов и применять сохраненные наборы параметров могут как пользователи с ролью Администратор, так и пользователи с ролями Аудитор, Старший сотрудник службы безопасности, Сотрудник службы безопасности.

Добавление нового вида с сохранением текущих параметров отображения карты сетевых взаимодействий

Чтобы добавить новый вид с сохранением текущих параметров отображения карты сетевых взаимодействий:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью **Администратор**.
2. В окне веб-интерфейса приложения выберите раздел **Карта сети**.
3. Перейдите на вкладку **Карта сетевых взаимодействий**.
4. Откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.
5. Нажмите на кнопку **Добавить**.
6. В поле ввода введите имя вида.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   Имя вида должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 100 символов;
   - не совпадает с именем другого вида (регистр символов не учитывается).
7. Нажмите на значок ✓ справа от поля ввода.

Обновление вида с сохранением текущих параметров отображения карты сетевых взаимодействий

Чтобы обновить вид с сохранением текущих параметров отображения карты сетевых взаимодействий:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью **Администратор**.
2. В окне веб-интерфейса приложения выберите раздел **Карта сети**.

   Перейдите на вкладку **Карта сетевых взаимодействий**.
3. Откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.
4. Выберите вид, в котором вы хотите сохранить текущие параметры отображения карты сетевых взаимодействий.
5. Нажмите на кнопку **Перезаписать**.

   Откроется окно с запросом подтверждения.
6. В окне запроса подтвердите сохранение текущих параметров в выбранном виде.

Переименование вида карты сетевых взаимодействий

Чтобы переименовать вид карты сетевых взаимодействий:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью **Администратор**.
2. В окне веб-интерфейса приложения выберите раздел **Карта сети**.
3. Перейдите на вкладку **Карта сетевых взаимодействий**.
4. Откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.
5. Выберите вид, который вы хотите переименовать.
6. Нажмите на значок справа от текущего имени вида.
7. В поле ввода введите новое имя вида.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   Имя вида должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 100 символов;
   - не совпадает с именем другого вида (регистр символов не учитывается).
8. Нажмите на значок справа от поля ввода.

Удаление вида карты сетевых взаимодействий

Чтобы удалить вид карты сетевых взаимодействий:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью **Администратор**.
2. В окне веб-интерфейса приложения выберите раздел **Карта сети**.
3. Перейдите на вкладку **Карта сетевых взаимодействий**.
4. Откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.
5. Выберите вид, который вы хотите удалить.
6. Нажмите на кнопку **Удалить**.
   Откроется окно с запросом подтверждения.
7. В окне запроса подтвердите удаление выбранного вида.

Применение на карте сетевых взаимодействий параметров, сохраненных в виде

Чтобы применить параметры, сохраненные в виде, на карте сетевых взаимодействий:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью **Администратор**.
2. В окне веб-интерфейса приложения выберите раздел **Карта сети**.
3. Перейдите на вкладку **Карта сетевых взаимодействий**.
4. Откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.
5. Выберите нужный вид в списке.
6. Нажмите на кнопку **Применить**.
   Откроется окно с запросом подтверждения.
7. В окне запроса подтвердите применение вида.

Мониторинг сетевых сеансов

Kaspersky Anti Targeted Attack Platform может обнаруживать в трафике сетевые сеансы, создаваемые устройствами для соединений с другими устройствами. Приложение регистрирует обнаруженные сетевые сеансы и сохраняет сведения, с помощью которых вы можете анализировать сетевую активность устройств и загружать данные о переданных сетевых пакетах из файлов дампа трафика. В отличие от соединений на карте сетевых взаимодействий, зарегистрированные сетевые сеансы позволяют получить более подробные сведения о взаимодействиях устройств, в том числе за счет раздельной регистрации сеансов для разных портов и протоколов, которые использовались при взаимодействиях.

Приложение обнаруживает сетевые сеансы, если включено применение метода Обнаружение сетевых сессий по технологии Контроль активов. Обнаружение сетевых сеансов может выполняться при анализе трафика, поступающего на точки мониторинга, а также при получении данных от компонента Endpoint Agent.

Каждый зарегистрированный сетевой сеанс содержит сведения о соединении между двумя устройствами, которые являются сторонами взаимодействия. Сетевой сеанс характеризуется адресной информацией сторон взаимодействия (MAC- и/или IP-адреса), номерами портов и прикладным протоколом, который использовался для соединения. Первым устройством в сетевом сеансе обычно считается устройство, которое инициировало отправку сетевых пакетов на другое устройство.

Вы можете посмотреть полный список протоколов, определяемых Kaspersky Anti Targeted Attack Platform в разделе *Протоколы, определяемые Kaspersky Anti Targeted Attack Platform*.

Сетевой сеанс считается завершенным, если в рамках этого сеанса не отправлялись сетевые пакеты в течение одной минуты или если технология обнаружения сетевых сессий была выключена на соответствующем узле или точке мониторинга.

При обнаружении чрезмерно большого количества сетевых сеансов в приложении применяются следующие ограничения для регистрации сеансов:

- количество регистрируемых сеансов между двумя сторонами взаимодействия с использованием одного и того же прикладного протокола – не более 1000 за одну минуту;
- общее количество регистрируемых сеансов между двумя сторонами взаимодействия – не более 5000 за одну минуту.

Приложение сохраняет данные о сетевых сеансах в базе данных на сервере Central Node. Суммарный объем сохраняемых записей не может превышать заданного ограничения. Если объем превышает заданное ограничение, приложение автоматически удаляет 10% самых старых записей.

В режиме распределенного решения и мультитенантности данные о сетевых сеансах серверов SCN не отображаются на PCN.

Таблица сетевых сеансов

Чтобы просмотреть список сетевых сеансов:

1. В окне веб-интерфейса приложения выберите раздел **Карта сети**.
2. Перейдите на вкладку **Сетевые сессии**.

Отобразится таблица сетевых сеансов.

Таблица содержит следующие сведения:

- **Статус** – статус сетевого сеанса. Зарегистрированный сетевой сеанс может иметь один из следующих статусов:
  - **Активна**. Этот статус присваивается при регистрации сетевого сеанса и сохраняется до тех пор, пока в рамках этого сеанса устройства отправляют сетевые пакеты.
  - **Завершена**. Этот статус присваивается сетевому сеансу, если в рамках этого сеанса не отправлялись сетевые пакеты в течение одной минуты или если технология обнаружения сетевых сессий была выключена на соответствующем узле или точке мониторинга.
- **Сторона 1** – MAC- и/или IP-адреса одной из сторон сетевого взаимодействия. Отображение MAC- и IP-адресов можно включать и выключать.
- **Порт стороны 1** – номер порта первой стороны взаимодействия.
- **Сторона 2** – MAC- и/или IP-адреса другой стороны сетевого взаимодействия. Отображение MAC- и IP-адресов можно включать и выключать.
- **Порт стороны 2** – номер порта второй стороны взаимодействия.
- **Устройство 1** – имя известного приложению устройства, которому соответствует адресная информация первой стороны взаимодействия.
- **Устройство 2** – имя известного приложению устройства, которому соответствует адресная информация второй стороны взаимодействия.
- **Протокол передачи** – название транспортного протокола, который использовался в сетевом сеансе.
- **Протокол приложений** – название протокола прикладного уровня, который использовался в сетевом сеансе.
- **Текущая скорость** – текущая скорость передачи данных в сетевом сеансе.
- **Средняя скорость** – средняя скорость передачи данных в сетевом сеансе.
- **Всего передано** – количество байт, переданных в сетевом сеансе.
- **Точки мониторинга** – имена точек мониторинга, на которые поступил трафик сетевого сеанса.

- **Начало** – дата и время первого сетевого пакета в сетевом сеансе или дата и время начала временного интервала, данные о котором поступили от EPP-приложения.

- **Последнее взаимодействие** – дата и время последнего сетевого пакета в сетевом сеансе или дата и время завершения временного интервала, данные о котором поступили от EPP-приложения (если в сетевом сеансе был получен только один пакет, то значение совпадает со значением параметра **Начало**).

- **Количество пакетов** – количество сетевых пакетов, переданных в сетевом сеансе.

При просмотре таблицы сетевых сеансов вы можете использовать функции настройки, фильтрации и сортировки, а также переходить к связанным элементам и экспортировать данные.

Просмотр сведений о сетевом сеансе

Подробные сведения о сетевом сеансе включают информацию из таблицы сетевых сеансов, а также название приложения, во время работы которого был инициирован сетевой сеанс (если Kaspersky Anti Targeted Attack Platform удалось определить название приложения).

Чтобы просмотреть сведения о сетевом сеансе:

1. В окне веб-интерфейса приложения выберите раздел **Карта сети**.

2. Перейдите на вкладку **Сетевые сессии**.

3. Нажмите на строку с нужным сеансом.

   Откроется окно с информацией о сетевом сеансе.

Скачивание трафика сетевых сеансов

При просмотре таблицы сетевых сеансов вы можете скачивать трафик, относящийся к выбранным сетевым сеансам. Скачивание трафика выполняется в файл формата PCAP. Для скачивания нужных данных вы можете настраивать фильтрацию сетевых пакетов.

Приложение скачивает трафик сетевых сеансов из хранилищ с файлами дампа трафика. Для скачивания может использоваться как внутреннее хранилище, созданное автоматически при установке Sensor, так и внешнее хранилище, если оно подключено.

При скачивании трафика сетевых сеансов вам нужно учитывать следующие особенности:

- Скачивание трафика возможно только для тех сетевых сеансов, которые были зарегистрированы при анализе трафика, поступившего на точки мониторинга. Если сетевой сеанс был зарегистрирован по данным, полученным от компонента Endpoint Agent, загрузить трафик этого сеанса нельзя.

- Файлы дампа трафика хранятся в хранилищах временно и автоматически удаляются по мере поступления нового трафика (периодичность удаления файлов зависит от интенсивности поступающего трафика и от заданных параметров хранения данных приложения). Скачивание трафика сетевого сеанса невозможна, если соответствующие ему файлы дампа трафика уже удалены из хранилищ.

Чтобы скачать трафик сетевых сеансов:

1. В окне веб-интерфейса приложения выберите раздел **Карта сети**.
2. Перейдите на вкладку **Сетевые сессии**.
3. Установите флажки рядом с теми сетевыми сеансами, трафик которых вы хотите скачать.

   Вы можете выбрать не более 100 сетевых сеансов.
4. Нажмите на кнопку **Скачать трафик**.

   В правой части окна веб-интерфейса появится область деталей.
5. Выполните следующие действия:

   - Если вы хотите скачать трафик за определенный период времени, задайте нужные границы с помощью параметра **Период трафика для скачивания**.

     По умолчанию задан максимально возможный период, начиная от даты и времени начала самого раннего сетевого сеанса и заканчивая датой и временем завершения самого позднего сеанса из числа выбранных сеансов. При необходимости вы можете задать границы внутри этого периода или задать пустое значение для одной из границ (например, для правой границы, чтобы скачать новый трафик еще не завершенных сеансов).

   - Задайте ограничение максимального объема для скачивания трафика в блоке **Ограничение объема скачивания**.

     Если объем скачиваемого трафика превысит заданное ограничение, будет отброшен более поздний трафик.

   - При необходимости включите фильтрацию в блоке **Фильтрация по точкам мониторинга** и укажите точки мониторинга, на которые поступал нужный трафик.

     По умолчанию заданы те точки мониторинга, на которые поступал трафик выбранных сетевых сеансов.

   - При необходимости включите фильтрацию в блоке **Фильтрация по адресным пространствам** и укажите адресные пространства, к которым относятся адреса в сетевых пакетах выбранных сетевых сеансов (блок отображается, если в приложение добавлены дополнительные адресные пространства).

     По умолчанию заданы все адресные пространства, созданные в приложении.

   - При необходимости включите фильтрацию в блоке **Фильтрация с использованием BPF** и введите выражение для фильтрации с использованием технологии BPF (Berkeley Packet Filter) по адресным параметрам в сетевых пакетах выбранных сетевых сеансов.

     Пример выражения для фильтрации:
     ```
     tcp port 102 or tcp port 502
     ```

   - При необходимости включите фильтрацию в блоке **Фильтрация с использованием регулярных выражений** и введите выражение для фильтрации по данным, составляющим полезную нагрузку в сетевых пакетах выбранных сетевых сеансов.

     Пример выражения для фильтрации:
     ```
     ^test.+xABxCD
     ```
6. Нажмите на кнопку **Скачать**.

Браузер сохранит скачанный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Поиск по сетевым пакетам

Вы можете найти и просмотреть трафик, относящийся к выбранным сетевым пакетам. При необходимости вы можете выгрузить дампы найденного трафика.

Чтобы найти трафик, относящийся к выбранным сетевым пакетам:

1. В окне веб-интерфейса приложения выберите раздел **Карта сети**.
2. Перейдите на вкладку **Сетевые сессии**.
3. Нажмите на кнопку **Поиск по пакетам**.

   Отобразится окно настройки параметров поиска по сетевым пакетам.
4. Выполните следующие действия:

   - В поле **Период трафика для скачивания** задайте границы, в рамках которых приложение будет искать сетевые пакеты.
   - При необходимости включите фильтрацию в блоке **Фильтрация с использованием BPF** и введите выражение для фильтрации с использованием технологии BPF (Berkeley Packet Filter) по адресным параметрам в сетевых пакетах выбранных сетевых сеансов. Для написания выражения фильтрации BPF используется формат libpcap. Подробнее об описании синтаксиса см. в Руководстве pcap-filter.

     Пример выражения для фильтрации:
     ```
     tcp port 102 or tcp port 502
     ```
   - При необходимости включите фильтрацию в блоке **Фильтрация с использованием регулярных выражений** и введите выражение для фильтрации по данным, составляющим полезную нагрузку в сетевых пакетах.

     Пример выражения для фильтрации:
     ```
     ^test.+xABxCD
     ```
   - При необходимости включите фильтрацию в блоке **Фильтрация по точкам мониторинга** и укажите точки мониторинга, с которых вы хотите получить трафик.
   - При необходимости включите фильтрацию в блоке **Фильтрация по адресным пространствам** и укажите адресные пространства, к которым относятся адреса в сетевых пакетах.
5. Нажмите на кнопку **Поиск**.

   В таблице отобразятся данные, соответствующие заданным критериям фильтрации.
6. Если вы хотите выгрузить дампы найденных сетевых пакетов, нажмите на кнопку **Скачать**.

Дампы сырого сетевого трафика будут выгружены в формате PCAP.

Преднастроенные правила поиска по сетевым пакетам

Вы можете выполнять поиск по трафику с помощью преднастроенных правил с использованием BPF и регулярных выражений.

Чтобы выполнить поиск по сетевым пакетам с использованием преднастроенного правила:

1. В окне веб-интерфейса приложения выберите раздел **Карта сети**.
2. Перейдите на вкладку **Сетевые сессии**.
3. Нажмите на кнопку **Поиск по пакетам**.

   Отобразится окно настройки параметров поиска по сетевым пакетам.
4. В поле **Период трафика для скачивания** задайте границы, в рамках которых приложение будет искать сетевые пакеты.
5. В таблице ниже скопируйте нужное выражение фильтрации из столбца **Фильтрация с использованием BPF** или **Фильтрация с использованием регулярных выражений** и вставьте скопированное значение в соответствующий блок в веб-интерфейсе параметров поиска по сетевым пакетам.
6. Нажмите на кнопку **Поиск**.

В таблице отобразятся данные, соответствующие заданным критериям фильтрации.

Преднастроенные правила приведены в таблице ниже.

Преднастроенные правила поиска по сетевым пакетам

Назначение правила	Фильтрация с использованием BPF	Фильтрация с использованием регулярных в
Поиск трафика по IP-адресу	`host <address>`	
Поиск трафика между двумя хостами	`host <address1> and host <address2>`	
Поиск трафика одной TCP-сессии	`tcp <port1> and host <address1> and tcp <port2> and host <address2>`	
Поиск трафика по нескольким IP-адресам	`host <address1> or host <address2> or host <addressN>`	
Поиск всех DNS-запросов от группы хостов	`udp and dst port 53 and ( src host <address1> or src host <address2> or src host <addressN> )`	
Поиск HTTP-трафика		`" HTTP/"`
Поиск DNS-трафика	`udp dst port 53 or tcp dst port 53`	

Назначение правила	Фильтрация с использованием BPF	Фильтрация с использованием регулярных в
Поиск HTTP-трафика с GET-запросом к определённому домену	`tcp port 80 or tcp port 8000 or tcp port 8080 or tcp port 8888`	`GET.{1,1000}<домен>`
Поиск ICMP-трафика конкретного хоста	`icmp and host <address>`	
Поиск аутентификационных данных, передаваемых в открытом виде	`tcp port 80 or tcp port 8000 or tcp port 8080 or tcp port 8888 or port ftp or port smtp or port imap or port pop3 or port telnet`	`"pass=|pwd=|log=|login=|user=|username=|pw=|passw=|passwd=|password=|pass:|user: |user|VXNlcm5hbWU6|UGFzc3dvcmQ6|LOGIN |USER|PASS "`
Поиск TCP-сессий, в которых хост выступает в роли клиента	`tcp[tcpflags] = tcp-syn and host <address>`	
Поиск HTTP-трафика в заданной подсети	`net xx.xx.xx.xx/yy and ( port 8080 or port 80)`	
Поиск трафика локального взаимодействия	`ip and src net (10 or 172.16/12 or 192.168/16) and dst net (10 or 172.16/12 or 192.168/16)`	
Поиск трафика взаимодействия с объектами интернет	`ip and not (src net (10 or 172.16/12 or 192.168/16) and dst net (10 or 172.16/12 or 192.168/16)) and not multicast and not broadcast and not net 169.254/16`	
Поиск трафика по полю UserAgent в HTTP-трафике	`User-Agent:`	

Протоколы, определяемые Kaspersky Anti Targeted Attack Platform

Список протоколов, определяемых Kaspersky Anti Targeted Attack Platform, приведен в таблице ниже.

Протоколы, определяемые Kaspersky Anti Targeted Attack Platform

Категория	Протокол
Протоколы канального уровня	ARP
	RARP
	Ethernet I
	Ethernet II
	MPLS
	MPLS multi
	STP
	LLDP
Протоколы сетевого уровня	IPv4
	IPv6
	IPv6 encapsulated
	IPX
	IS-IS over IP
	IS-IS over Ethernet I
	IS-IS over Ethernet II
	Loopback
	DHCP
	VRRP
Протоколы транспортного уровня	TCP
	UDP
	SCTP
	GRE
	ICMP
	IGMP
	PIM
	PRP
	QTP over UDP

Категория	Протокол
Удаленный доступ и администрирование	RDP
	SSH
	Telnet
	RLOGIN over TCP
	RSH over TCP
	VNC
	AeroAdmin
	AmmyyAdmin
	AnyDesk
	TeamViewer over TCP
	TeamViewer over UDP
	Remote Utilities
	Srv Tcp DameWare Mini Remote Control
	Radmin over TCP
Передача файлов	AFP over TCP
	FTP over TCP
	Tftp over TCP
	Tftp over UDP
	SFTP over TCP
	SMB over UDP
	Smb2 over TCP
	Smb2 over UDP
	Smb3 over TCP
	Smb3 over UDP
	BitTorrent
	NFS
Разрешение имен и сетевых сервисов	DNS
	DNS LLMNR over TCP
	DNS LLMNR over UDP
	mDNS over UDP
Почтовые протоколы	IMAP
	POP3
	SMTP
Синхронизация времени	NTP
	PTP
Аутентификация и каталоги	Kerberos
	LDAP
	LDP over UDP
	RADIUS

Категория	Протокол
Веб-протоколы и безопасность	HTTP over TCP
	HTTPS
	WebSocket
	SSL
Коммуникационные протоколы	VoIP: SIP
	IRC
	MSNP over TCP
	MSNP over UDP
Мультимедия и потоковая передача	Flash Media Server over TCP
	Voice IP: SIP
	MQTT
Облачные и файлообменные сервисы	DropBox sync over UDP
	Napster over TCP
Служебные и диагностические протоколы	ICMP
	Syslog
	Ident over TCP
	SNMP
Маршрутизация и отказоустойчивость	HSRP over UDP
	GLBP over UDP
	RIP
	EIGRP
Туннелирование и VPN	L2TP
	PPTP over TCP
	Tor over TCP
	Tor over UDP
Приложения и базы данных	Microsoft SQL
	MySQL
	Oracle
	DB2
	Tns over TCP
	Tns over UDP
Обнаружение	SSDP over UDP
Протоколы сеансового уровня	NetBIOS over TCP
	NetBIOS over UDP
Вспомогательные протоколы	Finger over TCP
Специализированные протоколы	Bitcoin over TCP

Контроль рисков

Kaspersky Anti Targeted Attack Platform может обнаруживать риски, которым подвержены ресурсы информационной системы. Приложение определяет риски по результатам анализа трафика и по полученным сведениям об устройствах.

Обнаруживаемые риски могут принадлежать следующим категориям:

- Уязвимость. К этой категории относятся обнаруженные уязвимости устройств.
- Проблемы конфигурации. К этой категории относятся риски для безопасной работы устройств из-за неверно настроенных конфигураций и риски компрометации данных при записи и чтении конфигураций устройств.
- Небезопасная архитектура сети. К этой категории относятся риски, связанные с обнаружением небезопасных сетевых взаимодействий, устройств, протоколов и программного обеспечения, риски из-за прекратившейся активности разрешенных устройств, а также риски из-за отсутствия или неполноценной работы EPP-приложений на устройствах.

Каждый риск оценивается по шкале от 0.0 до 10.0. Приложение выполняет расчет числового значения оценки для риска с учетом имеющихся сведений об устройстве, с которым связан обнаруженный риск. При расчете значения оценки приложение учитывает уровень значимости устройства, а также другие риски, связанные с этим устройством. В качестве исходного значения для расчета используется *базовая оценка*. Базовые оценки рисков категории Уязвимость определяются по общей системе оценки уязвимостей (Common Vulnerability Scoring System – CVSS). Для остальных категорий рисков используются базовые оценки, заданные в таблице типов рисков.

Информация о рисках загружается в базу данных обнаруженных рисков на Central Node. Суммарный объем сохраняемых записей в базе данных не может превышать заданное ограничение. Если объем превышает заданное ограничение, приложение автоматически удаляет 10% самых старых записей. Вы можете задать ограничение максимального объема для обнаруженных рисков при настройке параметров хранения данных.

Содержимое базы данных обнаруженных рисков отображается в разделе **Риски** веб-интерфейса приложения. Вы также можете просматривать общие сведения о наличии рисков, связанных с устройствами, в разделе **Активы** на вкладке **Устройства**.

О рисках категории Уязвимость

Риски категории Уязвимость регистрируются при обнаружении уязвимостей в контролируемых устройствах корпоративной сети. *Уязвимость* – это недостаток в программном или аппаратном обеспечении устройства, используя который злоумышленник может повлиять на работу информационной системы или получить несанкционированный доступ к информации.

Приложение обнаруживает уязвимости, анализируя имеющиеся сведения об устройствах. Сведения, по которым можно найти известную уязвимость для устройства, сравниваются с определенными полями в *базе данных известных уязвимостей*. База данных известных уязвимостей встроена в приложение. Эту базу данных формируют специалисты "Лаборатории Касперского", размещая в ней сведения о наиболее актуальных или часто встречающихся уязвимостях устройств.

База данных известных уязвимостей содержит описания уязвимостей, а также устройств, которые подвержены этим уязвимостям. Кроме того, эта база данных содержит рекомендации для защиты системы в виде текстов или ссылок на общедоступные ресурсы. В базу данных известных уязвимостей загружены описания и рекомендации из различных источников, среди которых могут быть производители устройств и программного обеспечения, а также различные организации, специализирующиеся в области безопасности. Описания и рекомендации в базе данных приводятся на английском языке.

После установки приложения используется исходная база данных известных уязвимостей. Вы можете поддерживать базу данных в актуальном состоянии, устанавливая обновления.

Kaspersky Anti Targeted Attack Platform сравнивает имеющиеся сведения об устройствах с полями в базе данных известных уязвимостей, которые описывают устройства, подверженные уязвимостям. Для обнаружения уязвимостей приложение использует следующие сведения об устройствах:

- **Производитель аппаратной части**.
- **Модель аппаратной части**.
- **Версия аппаратной части**.
- **Производитель ПО**. Если в сведениях об устройстве не была обнаружена информация о производителе ПО, Kaspersky Anti Targeted Attack Platform переиспользует значение параметра **Производитель аппаратной части**.
- **Название ПО**. Если в сведениях об устройстве не было обнаружено название ПО, Kaspersky Anti Targeted Attack Platform переиспользует значение параметра **Модель аппаратной части**.
- **Версия ПО**.

В базе данных известных уязвимостей описания устройств хранятся в формате языка CPE (Common Platform Enumeration). Приложение сравнивает имеющиеся сведения об устройствах с этими описаниями, автоматически преобразовывая сведения в формат языка CPE. Для каждой уязвимости содержимое совпавших описаний приводится в области деталей риска в разделе **Совпавшие CPE**.

Основным параметром, который идентифицирует уязвимость, является ее идентификационный номер в списке общеизвестных уязвимостей и рисков (Common Vulnerabilities and Exposures – CVE). Этот идентификационный номер называется *CVE-идентификатором*. Если уязвимости еще не присвоен CVE-идентификатор, для нее указывается идентификационный номер, полученный в других общедоступных ресурсах с описаниями уязвимостей.

В Kaspersky Anti Targeted Attack Platform поддерживается получение идентификаторов и ссылок на описания уязвимостей, предоставляемых Федеральной службой по техническому и экспортному контролю (ФСТЭК) России в Банке данных угроз безопасности информации (далее также "БДУ"). Если загружаемая информация об уязвимости содержит такие сведения из БДУ ФСТЭК, приложение отображает эти сведения в виде соответствующих идентификаторов в формате BDU:<год>-<номер>.

Сценарий реализации для процесса непрерывного управления рисками

Функциональность обнаружения рисков позволяет реализовать непрерывное (циклическое) управление рисками в вашей информационной системе. Для управления рисками Kaspersky Anti Targeted Attack Platform предоставляет информацию об обнаруженных рисках, на основе которой вы можете предпринять нужные меры по их устранению или минимизации.

Сценарий реализации для процесса непрерывного управления рисками состоит из следующих этапов:

1. **Инвентаризация устройств**

   Этот этап реализуется с использованием методов обнаружения активности устройств и обнаружения сведений об устройствах (применение методов должно быть включено). На этом этапе приложение автоматически обнаруживает новые устройства и обновляет сведения об устройствах. Если в сети есть устройства, которые не были обнаружены автоматически, вам нужно добавить их вручную или импортировать из внешних проектов.

   Для всех сведений, определяющих классификацию и эксплуатационные особенности устройств (например, информация о модели и версии программного обеспечения на устройстве), требуется включить автоматическое изменение в параметрах устройств. Если автоматическое изменение таких сведений не может выполняться по каким-либо причинам, эти сведения следует актуализировать вручную.

2. **Обнаружение рисков при пассивном и активном сканировании**

   Приложение выполняет пассивное сканирование устройств на наличие рисков, используя имеющиеся сведения об устройствах. Также для обнаружения рисков приложение анализирует сетевые взаимодействия в трафике корпоративной сети. Обнаружение рисков реализуется с использованием метода обнаружения рисков (применение метода должно быть включено).

   Вы также можете выполнять активный опрос устройств для быстрого получения сведений от этих устройств. При активном опросе устройств дополнительно предоставляются возможности обнаружения некоторых типов рисков, если выбраны соответствующие методы для анализа рисков. Для проведения активного опроса устройств вам нужно добавить в приложение один или несколько коннекторов типа **Active poll**.

   Обнаружение рисков категории Уязвимость происходит автоматически после обновления базы данных известных уязвимостей в приложении или после добавления/изменения тех сведений об устройствах, которые используются для сравнения (например, после сохранения информации о модели и версии программного обеспечения на устройстве).

3. **Оценка обнаруженных рисков и их классификация**

   Для каждого обнаруженного риска приложение выполняет расчет значения оценки. Оценка определяет уровень критичности риска. В зависимости от числового значения оценки риск может относиться к уровням критичности *Низкий* (оценки 0.0–3.9), *Средний* (оценки 4.0–7.9) или *Высокий* (оценки 8.0–10.0).

   На основании уровней критичности со значениями оценок, а также с учетом факторов, связанных с особенностями использования устройств в вашей информационной системе, вы можете классифицировать обнаруженные риски по их значимости. Если вы оцениваете риск как незначительный, его статус можно вручную изменить со статуса *Актуальный* (присвоен риску по умолчанию после обнаружения) на статус *Принят*, например, в случае, если условия для эксплуатации уязвимости не могут быть воспроизведены. При изменении статуса риска рекомендуется добавить или изменить комментарий к нему.

   Все риски, по которым требуется выполнить какие-либо дополнительные действия, следует оставить со статусом *Актуальный*.

4. **Устранение рисков**

   На этом этапе вам нужно выполнить действия, которые позволят устранить обнаруженные риски или минимизировать угрозы, связанные с возможной реализацией этих рисков. Для этого проверьте все обнаруженные риски со статусом *Актуальный*, начиная с рисков, имеющих наибольшие значения оценок. Выполните нужные действия в вашей информационной системе (например, для устранения уязвимости устройства установите необходимое обновление программного обеспечения, а если это невозможно, то изолируйте это устройство от внешних сетей). Для некоторых рисков (например, для уязвимостей) представлена информация о рекомендуемых действиях.

   Действия по устранению обнаруженных рисков выполняются без участия Kaspersky Anti Targeted Attack Platform.

5. **Проверка устранения рисков**

   Этот этап аналогичен этапу обнаружения рисков при сканировании. В результате выполнения этого этапа в таблице рисков не должно остаться рисков со статусом *Актуальный*.

   Для большинства рисков, которые приложение обнаруживает при пассивном сканировании (например, уязвимости), приложение автоматически присваивает статус *Устранен*, если перестали выполняться условия для обнаружения этих рисков. Например, после изменения сведений о версии программного обеспечения на устройстве приложение присваивает статус *Устранен* риску категории Уязвимость, который был зарегистрирован из-за указанной ранее уязвимой версии программного обеспечения. Статус *Устранен* также присваивается тем рискам, для которых больше нет описания в базе данных известных уязвимостей (в случае удаления описания из базы данных после загрузки обновлений).

   При удалении устройств приложение удаляет и риски, которые были связаны с этими устройствами.

   Если после выполнения действий по устранению риска не изменились условия для его обнаружения (например, уязвимое устройство изолировано от внешних сетей, но сведения об этом устройстве не изменились), вы можете вручную присвоить этому риску статус *Принят*. При изменении статуса риска рекомендуется добавить или изменить комментарий к нему.

   Некоторые риски не предусматривают автоматического присвоения статуса *Устранен* (например, автоматическое присвоение статуса *Устранен* не выполняется для рисков, обнаруженных при активном опросе устройств). Для таких рисков также требуется вручную присвоить статус *Принят* после выполнения действий по устранению риска.

   Если риск связан с событием, вы можете присвоить этому риску статус *Принят* одновременно с изменением статуса события на статус *Обработано*.

Просмотр таблицы рисков

Таблица рисков отображается в разделе **Риски и аномалии** окна веб-интерфейса приложения.

Параметры рисков отображаются в следующих столбцах таблицы:

- **Категория**.

  Название категории риска.

- **Название**.

  Название риска. Для риска категории Уязвимость используется CVE-идентификатор обнаруженной уязвимости (если CVE-идентификатор отсутствует, отображается идентификационный номер, полученный в других общедоступных ресурсах с описаниями уязвимостей).

- **CVE**.

  Для риска категории Уязвимость: CVE-идентификатор обнаруженной уязвимости.

- **БДУ**.

  Для риска категории Уязвимость: идентификатор уязвимости в базе БДУ. Если одной уязвимости с CVE-идентификатором соответствуют несколько уязвимостей с разными идентификаторами в базе БДУ, столбец содержит все такие идентификаторы.

- **ID риска**.

  Уникальный идентификатор риска.

- **Оценка**.

  Рассчитанное значение оценки для риска. Числовое значение определяет, к какому уровню критичности относится риск. В зависимости от уровня критичности, значение оценки может быть окрашено одним из следующих цветов:

  - Красный – риск с уровнем критичности *Высокий*.
  - Желтый – риск с уровнем критичности *Средний*.
  - Синий – риск с уровнем критичности *Низкий*.

  Для рисков со статусом *Актуальный* значение оценки окрашено ярким цветом. Если риску присвоен статус *Устранен* или *Принят*, его значение оценки окрашено бледным цветом.

  В области деталей этот параметр называется **Базовая оценка**.

- **Сторона 1**.

  Адресная информация одной из сторон сетевого взаимодействия (указывается для некоторых типов рисков). Отображение MAC- и IP-адресов можно включать и выключать по отдельности. Если в приложении добавлены дополнительные адресные пространства, при настройке таблицы рисков можно включать и выключать отображение имен адресных пространств с помощью параметра **Отображать адресные пространства**.

- **Сторона 2**.

  Адресная информация другой стороны сетевого взаимодействия (указывается для некоторых типов рисков). Отображение адресной информации можно настраивать аналогично, как для столбца **Сторона 1**.

- **Группа устройств**.

  Имя группы, в которую помещено устройство с обнаруженным риском (содержит имя самой группы и имена всех ее родительских групп).

- **Устройство**.

  Имя и адрес устройства.

- **Источник**.

  Для риска категории Уязвимость: название источника, из которого загружены сведения в базу данных известных уязвимостей. В области деталей этот параметр называется **Источник уязвимости**.

- **Статус**.

Текущий статус риска. Предусмотрены следующие статусы:

- *Актуальный* – статус по умолчанию при первом обнаружении риска (а также при повторном обнаружении, если риску был присвоен статус *Устранен*). Также риску можно вручную присвоить статус *Актуальный*, если его текущий статус *Принят*.
- *Устранен* – автоматически присваиваемый статус, если перестали выполняться условия для обнаружения риска.
- *Принят* – статус, присваиваемый риску вручную, если риск оценивается как незначительный или если действия по устранению риска не привели к автоматическому присвоению статуса *Устранен*.

- **Обнаружен**.

  Дата и время обнаружения риска.

- **Последнее изменение статуса**.

  Дата и время последнего изменения статуса риска.

- **Совпавшие CPE**.

  Для риска категории Уязвимость: описания устройств, хранящиеся в базе данных известных уязвимостей. Приводятся описания, которые совпали со сведениями об устройстве в таблице устройств.

При просмотре таблицы рисков вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Просмотр сведений о риске

Подробные сведения о риске включают информацию из таблицы рисков, а также следующие поля:

- **Тип риска** – код типа риска.
- **Описание** – описание, заданное для типа риска или для уязвимости.
- **Базовая оценка** – исходное значение для расчета числового значения оценки риска.

Для риска категории Уязвимость выводится дополнительная информация в следующих полях и группах полей:

- **Вектор CVSS** – запись метрик для вычисления оценки уязвимости по системе CVSS.
- **Условия эксплуатации уязвимости** – описание условий эксплуатации уязвимости.
- **Возможные последствия** – описание возможных последствий при эксплуатации уязвимости.
- **Рекомендации** – рекомендации по устранению уязвимости (например, сведения о том, какую версию программного обеспечения рекомендуется установить на устройстве).
- **Ссылки** – ссылки на общедоступные ресурсы с дополнительными сведениями об уязвимости.
- **История CVE** – даты этапов выявления, подтверждения и публикации уязвимости в общедоступных источниках.

Чтобы просмотреть сведения о риске:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Устройства**.
3. Нажмите на название уязвимости (в виде CVE-идентификатора или другого идентификационного номера уязвимости) в столбце **Риски**.

   Откроется окно с информацией об уязвимости.

Изменение статусов рисков вручную

При работе в разделе **Риски и аномалии** вы можете вручную изменять статусы любых рисков со статуса *Актуальный* на статус *Принят* и обратно. При работе в разделе **Активы** вы можете менять статус только рисков категории Уязвимость и только со статуса *Актуальный* на статус *Принят*.

Также вы можете присвоить риску статус *Принят* при присвоении статуса *Обработано* событиям, которые связаны с этим риском.

Чтобы изменить статус риска вручную:

1. Откройте область деталей риска или окно с подробными сведениями о риске.
2. Откройте раскрывающийся список **Изменить статус**.
3. В зависимости от того, какой статус вы хотите присвоить риску, в раскрывающемся списке выберите один из следующих пунктов:

   - **Принят** – если вы хотите изменить статус риска со статуса *Актуальный* на статус *Принят*.
   - **Актуальный** – если вы хотите вернуть риску статус *Актуальный*.

   Откроется окно с запросом подтверждения.
4. Если с выбранным риском связаны события и вы хотите одновременно присвоить статус *Обработано* всем этим событиям, установите флажок **Присвоить статус Обработано всем связанным событиям**.

   Риски могут быть связаны с событиями при регистрации событий некоторых типов по технологии Контроль активов.
5. В окне запроса нажмите на кнопку **ОК**.

Просмотр сведений о рисках при работе с таблицей устройств

При работе с таблицей устройств вы можете просматривать сведения о рисках, которые были обнаружены на устройствах. Для каждого устройства с рисками категории Уязвимость отображаются названия обнаруженных уязвимостей (в виде CVE-идентификаторов или других идентификационных номеров уязвимостей). Если на устройстве обнаружены риски других категорий, для этого устройства отображаются названия этих категорий рисков. Названия уязвимостей и категорий рисков отображаются в столбце **Риски** и в области деталей при выборе устройства.

По умолчанию в таблице устройств отображаются сведения только о тех рисках, которым присвоен статус *Актуальный*. При необходимости вы можете включить отображение сведений обо всех рисках, установив флажок **Отображать устраненные и принятые риски** при настройке таблицы устройств.

Для обозначения уровней критичности рисков названия уязвимостей и категорий окрашиваются одним из следующих цветов:

- Красный – риски с уровнем критичности *Высокий*.
- Желтый – риски с уровнем критичности *Средний*.
- Синий – риски с уровнем критичности *Низкий*.

Для рисков со статусом *Актуальный* названия окрашены ярким цветом. Для рисков со статусом *Устранен* или *Принят* названия окрашены бледным цветом.

Если с устройством связаны риски одной и той же категории, название этой категории окрашивается цветом наиболее высокого уровня критичности из всех этих рисков.

Если вы хотите просмотреть подробные сведения о рисках, вы можете использовать отображаемые названия уязвимостей и категорий рисков. При нажатии на название уязвимости (в виде CVE-идентификатора или другого идентификационного номера уязвимости) открывается окно деталей уязвимости. При нажатии на название категории риска приложение выполняет переход к таблице рисков и применяет фильтрацию для отображения рисков выбранной категории, связанных с устройством.

При просмотре таблицы устройств вы можете настроить параметры фильтрации устройств по связанным с ними рискам. Также вы можете выполнять поиск устройств по названиям уязвимостей (в виде CVE-идентификаторов или других идентификационных номеров уязвимостей).

Настройка типов событий NDR

Типы событий задают параметры, используемые при регистрации событий: заголовки, описания, базовые оценки и параметры регистрации. В Kaspersky Anti Targeted Attack Platform вы можете просматривать параметры типов событий, изменять некоторые параметры типов событий и настраивать автоматическое сохранение трафика и передачу зарегистрированных событий через коннекторы.

Просмотр таблицы типов событий

Предусмотренные в приложении типы событий отображаются в разделе **Параметры**, подразделе **Типы событий** веб-интерфейса приложения.

Таблица типов событий содержит *системные типы событий*. Эти типы событий создаются приложением при установке и не могут быть удалены из списка. Для реализованных в приложении технологий регистрации событий используются различные наборы системных типов событий.

На основе некоторых системных типов событий могут быть настроены *пользовательские параметры событий*, которые будут использоваться при регистрации событий в определенных случаях. Пользовательские параметры могут быть заданы для типа события по технологии Внешние системы с кодом 4000005400 – для регистрации событий с использованием NDR API.

Пользовательские параметры имеют приоритет при регистрации событий. Параметры, заданные в системных типах событий, используются в том случае, если не заданы пользовательские параметры.

Для типов событий предусмотрены следующие параметры:

- **Код** – уникальный номер типа события. В таблице типов событий номер отображается вместе с заголовком события в столбце **Код и заголовок**. В таблице зарегистрированных событий номер типа события отображается в столбце **Тип события**.

- **Заголовок** – содержимое заголовка события, представленное текстом и/или переменными. В системных типах событий могут использоваться специфические переменные только для этих типов событий или общие переменные, которые также можно использовать и в пользовательских параметрах. В таблице типов событий содержимое заголовка отображается вместе с номером типа события в столбце **Код и заголовок**. В таблице зарегистрированных событий текст заголовка и/или полученные значения переменных отображаются в столбце **Заголовок**.

- **Базовая оценка** – исходное значение для расчета оценки зарегистрированного события. Если у типа события могут быть различные базовые оценки, то отображается максимальное значение. Этот параметр отображается в таблице типов событий.

- **Технология** – технология регистрации события. Этот параметр отображается в таблице типов событий.

- **Описание** – дополнительный текст, описывающий тип события. Аналогично заголовку, может содержать переменные. Этот параметр не отображается в таблице типов событий. Вы можете просмотреть описание в области деталей выбранного типа события. В таблице зарегистрированных событий текст описания и/или полученные значения переменных отображаются в столбце **Описание**.

- **<Имя коннектора-получателя>** – имя коннектора, через который приложение передает события в стороннюю систему. Приложение передает в сторонние системы события только тех типов, для которых настроена передача событий через коннектор. Каждый коннектор, через который настроена передача событий в сторонние системы, отображается в отдельном столбце таблицы типов рисков. Этот параметр не отображается в области деталей выбранного типа событий.

- **Время разрешения повтора события** – максимальный период времени, по истечении которого разрешается повторная регистрация события. Если до истечения заданного периода времени повторяются условия для регистрации события, то новое событие не регистрируется, а увеличивается счетчик количества повторов ранее зарегистрированного события и обновляются дата и время последнего появления события. После окончания этого периода при повторении условий для регистрации события приложение зарегистрирует новое событие такого типа. Период разрешения повтора отсчитывается от момента последней регистрации события такого типа. Например, если задано время 8 часов, то при обнаружении условий для регистрации этого события через два часа после предыдущего события, новое событие не будет зарегистрировано. Новое событие будет зарегистрировано при обнаружении условий для регистрации через 8 часов и более. Этот параметр не отображается в таблице типов событий. Вы можете просмотреть и настроить этот параметр в области деталей выбранного типа события.

  Для зарегистрированных событий время разрешения повтора может наступить раньше заданного периода. Повторная регистрация события разрешается раньше заданного периода, если событию присвоен статус *Обработано*, а также если был перезагружен компьютер, на котором установлен Central Node.

- **Сохранять трафик** – параметр для включения и выключения автоматического сохранения трафика при регистрации события. Этот параметр не отображается в таблице типов событий. Вы можете просмотреть и настроить этот параметр в области деталей выбранного типа события.

  Если автоматическое сохранение трафика выключено, вы можете загружать трафик вручную в течение некоторого времени после регистрации события этого типа. При поступлении запроса на загрузку трафика приложение выполняет поиск сетевых пакетов в файлах дампа трафика, временно создаваемых приложением. Если в файлах дампа трафика найдены нужные сетевые пакеты, они загружаются (с предварительным сохранением в базе данных).

При просмотре таблицы типов событий вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Изменение параметров системного типа события

Чтобы изменить параметры системного типа события:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Типы событий**.
2. В таблице типов событий выберите тип события, который вы хотите изменить.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.
4. Настройте изменяемые параметры: время разрешения повтора события и параметры сохранения трафика.
5. Нажмите на кнопку **Сохранить**.

Настройка автоматического сохранения трафика для системных типов событий

При изменении типов событий вы можете включать и выключать автоматическое сохранение трафика для событий при их регистрации. Если сохранение трафика включено, в базе данных сохраняется сетевой пакет, вызвавший регистрацию события, а также пакеты до и после регистрации события, обнаруженные в рамках сетевого сеанса, в котором было зарегистрировано событие. Параметры сохранения трафика определяют количество сохраняемых сетевых пакетов и ограничения по времени.

Если автоматическое сохранение трафика выключено для типа события и для этого типа события не заданы пользовательские параметры, включающие автоматическое сохранение трафика, возможность загрузки трафика будет доступна только в течение некоторого времени после регистрации события этого типа. В этом случае для загрузки трафика приложение использует файлы дампа трафика. Эти файлы хранятся временно и автоматически удаляются по мере поступления трафика. При загрузке трафика из этих файлов в базе данных сохраняются сетевые пакеты в том объеме, который задан по умолчанию при включении сохранения трафика для типов событий.

> Приложение сохраняет трафик в базе данных только при регистрации события. Если в течение времени разрешения повтора события повторяются условия для регистрации этого события, трафик на этот момент времени не сохраняется в базе данных.

Вы можете включить и настроить сохранение трафика для любых типов событий.

Если включено сохранение трафика для агрегирующих событий (то есть для системного типа события, которому присвоен код 8000000001), то при регистрации агрегирующего события приложение сохраняет трафик для всех вложенных событий. Для сохранения трафика вложенных событий применяются параметры, заданные для агрегирующего события. При этом параметры сохранения трафика, заданные непосредственно для типов событий, вложенных в агрегирующее событие, имеют приоритет перед параметрами, заданными для агрегирующего события. То есть трафик для вложенных событий будет сохранен в соответствии с параметрами, заданными для типов этих событий, а при отсутствии таких параметров – в соответствии с параметрами, заданными для агрегирующего события.

Чтобы включить и настроить параметры сохранения трафика для типа события:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Типы событий**.
2. В таблице типов событий выберите тип события, который вы хотите изменить.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.
4. Установите переключатель **Сохранять трафик** в положение *Включено*.
5. Настройте сохранение трафика до момента регистрации события. Для этого укажите нужные значения в полях **Пакетов до события, шт.** и/или **Время до события, мс**. При нулевом значении параметр не применяется. Если значения заданы в обоих этих полях, приложение будет сохранять минимальное количество пакетов, которое соответствует одному из заданных значений.

6. Настройте сохранение трафика после момента регистрации события. Для этого укажите нужные значения в полях **Пакетов после события, шт.** и/или **Время после события, мс**. При нулевом значении параметр не применяется. Если значения заданы в обоих этих полях, приложение будет сохранять минимальное количество пакетов, которое соответствует одному из заданных значений.

   Для некоторых технологий (в частности, Контроль технологического процесса) в событиях может сохраняться меньше пакетов после момента регистрации, чем задано параметрами сохранения трафика. Это связано с технологическими особенностями отслеживания трафика.

7. Нажмите на кнопку **Сохранить**.

Настройка передачи событий через коннекторы

При настройке системных типов событий вы можете указать коннекторы, через которые Kaspersky Anti Targeted Attack Platform будет передавать зарегистрированные события в сторонние системы. Kaspersky Anti Targeted Attack Platform может передавать информацию о событиях одновременно через несколько коннекторов.

Чтобы настроить передачу событий через коннекторы в сторонние системы:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Типы событий**.
2. Убедитесь, что в таблице типов событий отображаются столбцы с нужными коннекторами.

   Если столбец с нужным коннектором отсутствует, проверьте параметры отображения столбцов. Если коннектор не был добавлен в список коннекторов, добавьте его.

3. В таблице типов событий выберите типы событий, для которых вы хотите включить или выключить передачу через коннекторы.

   Если вы выбрали один тип события, в правой части окна веб-интерфейса появится область деталей.

4. Выполните одно из следующих действий:

   - Если вы выбрали один тип события, в области деталей нажмите на кнопку **Выбрать коннекторы**.
   - Если вы выбрали несколько типов событий, в верхней части окна нажмите на кнопку **Выбрать коннекторы**.

   Откроется окно **Коннекторы-получатели событий**.

5. Установите флажки напротив тех коннекторов, через которые вы хотите передавать события в сторонние системы.
6. Нажмите на кнопку **OK**.

Общие переменные для подстановки значений в Kaspersky Anti Targeted Attack Platform

Для подстановки текущих значений в Kaspersky Anti Targeted Attack Platform могут использоваться общие переменные. Вы можете использовать общие переменные в следующих параметрах:

- заголовки и описания событий в пользовательских параметрах для регистрации событий;
- параметры передачи событий, сообщений приложения или записей аудита через коннектор для электронной почты.

Чтобы вставить общую переменную в поле ввода,

начните вводить имя переменной с символа $ и выберите подходящую общую переменную в появившемся списке.

В зависимости от своего назначения, общие переменные могут использоваться для подстановки значений в различных параметрах (см. таблицу ниже).

Общие переменные для подстановки значений

Переменная	Назначение	Где используется
`$communications`	Строки описания сетевых взаимодействий (по одной строке на каждое сетевое взаимодействие) с указанием протокола и адресов отправителя и получателя сетевого пакета	• Пользовательские параметры для регистрации событий. • Параметры передачи событий через коннектор.
`$dst_address`	Адрес получателя сетевого пакета (в зависимости от доступных в протоколе данных это могут быть IP-адрес, номер порта, MAC-адрес и/или другие адресные данные)	• Пользовательские параметры для регистрации событий.
`$extra.<paramName>`	Дополнительная переменная, добавленная с помощью функции `AddEventParam` для внешней системы или Lua-скрипта	• Пользовательские параметры для регистрации событий.
`$monitoring_point`	Имя точки мониторинга, трафик с которой вызвал регистрацию события	• Пользовательские параметры для регистрации событий. • Параметры передачи событий через коннектор.
`$occurred`	Дата и время регистрации	• Пользовательские параметры для регистрации событий. • Параметры передачи событий через коннектор. • Параметры передачи сообщений приложения через коннектор. • Параметры передачи записей аудита через коннектор.
`$protocol`	Название протокола прикладного уровня, при отслеживании которого зарегистрировано событие	• Пользовательские параметры для регистрации событий.
`$src_address`	Адрес отправителя сетевого пакета (в зависимости от доступных в протоколе данных это могут быть IP-адрес, номер порта, MAC-адрес и/или другие адресные данные)	• Пользовательские параметры для регистрации событий.
`$technology_rule`	Имя правила в событии	• Пользовательские параметры для регистрации событий. • Параметры передачи событий через коннектор.
`$top_level_protocol`	Название протокола верхнего уровня	• Пользовательские параметры для регистрации событий.
`$type_id`	Код типа события, сообщения приложения или записи аудита	• Пользовательские параметры для регистрации событий (также может использоваться переменная `$event_type_id`). • Параметры передачи событий через коннектор. • Параметры передачи сообщений приложения через коннектор. • Параметры передачи записей аудита через коннектор.
`$closed`	Дата и время присвоения статуса *Обработано* или дата и время разрешения повтора события (для событий, не являющихся агрегирующими событиями), либо дата и время регистрации последнего события, включенного в агрегирующее событие (для агрегирующих событий)	• Параметры передачи событий через коннектор.
`$count`	Количество срабатываний вложенного или агрегирующего события	• Параметры передачи событий через коннектор.
`$description`	Описание	• Параметры передачи событий через коннектор. • Параметры передачи сообщений приложения через коннектор. • Параметры передачи записей аудита через коннектор.
`$id`	Уникальный идентификатор зарегистрированного события, сообщения приложения или записи аудита	• Параметры передачи событий через коннектор. • Параметры передачи сообщений приложения через коннектор. • Параметры передачи записей аудита через коннектор.

`$message_category`	Категория переданных данных (событие, сообщение приложения или запись аудита)	• Параметры передачи событий через коннектор. • Параметры передачи сообщений приложения через коннектор. • Параметры передачи записей аудита через коннектор.
`$message_count`	Количество передаваемых событий, сообщений приложения или записей аудита	• Параметры передачи событий через коннектор. • Параметры передачи сообщений приложения через коннектор. • Параметры передачи записей аудита через коннектор.
`$messages`	Шаблон, представляющий собой блок со списком данных	• Параметры передачи событий через коннектор. • Параметры передачи сообщений приложения через коннектор. • Параметры передачи записей аудита через коннектор.
`$msg_line_templ`	Шаблон строк для уведомлений в письмах	• Параметры передачи событий через коннектор. • Параметры передачи сообщений приложения через коннектор. • Параметры передачи записей аудита через коннектор.
`$node`	Узел с установленным компонентом приложения, от которого поступили данные	• Параметры передачи сообщений приложения через коннектор. • Параметры передачи записей аудита через коннектор.
`$result`	Результат действия в записи аудита	• Параметры передачи записей аудита через коннектор.
`$score`	Значение оценки события	• Параметры передачи событий через коннектор.
`$severity`	Уровень критичности события	• Параметры передачи событий через коннектор.
`$status`	Статус сообщения приложения	• Параметры передачи сообщений приложения через коннектор.
`$system_process`	Процесс приложения, который вызвал регистрацию сообщения	• Параметры передачи сообщений приложения через коннектор.
`$technology`	Технология, к которой относится событие	• Параметры передачи событий через коннектор.
`$title`	Заголовок события, текст сообщения или зарегистрированное действие	• Параметры передачи событий через коннектор. • Параметры передачи сообщений приложения через коннектор. • Параметры передачи записей аудита через коннектор.
`$user`	Имя пользователя, который совершил зарегистрированное действие	• Параметры передачи записей аудита через коннектор.

Технологии регистрации событий NDR

Kaspersky Anti Targeted Attack Platform регистрирует события NDR по одной из следующих технологий:

- *Обнаружение вторжений* (IDS).

  По этой технологии регистрируются события NDR, связанные с обнаружением в трафике аномалий, которые являются признаками атак (например, событие NDR при обнаружении признаков ARP-спуфинга).

- *Внешние системы* (EXT).

  К этой технологии относятся агрегирующие и вложенные события NDR, которые поступают в Kaspersky Anti Targeted Attack Platform от сторонних систем с использованием методов API NDR.

- *Контроль активов* (AM).

  По этой технологии регистрируются события NDR, связанные с обнаружением информации об устройствах в трафике или в полученных данных от EPP-приложений (например, событие NDR при обнаружении нового IP-адреса у устройства).

- *Защита конечных устройств* (EPP).

  По этой технологии регистрируются события NDR об угрозах, обнаруженных приложениями "Лаборатории Касперского", которые выполняют функции защиты рабочих станций и серверов (например, событие при обнаружении вредоносной программы).

Системные типы событий в Kaspersky Anti Targeted Attack Platform

Для регистрации событий в Kaspersky Anti Targeted Attack Platform используются системные типы событий, автоматически созданные при установке приложения.

Каждый тип события относится к определенной технологии регистрации событий.

Системные типы событий по технологии Обнаружение вторжений

В этой статье приведено описание системных типов событий, относящихся к технологии Обнаружение вторжений (см. таблицу ниже).

Системные типы событий по технологии Обнаружение вторжений (IDS)

Код	Заголовок типа события	Условия для регистрации
4000003000	Сработало правило из набора $fileName (системный набор правил)	Сработало правило обнаружения вторжений, входящее в системный набор правил. В заголовке и в описании типа события используются следующие переменные: • $fileName – название набора правил; • $category – класс правила; • $ruleName – название правила; • $signature_id – идентификатор правила (sid).
4000003001	Сработало правило из набора $fileName (пользовательский набор правил)	Сработало правило обнаружения вторжений, входящее в пользовательский набор правил. В заголовке и в описании типа события используются следующие переменные: • $fileName – название набора правил; • $category – класс правила; • $ruleName – название правила; • $signature_id – идентификатор правила (sid); • $action – тип действия с сетевыми пакетами, заданный в правиле (действия типов `drop` или `reject` не выполняются в Kaspersky Anti Targeted Attack Platform).
4000003002	Обнаружены признаки подбора или сканирования	Сработало правило обнаружения атак с использованием методов подбора или сканирования. В описании типа события используется переменная $ruleName для названия правила.

Код	Заголовок типа события	Условия для регистрации
4000004001	Обнаружены признаки ARP-спуфинга в ARP-ответах	Обнаружены признаки подмены адресов в ARP-пакетах: несколько ARP-ответов, которые не связаны с ARP-запросами. В описании типа события используются следующие переменные: • $senderIp – подменяемый IP-адрес; • $targetIp – IP-адрес целевого узла; • $attackStartTimestamp – время обнаружения первого ARP-ответа.
4000004002	Обнаружены признаки ARP-спуфинга в ARP-запросах	Обнаружены признаки подмены адресов в ARP-пакетах: несколько ARP-запросов с одного MAC-адреса разным получателям. В описании типа события используются следующие переменные: • $senderIp – подменяемый IP-адрес; • $targetIp – IP-адрес целевого узла; • $attackStartTimestamp – время обнаружения первого ARP-ответа.
4000005100	Обнаружена аномалия в протоколе IP: конфликт данных при сборке IP-пакета	Обнаружена аномалия в протоколе IP: при наложении фрагментов IP-пакета данные не совпадают.
4000005101	Обнаружена аномалия в протоколе IP: превышение размера фрагментированного IP-пакета	Обнаружена аномалия в протоколе IP: фактический суммарный размер фрагментированного IP-пакета после сборки превышает допустимый предел.
4000005102	Обнаружена аномалия в протоколе IP: размер начального фрагмента IP-пакета меньше ожидаемого	Обнаружена аномалия в протоколе IP: размер начального фрагмента IP-пакета меньше минимально допустимого значения.
4000005103	Обнаружена аномалия в протоколе IP: несоответствие фрагментов IP-пакета (mis-associated fragments)	Обнаружена аномалия в протоколе IP: фрагменты собираемого IP-пакета содержат различные данные о длине фрагментированного пакета.
4000002701	Обнаружена аномалия в протоколе TCP: подмена содержимого в перекрывающихся TCP-сегментах	Обнаружена аномалия в протоколе TCP: пакеты содержат перекрывающиеся TCP-сегменты с различающимся содержимым.
4000000003	Тестовое событие (IDS)	Обнаружен тестовый сетевой пакет (при включенном методе обнаружения вторжений по правилам).

Системные типы событий по технологии Контроль активов

В этой статье приведено описание системных типов событий, относящихся к технологии Контроль активов (см. таблицу ниже).

Системные типы событий по технологии Контроль активов (AM)

Код	Заголовок типа события	Условия для регистрации
4000005003	Обнаружено новое устройство с адресом $owner_ip_or_mac	В режиме наблюдения контроля активов автоматически добавлено новое устройство по обнаруженному IP- или MAC-адресу, который не указан для других устройств в таблице. Одновременно с регистрацией события приложение может зарегистрировать для этого устройства и риск **Неразрешенное устройство**. В этом случае устанавливается связь риска и события. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – присвоенное имя устройства; • $assigned_mac – присвоенный MAC-адрес (если определен); • $owner_ip – присвоенный IP-адрес (если определен); • $asset_id – идентификатор устройства.
4000005004	Получена новая информация об устройстве с адресом $owner_ip_or_mac	В режиме наблюдения контроля активов автоматически обновлены сведения об устройстве на основе полученных данных из трафика. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – имя устройства; • $updated_params – список обновленных сведений; • $asset_id – идентификатор устройства.

Код	Заголовок типа события	Условия для регистрации
4000005005	Обнаружен конфликт IP-адреса $owner_ip	В режиме наблюдения контроля активов обнаружено использование IP-адреса не тем устройством, для которого был указан этот IP-адрес. В заголовке и в описании типа события используются следующие переменные: • $owner_ip – IP-адрес; • $challenger_asset_name – имя устройства, которое использовало IP-адрес; • $challenger_mac – MAC-адрес устройства, которое использовало IP-адрес; • $asset_name – имя устройства, в параметрах которого был указан IP-адрес; • $owner_mac – MAC-адрес устройства, в параметрах которого был указан IP-адрес; • $challenger_ips_list – список других IP-адресов устройства, которое использовало IP-адрес; • $asset_id – идентификатор устройства, в параметрах которого был указан IP-адрес; • $challenger_id – идентификатор устройства, которое использовало IP-адрес.
4000005006	Обнаружен трафик с адреса $owner_ip_or_mac, который закреплен за устройством со статусом Неиспользуемое	В режиме наблюдения контроля активов или по полученным данным от EPP-приложения обнаружена активность устройства, которому был присвоен статус *Неиспользуемое*. Одновременно с регистрацией события приложение может зарегистрировать для этого устройства и риск **Неразрешенное устройство**. В этом случае устанавливается связь риска и события. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – имя устройства; • $last_seen_timestamp – дата и время последнего появления устройства в сети; • $asset_id – идентификатор устройства.
4000005007	Обнаружен новый IP-адрес $new_ip_addr у устройства с MAC-адресом $owner_mac	В режиме наблюдения контроля активов обнаружен новый IP-адрес, использованный устройством. В заголовке и в описании типа события используются следующие переменные: • $new_ip_addr – обнаруженный IP-адрес; • $owner_mac – MAC-адрес устройства; • $asset_name – имя устройства; • $owner_ips_list – список других IP-адресов устройства; • $asset_id – идентификатор устройства.
4000005008	Добавлен MAC-адрес $owner_mac устройству с IP-адресом $owner_ip	В режиме наблюдения контроля активов автоматически добавлен MAC-адрес для сетевого интерфейса, у которого был указан только IP-адрес (при этом устройство было со статусом *Неразрешенное* или *Неиспользуемое*). В заголовке и в описании типа события используются следующие переменные: • $owner_mac – обнаруженный MAC-адрес устройства; • $owner_ip – IP-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства.
4000005009	Добавлен IP-адрес $owner_ip устройству с MAC-адресом $owner_mac	В режиме наблюдения контроля активов автоматически добавлен IP-адрес для сетевого интерфейса, у которого был указан только MAC-адрес (при этом устройство было со статусом *Неразрешенное* или *Неиспользуемое*). В заголовке и в описании типа события используются следующие переменные: • $owner_ip – обнаруженный IP-адрес устройства; • $owner_mac – MAC-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства.
4000005010	Обнаружен новый MAC-адрес $new_mac_addr у устройства с IP-адресом $owner_ip	В режиме наблюдения контроля активов обнаружен новый MAC-адрес, использованный устройством (при этом для устройства выключено автоматическое обновление адресной информации). В заголовке и в описании типа события используются следующие переменные: • $new_mac_addr – обнаруженный MAC-адрес; • $owner_ip – IP-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства.
4000005011	Обнаружено изменение MAC-адреса $owner_mac на адрес $challenger_mac в полученных данных об устройстве от EPP-приложения	По полученным данным от EPP-приложения обновлен MAC-адрес устройства. В заголовке и в описании типа события используются следующие переменные: • $owner_mac – старый MAC-адрес устройства; • $challenger_mac – новый MAC-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства.

Код	Заголовок типа события	Условия для регистрации
4000005012	Обнаружена новая адресная информация устройства $asset_name в полученных данных от EPP-приложения	В полученных данных от EPP-приложения обнаружена новая адресная информация устройства. Событие этого типа регистрируется, если изменение адресной информации устройства не было обработано приложением как событие с кодом 4000005009 или 4000005010. В заголовке и в описании типа события используются следующие переменные: • $asset_name – имя устройства; • $detected_epp_addresses – адресная информация; • $asset_id – идентификатор устройства.
4000005013	Обнаружен конфликт в адресах устройств $conflicted_epp_assets после получения данных от EPP-приложения	По полученным данным от EPP-приложения обнаружен конфликт с адресами нескольких устройств в Kaspersky Anti Targeted Attack Platform. По данным от EPP-приложения, адреса принадлежат одному устройству. В заголовке и в описании типа события используются следующие переменные: • $conflicted_epp_assets – устройства, у которых обнаружен конфликт адресов; • $unaccepted_epp_addresses – адреса, для которых установлена принадлежность одному устройству.
4000005014	Добавлена подсеть $subnet_mask по данным от EPP-приложения	После получения данных от EPP-приложения в список известных подсетей автоматически добавлена новая подсеть. Подсеть добавляется в то адресное пространство, в котором источником данных может являться сервер интеграции, получающий данные от EPP-приложения. При наличии нескольких таких адресных пространств выбирается то АП, которое содержит наиболее подходящую подсеть для автоматического добавления новой вложенной подсети. В заголовке и в описании типа события используются следующие переменные: • $subnet_mask – адрес подсети; • $subnet_type – тип подсети.
4000005016	Обнаружен несанкционированный DHCP-сервер с IP-адресом $owner_ip	Устройство $asset_name (ID: $asset_id) с адресом $owner_ip_or_mac определено как несанкционированный DHCP-сервер. В заголовке и в описании типа события используются следующие переменные: • $asset_id – идентификатор устройства; • $owner_ip_or_mac – IP- или MAC-адрес устройства.
4000005017	Обнаружен несанкционированный DHCP-ретранслятор с IP-адресом $owner_ip	Устройство $asset_name (ID: $asset_id) с адресом $owner_ip_or_mac определено как несанкционированный DHCP-ретранслятор. В заголовке и в описании типа события используются следующие переменные: • $asset_name – имя устройства; • $owner_ip_or_mac – IP- или MAC-адрес устройства.
4000005600	Обнаружены изменения в списке пользователей устройства с адресом $owner_ip_or_mac	При контроле пользователей на устройствах обнаружены изменения сведений о пользователях. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства; • $added_asset_users – список добавленных пользователей; • $modified_asset_users – список измененных пользователей; • $removed_asset_users – список удаленных пользователей.
4000005601	Обнаружены изменения в списке приложений устройства с адресом $owner_ip_or_mac	При контроле приложений и патчей на устройствах обнаружены изменения сведений о приложениях устройства. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства; • $added_asset_apps – список добавленных приложений; • $removed_asset_apps – список удаленных приложений.
4000005602	Обнаружены изменения в списке патчей устройства с адресом $owner_ip_or_mac	При контроле приложений и патчей на устройствах обнаружены изменения сведений о патчей устройства. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства; • $added_asset_patches – список добавленных патчей; • $removed_asset_patches – список удаленных патчей.

Код	Заголовок типа события	Условия для регистрации
4000005603	Обнаружены изменения в компоненте конфигурации $inventory_loc_key на устройстве	При контроле конфигураций устройств обнаружены изменения в компоненте конфигурации при сравнении с предыдущей конфигурацией по результатам сканирования устройства (для заданий в режимах обработки конфигураций **Только обновление** и/или **Архивирование версий**). В заголовке и в описании типа события используются следующие переменные: • $inventory_loc_key – название компонента конфигурации; • $device_config_inventory_changed_format – обнаруженные изменения в компоненте конфигурации.
4000005604	Обнаружены отличия от эталонного компонента конфигурации $inventory_loc_key на устройстве	При контроле конфигураций устройств обнаружены отличия от эталонного компонента конфигурации по результатам сканирования устройства (для заданий в режиме обработки конфигураций **Сравнение с эталоном**). В заголовке и в описании типа события используются следующие переменные: • $inventory_loc_key – название компонента конфигурации; • $device_config_diverged_format – обнаруженные отличия от эталонного компонента конфигурации.
4000005700	Обнаружено несовпадение открытого ключа при удаленном подключении к устройству	При удаленном подключении к устройству обнаружено несовпадение полученного открытого ключа устройства со значением, сохраненным в приложении. Сканирование устройства отменено. В описании типа события используются следующие переменные: • $asset_name – имя устройства; • $new_asset_sshpublickey – полученный открытый ключ; • $old_asset_sshpublickey – сохраненный открытый ключ.
4000005701	Обнаружено несовпадение открытого ключа при активном опросе устройства	При активном опросе устройства обнаружено несовпадение полученного открытого ключа устройства со значением, сохраненным в приложении. Активный опрос устройства отменен. В описании типа события используются следующие переменные: • $asset_name – имя устройства; • $new_asset_sshpublickey – полученный открытый ключ; • $old_asset_sshpublickey – сохраненный открытый ключ.
4000000004	Тестовое событие (AM)	Обнаружен тестовый сетевой пакет (при включенном методе обнаружения активности устройств).

Системные типы событий по технологии Внешние системы

В этой статье приведено описание системных типов событий, относящихся к технологии Внешние системы (см. таблицу ниже).

Системные типы событий по технологии Внешние системы (EXT)

Код	Заголовок типа события	Условия для регистрации
8000000001	Агрегирующее событие	Обнаружена последовательность событий, удовлетворяющих условиям правила корреляции. При регистрации агрегирующего события в качестве заголовка и описания указываются заголовок и описание из правила корреляции.
4000005400	Событие от внешней системы	Поступило событие от внешней системы с использованием NDR API. При регистрации события содержимое заголовка и описания определяются внешней системой.

Системные типы событий по технологии Защита конечных устройств

В этой статье приведено описание системных типов событий, относящихся к технологии Защита конечных устройств (см. таблицу ниже).

Системный тип события по технологии Защита конечных устройств (EPP)

Код	Заголовок типа события	Условия для регистрации
4000005500	Активность, характерная для сетевых атак	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Защита от сетевых угроз. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005501	Подключение недоверенного внешнего устройства	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Контроль устройств. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005502	Попытка запуска неразрешенной или недоверенной программы	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Контроль запуска программ. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005503	Неразрешенная файловая операция в заданной области мониторинга	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Мониторинг файловых операций. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005504	Изменены файлы в заданной области мониторинга	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Мониторинг целостности файлов на основе эталона. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005505	Сетевое подключение, не разрешенное правилами сетевого экрана	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Управление сетевым экраном. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005506	Изменения системного реестра в заданной области мониторинга	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Мониторинг реестра. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005507	Сработало правило анализа журналов	На сервер интеграции поступили данные о срабатывании правила компонента EPP-приложения Анализ журналов. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005508	Попытка эксплуатации уязвимости в защищаемом процессе	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Защита от эксплойтов. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005509	Попытка вредоносного шифрования сетевых файловых ресурсов	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Защита от шифрования. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005510	Попытка подключения к сети Wi-Fi	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Контроль Wi-Fi. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005512	Обнаружен зараженный или возможно зараженный объект	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Постоянная защита файлов. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005513	Сработало Sigma-правило $sigmaAlertTitle	На сервер интеграции поступили данные о срабатывании Sigma-правила компонента Endpoint Agent. В заголовке и в описании типа события используются следующие переменные: • $sigmaAlertTitle – название Sigma-правила; • $sigma_detection_type – технология обнаружения; • $sigma_object_type – тип объекта, вызвавшего срабатывание Sigma-правила; • $sigma_object_name – имя объекта, для которого сработало Sigma-правило, или название первого сработавшего Sigma-правила; • $sigma_status – статус обнаружения.

Настройка типов рисков

Типы рисков задают параметры, используемые при регистрации рисков в Kaspersky Anti Targeted Attack Platform: названия, категории и базовые оценки для рисков. Вы можете просматривать параметры типов рисков и при необходимости изменять значения базовых оценок для некоторых типов рисков.

После установки приложения используется исходный список типов рисков. Вы можете обновлять и дополнять поддерживаемые типы рисков, устанавливая обновления.

Просмотр таблицы типов рисков

Таблица типов рисков отображается в разделе **Параметры**, подразделе **Типы рисков** веб-интерфейса приложения.

Параметры типов рисков отображаются в следующих столбцах таблицы:

- **Код**.

  Уникальный номер типа риска. В таблице зарегистрированных рисков номер типа риска отображается в области деталей выбранного риска.

- **Название**.

  Название типа риска, отображаемое в таблице типов рисков. При регистрации риска его название может не полностью совпадать с названием использованного типа риска. Названия некоторых типов рисков могут быть полностью заменены на другие названия для зарегистрированных рисков. В частности, к типам рисков с такими названиями относятся типы рисков **Риск от внешней системы**. Если такой тип риска используется при регистрации риска, в приложении будет сохранено название риска, указанное в источнике сведений о риске (например, во внешней системе, которая использует NDR API).

- **Категория**.

  Название категории риска.

- **Базовая оценка**.

  Исходное значение для расчета оценки зарегистрированного риска. Заданные значения базовых оценок применяются при регистрации всех рисков, кроме рисков от внешних систем. Типы рисков с названиями **Риск от внешней системы** имеют нулевые значения базовых оценок. Базовые оценки для таких рисков должны быть указаны во внешних системах, которые регистрируют риски с помощью NDR API.

При просмотре таблицы типов рисков вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Изменение базовой оценки для типа риска

Изменение базовых оценок недоступно для типов рисков с названием **Риск от внешней системы**. Если такой тип риска используется для регистрации риска, базовая оценка этого риска должна быть определена из источника сведений о риске (например, внешней системой, которая использует NDR API).

Чтобы изменить базовую оценку для типа риска:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Типы рисков**.
2. В таблице типов рисков выберите тип риска, для которого вы хотите изменить базовую оценку.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.
4. Укажите нужное значение базовой оценки.
5. Нажмите на кнопку **Сохранить**.

Управление параметрами хранения рисков

Вы можете изменить ограничения максимального объема для хранения рисков.

Чтобы изменить параметры хранения рисков:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Серверы Sensor**.
3. Выберите карточку сервера Central Node.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для изменения параметров сервера.
5. На вкладке **Общие** перейдите к блоку параметров **Риски** и задайте ограничение занимаемого объема для хранения рисков с помощью параметра **Макс. объем**.

   Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

   При изменении значения параметра вам нужно учитывать, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для узла.
6. При необходимости с помощью параметра **Время хранения (дней)** включите ограничение на минимальное время хранения рисков и укажите нужное количество дней для хранения.
7. Нажмите на кнопку **Сохранить**.

Работа с информацией о хостах с компонентом Endpoint Agent

Приложение, выступающее в роли компонента Endpoint Agent, устанавливается на отдельные компьютеры (далее также "хосты"), входящие в IT-инфраструктуру организации. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих хостах, открытыми сетевыми соединениями и изменяемыми файлами.

Пользователи с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Аудитор** и **Администратор** могут оценить регулярность получения данных с хостов с компонентом Endpoint Agent, на закладке **Endpoint Agents** окна веб-интерфейса сервера Central Node в рамках тех тенантов, к данным которых у них есть доступ. Если вы используете режим распределенного решения и мультитенантности, то в веб-интерфейсе сервера PCN отображается список хостов с компонентом Endpoint Agent для PCN и всех подключенных SCN.

Пользователи с ролью **Администратор** могут настроить отображение регулярности получения данных с хостов с компонентом Endpoint Agent в рамках тех тенантов, к данным которых у них есть доступ.

В случае возникновения подозрительной сетевой активности пользователь с ролью **Старший сотрудник службы безопасности** может изолировать от сети любой из хостов с компонентом Endpoint Agent в рамках тех тенантов, к данным которых у него есть доступ. При этом соединение между сервером с компонентом Central Node и хостом с компонентом Endpoint Agent не будет прервано.

Для оказания поддержки при неполадках в работе компонента Endpoint Agent специалисты Службы технической поддержки могут попросить вас в отладочных целях выполнить следующие действия (в том числе в режиме Technical Support Mode):

- Активировать функциональность получения расширенной диагностической информации.
- Изменить параметры отдельных компонентов приложения.
- Изменить параметры хранения и отправки получаемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Специалисты Службы технической поддержки сообщат вам необходимую для выполнения перечисленных действий информацию (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав получаемых в отладочных целях данных. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка полученных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы приложения способами, не описанными в настоящем руководстве, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

Просмотр таблицы хостов с компонентом Endpoint Agent

Чтобы просмотреть таблицу хостов с компонентом Endpoint Agent:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Отобразится таблица хостов с компонентом Endpoint Agent.

Если вы используете режим распределенного решения и мультитенантности, в таблице содержится информация о хостах с компонентом Endpoint Agent, подключенных к PCN и всем серверам SCN.

В таблице могут отображаться следующие данные:

- Количество хостов и показатели активности компонента Endpoint Agent:
  - **Критическое бездействие** – количество хостов, от которых последние данные были получены очень давно.
  - **Предупреждение** – количество хостов, от которых последние данные были получены давно.
  - **Нормальная активность** – количество хостов, от которых последние данные были получены недавно.
- **Хост** – имя хоста с компонентом Endpoint Agent.
- **Серверы** – имя сервера, к которому подключен хост с компонентом Endpoint Agent.

  Поле отображается, если вы используете режим распределенного решения и мультитенантности.
- **IP** – IP-адрес хоста, на который установлен компонент Endpoint Agent.
- **ОС** – версия операционной системы, установленной на хосте с компонентом Endpoint Agent.
- **Версия** – версия установленного компонента Endpoint Agent.
- **Активность** – показатель активности компонента Endpoint Agent.
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.
- **Последнее подключение** – дата и время последнего подключения компонента Endpoint Agent к серверу Central Node.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- Выполнить задачи:
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Завершить по уникальному PID**.
  - **Получить файл**.
  - **Собрать форензику.**
  - **Поместить файл на карантин**.
  - **Запустить программу**.

- **Новое правило запрета**.
- **Изолировать от сети**.
- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

Список доступных действий зависит от типа компонента Endpoint Agent: для Windows, Linux или Mac (см. подробнее раздел *Принцип работы приложения*).

По ссылке с IP-адресом раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

Если вы используете только функциональность KATA (ключ KATA), в списке по ссылке с именем хоста доступны следующие действия:

- **Найти алерты** (отображается для пользователей с ролями **Старший сотрудник службы безопасности**).
- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

По ссылке в любом другом столбце таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

Настройка отображения таблицы хостов с компонентом Endpoint Agent

Вы можете настроить отображение столбцов, а также порядок их следования в таблице хостов с компонентом Endpoint Agent.

Чтобы настроить отображение таблицы хостов с компонентом Endpoint Agent:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.
3. В заголовочной части таблицы нажмите на кнопку  .
4. Отобразится окно **Настройка таблицы**.
5. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.

6. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку  и переместите строку с параметром в нужное место.
7. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.
8. Нажмите на кнопку **Применить**.

Отображение таблицы хостов с компонентом Endpoint Agent будет настроено.

Просмотр информации о хосте

Чтобы просмотреть информацию о хосте с компонентом Endpoint Agent:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.
3. Выберите хост, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о хосте.

Окно содержит следующую информацию:

- Блок рекомендаций:
  - Алерты – ссылка, по которой открывается раздел **Алерты** с условием поиска, содержащим выбранный хост.
  - События – ссылка, по которой открывается раздел **Поиск угроз** с условием поиска, содержащим выбранный хост.
  - **События, по которым сработали правила запрета** – ссылка, по которой открывается раздел **Поиск угроз** с условием поиска, содержащим выбранный хост и тип события **Правило запрета**.

Если вы используете только функциональность KATA (ключ KATA), в блоке рекомендаций отображается только ссылка **Алерты**.

- На закладке **Сведения**, в разделе **Хост** отображается следующая информация:
  - **Имя** – имя хоста с компонентом Endpoint Agent.
  - **IP** – IP-адрес хоста, на который установлен компонент Endpoint Agent.
  - **ОС** – версия операционной системы хоста, на который установлен компонент Endpoint Agent.
- На закладке **Сведения**, в разделе **Endpoint Agent** отображается следующая информация:
  - **Версия** – версия установленного компонента Endpoint Agent.
- **Активность** – показатель активности компонента Endpoint Agent. Может иметь следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.
- **Сервер** – имя сервера SCN или PCN. Отображается только в режиме распределенного решения и мультитенантности.
- **Подключен к серверу** – имя сервера Central Node.
- **Последнее подключение** – время последнего соединения с сервером Central Node, SCN или PCN.
- **Лицензия** – например, "OK".
- На закладке **Правила запрета** вы можете просмотреть, запуск или открытие файлов с какими MD5- или SHA256-хешами были запрещены на хосте. Отображается следующая информация:
  - **Имя** – имя файла.
  - **Состояние** – состояние правила запрета.
  - **Хеш** – алгоритм хеширования.

Если вы используете только функциональность KATA (ключ KATA), закладка **Правила запрета** не отображается.

- На закладке **Задачи** вы можете просмотреть, какие задачи были запущены на хосте. Отображается следующая информация:
  - **Время создания** – дата и время создания задачи.
  - **Имя** – название задачи.

- **Сведения** – полный путь к файлу или потоку данных, для которого создана задача.
- **Состояние** – статус выполнения задачи.

Если вы используете только функциональность KATA (ключ KATA), закладка **Задачи** не отображается.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Выполнить задачи:
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Получить файл**.
  - **Собрать форензику.**
  - **Поместить файл на карантин**.
  - **Запустить программу**.
- **Новое правило запрета**.
- **Изолировать от сети**.
- **Найти события**.
- **Найти алерты**.
- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

Список доступных действий зависит от типа компонента Endpoint Agent: для Windows, Linux или Mac (см. подробнее раздел *Принцип работы приложения*).

По ссылке с IP-адресом раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

Если вы используете только функциональность KATA (ключ KATA), в списках по ссылкам с именем хоста и его IP-адресом доступны следующие действия:

- **Найти алерты**.
- **Скопировать значение в буфер**.

Фильтрация и поиск хостов с компонентом Endpoint Agent по имени хоста

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по имени хоста:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.
3. По ссылке **Хост** откройте окно настройки фильтрации.
4. Если вы хотите, чтобы отобразились только изолированные хосты, установите флажок **Показывать только изолированные Endpoint Agents**.
5. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
6. В поле ввода укажите один или несколько символов имени хоста.
7. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
8. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
9. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent, изолированных от сети

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent, изолированные от сети:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.

3. По ссылке **Хост** откройте окно настройки фильтрации.

4. Установите флажок **Показывать только изолированные Endpoint Agents**.

5. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

   В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по именам серверов PCN и SCN

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать или найти хосты с компонентом Endpoint Agent по именам серверов PCN и SCN, к которым подключены эти хосты.

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по именам серверов PCN и SCN:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.

2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.

3. По ссылке **Серверы** откройте окно настройки фильтрации.

4. Установите флажки рядом с теми именами серверов, по которым вы хотите отфильтровать или найти хосты с компонентом Endpoint Agent.

5. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

   В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по IP-адресу компьютера

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по IP-адресу компьютера, на котором установлено приложение:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.
3. По ссылке **IP** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов IP-адреса компьютера. Вы можете ввести IP-адрес компьютера или маску подсети в формате IPv4 (например, `192.0.0.1` или `192.0.0.0/16`).
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по версии операционной системы на компьютере

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по версии операционной системы, установленной на компьютере:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.

3. По ссылке **ОС** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов версии операционной системы.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
8. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

   В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по версии компонента

Вы можете отфильтровать хосты по версии приложения, которое используется в роли компонента Endpoint Agent.

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по версии компонента:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.
3. По ссылке **Версия** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов версии приложение, которое используется в роли компонента Endpoint Agent.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

7. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.

8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по их активности

Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по их активности:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.

2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.

3. По ссылке **Активность** откройте окно настройки фильтрации.

   Установите флажки рядом с одним или несколькими показателями активности:

   - **Нормальная активность**, если вы хотите найти хосты, от которых последние данные были получены недавно.
   - **Предупреждение**, если вы хотите найти хосты, от которых последние данные были получены давно.
   - **Критическое бездействие**, если вы хотите найти хосты, от которых последние данные были получены очень давно.

4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Быстрое создание фильтра хостов с компонентом Endpoint Agent

Чтобы быстро создать фильтр хостов с компонентом Endpoint Agent:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.
3. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:

   a. Наведите курсор мыши на ссылку с тем значением столбца таблицы, которое вы хотите добавить в качестве условия фильтрации.

   b. Нажмите на левую клавишу мыши.

   Откроется список действий над значением.

   c. В открывшемся списке выберите одно из следующих действий:

   - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
   - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.
4. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Сброс фильтра хостов с компонентом Endpoint Agent

Чтобы сбросить фильтр хостов с компонентом Endpoint Agent по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.
3. Нажмите на кнопку справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Удаление хостов с компонентом Endpoint Agent

Чтобы удалить один или несколько хостов из таблицы **Endpoint Agents**:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.
3. Установите флажки рядом с одним или несколькими хостами, которые вы хотите удалить. Вы можете выбрать все хосты, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.
4. Нажмите на кнопку **Удалить**.
5. В открывшемся окне подтверждения действия нажмите на кнопку **Да**.

Выбранные хосты будут удалены из таблицы **Endpoint Agents**.

При удалении хостов в веб-интерфейсе Kaspersky Anti Targeted Attack Platform происходят следующие изменения:

- Для удаленного хоста нельзя создать задачу, правило запрета и правило сетевой изоляции.
- Если для хоста ранее было создано правило запрета, при удалении этого хоста его имя в окне просмотра правила (поле **Запрет для**) будет скрыто. Правило продолжит действовать.

  При повторном подключении этого хоста к серверу Central Node имя хоста будет восстановлено в поле **Запрет для** и правило запрета снова будет на него распространяться.
- Если для хоста ранее было создано правило сетевой изоляции, оно продолжит действовать до истечения времени, указанного в правиле.

  При повторном подключении этого хоста к серверу Central Node правило снова будет распространяться на этот хост.
- Метаданные объектов, помещенных на карантин на удаленном хосте, удаляются из карантина Kaspersky Anti Targeted Attack Platform.

  При повторном подключении этого хоста к серверу Central Node метаданные объектов в карантине Kaspersky Anti Targeted Attack Platform **не** восстанавливаются. Вы можете избежать переполнения карантина на хосте, очистив его с помощью командной строки или через Kaspersky Security Center. Подробнее см. в справке приложения, которое используется в роли компонента Endpoint Agent.
- Если объект был помещен на карантин по задаче **Поместить файл на карантин** только на одном хосте и этот хост был удален, в окне просмотра задачи кнопка **Восстановить все** будет неактивна, так как восстановить файл на удаленном хосте нельзя.

Поиск событий по имени удаленного хоста остается доступным.

Ограничение объема телеметрии от Endpoint Agent

По умолчанию Kaspersky Anti Targeted Attack Platform обрабатывает *все* данные о событиях (телеметрию), поступающие от Endpoint Agent. Ограничив объем телеметрии, можно снизить нагрузку на серверы, предназначенные для хранения и обработки телеметрии. Телеметрия в ограниченном объеме включает в себя полную информацию о самих событиях и наиболее важные сведения о процессах, запустивших эти события. Информация о прочих процессах, связанных с событиями, исключается.

Ограничить объем телеметрии могут пользователи с ролью **Старший сотрудник службы безопасности**. Пользователи с ролью **Администратор** и **Аудитор** могут просмотреть настройки ограничения телеметрии, но не могут их изменить. Пользователь с ролью **Сотрудник службы безопасности** не имеет доступа к настройкам телеметрии.

Чтобы ограничить объем телеметрии от Endpoint Agent:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Endpoint Agents**.
2. В блоке параметров **Телеметрия** выберите вариант **Ограниченный**.
3. Нажмите на кнопку **Применить** в нижней части окна.

Телеметрия будет ограничена.

Особенности ограничения телеметрии на Central Node и SCN

После нажатия кнопки **Применить** может появиться сообщение *Не удалось ограничить объем получаемых данных*. Это означает, что среди пользовательских правил TAA (IOA) есть такие, которые не позволяют включить ограничение телеметрии, так как содержат поля, которые при ограничении телеметрии не обрабатываются. Вы можете отключить эти правила или удалить их.

Список правил, которые требуется отключить или удалить, отображается в окне предупреждения под заголовком **Правила TAA, которые нужно отключить или изменить**. Вы можете скопировать список этих правил, нажав на кнопку **Копировать список**, и сохранить его любым удобным для вас способом. Кнопка **Перейти к правилам TAA** в окне предупреждения позволяет перейти в раздел пользовательских правил TAA (IOA).

Особенности ограничения телеметрии на PCN

Kaspersky Anti Targeted Attack Platform не проверяет пользовательские правила TAA (IOA), действующие на PCN, на работоспособность в режиме ограниченной телеметрии. Мы рекомендуем проверить на работоспособность каждое пользовательское правило TAA (IOA) самостоятельно.

Проверка пользовательских правил TAA (IOA) на работоспособность в режиме ограниченной телеметрии включает следующие этапы:

1. Включение режима ограниченной телеметрии.

2. Поиск событий по коду запроса из правила.

   Чтобы выполнить поиск событий по коду из правила, откройте окно просмотра правила и нажмите на кнопку **Запрос**. После запуска поиска открывается окно **Поиск угроз**.

   Правило TAA (IOA) является работоспособным, если в открывшемся окне отображается таблица событий, соответствующих условиям поиска. Если в открывшемся окне напротив имени PCN отображается ошибка *Server error: Request failed*, правило не является работоспособным.

3. Отключение или удаление неработоспособных правил TAA (IOA).

   Если вы хотите удалить или отключить неработоспособное правило на PCN, но при этом хотите применять правило на SCN, вам нужно создать аналогичное правило в веб-интерфейсе каждого SCN, на котором должно работать правило.

   Если вы не хотите отключать или удалять правила, откажитесь от ограничения телеметрии.

Сетевая изоляция хостов с компонентом Endpoint Agent

В рамках действия по реагированию на угрозы пользователи с ролью **Старший сотрудник службы безопасности** могут на время расследования инцидента изолировать хосты, на которых обнаружены объекты, требующие вашего внимания.

Сетевая изоляция не является самостоятельным действием по реагированию на угрозу. Сотруднику службы безопасности требуется расследовать инцидент самостоятельно за период действия сетевой изоляции хоста. Вы можете настроить период действия сетевой изоляции хоста при создании правила сетевой изоляции.

Для корректной работы изолированного хоста рекомендуется выполнять следующие условия:

- Создать на хосте учетную запись локального администратора или сохранить данные доменной учетной записи в кеш перед включением правила сетевой изоляции.

- Не заменять сертификат и IP-адрес сервера с компонентом Central Node при включенном правиле сетевой изоляции.

Изолированным хостам доступны по сети следующие ресурсы:

- Сервер с компонентом Central Node.

- Источник обновлений баз приложения (сервер обновлений "Лаборатории Касперского" или пользовательский источник).

- Серверы службы KSN.
- Хосты, добавленные в исключения правила сетевой изоляции.

Если компонент Endpoint Agent на хосте отключен, а также в течение некоторого времени после включения компонента или после перезагрузки компьютера с компонентом, сетевая изоляция этого хоста может не действовать.

При необходимости вы можете отключить сетевую изоляцию одним из следующих способов:

- С помощью запроса KEDR API.
- Удалив правило сетевой изоляции в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.
- Через командную строку.

  Подробнее от отключении сетевой изоляции через командную строку см. в справке Kaspersky Endpoint Security для Windows.

При применении сетевой изоляции действует ряд ограничений.

Создание правила сетевой изоляции

Чтобы создать правило сетевой изоляции:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.
2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.
3. Выберите хост, для которого вы хотите включить или отключить правило сетевой изоляции.

   Откроется окно с информацией о хосте.
4. Нажмите на кнопку **Изолировать**.
5. В поле **Отключить изоляцию через** введите количество часов от 1 до 9999, в течение которых будет действовать сетевая изоляция хоста.
6. В блоке параметров **Исключения для правила изоляции хоста** в списке **Направление трафика** выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.

7. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.

   Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent, вы можете использовать прокси-сервер для соединения Kaspersky Endpoint Agent для Windows с Kaspersky Anti Targeted Attack Platform. При добавлении этого прокси-сервера в исключения сетевые ресурсы, к которым открыт доступ через прокси-сервер, также добавляются в исключения. Если в исключения добавлены сетевые ресурсы, соединение с которыми происходит через прокси-сервер, но при этом исключение для самого прокси-сервера не настроено, исключение не будет работать.

8. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.

9. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия по заполнению полей **Направление трафика**, **IP** и **Порты**.

10. Нажмите на кнопку **Сохранить**.

    Хост будет изолирован от сети.

Вы также можете создать правило сетевой изоляции по ссылке **Изолировать <имя хоста>** в информации о событии и в информации об обнаружении.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания правила сетевой изоляции недоступна.

Для хостов с приложением Kaspersky Endpoint Security 11.4 для Linux в роли компонента Endpoint Agent функция сетевой изоляции не предусмотрена.

Добавление исключения из правила сетевой изоляции

Чтобы добавить исключение в ранее созданное правило сетевой изоляции:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.

2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.

3. Выберите хост, изолированный от сети, для которого вы хотите создать исключение из правила сетевой изоляции.

   Откроется окно с информацией о хосте.

4. По ссылке **Добавить в исключения** раскройте блок параметров **Исключения для правила изоляции хоста**.

5. Выберите направление сетевого трафика, которое не должно быть заблокировано:

   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.

6. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.

7. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.

8. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия по заполнению полей **Направление трафика**, **IP** и **Порты**. Нажмите на кнопку **Сохранить**.

Исключение из правила сетевой изоляции будет добавлено.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания исключения из правила сетевой изоляции недоступна.

Удаление правила сетевой изоляции

Чтобы удалить правило сетевой изоляции:

1. В окне веб-интерфейса приложения выберите раздел **Активы**.

2. Перейдите на вкладку **Endpoint Agents**.

   Откроется таблица хостов.

3. Нажатием левой клавиши мыши по имени хоста, для которого вы хотите удалить правило сетевой изоляции, раскройте меню действий над этим хостом.

4. Выберите действие **Удалить правило изоляции хоста**.

   Откроется окно подтверждения действия.

5. Нажмите на кнопку **Да**.

Правило сетевой изоляции хоста будет удалено.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления правила сетевой изоляции недоступна.

Ограничения, действующие при сетевой изоляции

При применении сетевой изоляции действует ряд ограничений:

- При включении правила сетевой изоляции на хосте прерываются все текущие соединения, а также становится недоступно VPN-подключение.
- Если администратор приложения заменяет сертификат сервера с компонентом Central Node при включенном правиле сетевой изоляции, то отключение правила становится недоступно.
- Приложение блокирует соединение изолированных хостов с сервером Active Directory. Если параметры операционной системы требуют подключения к службам Active Directory для авторизации, то пользователь изолированного хоста не сможет войти в систему.

Автоматическая отправка файлов с хостов с компонентом Endpoint Agent на проверку в Sandbox по правилам TAA (IOA) "Лаборатории Касперского"

Если функция включена, приложение может автоматически отправлять файлы с хостов с компонентом Endpoint Agent на проверку компоненту Sandbox в соответствии с правилами TAA (IOA) "Лаборатории Касперского". Отправка файлов на проверку осуществляется по следующему принципу:

1. Kaspersky Anti Targeted Attack Platform проверяет базу событий и отмечает события, соответствующие правилам TAA (IOA).
2. При наличии соответствующих условий в правилах TAA (IOA), Kaspersky Anti Targeted Attack Platform отправляет файлы на проверку компоненту Sandbox.

   Запросы на отправку файлов на проверку компоненту Sandbox не отображаются в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

3. По результатам проверки приложение может создать алерт.

   Вы можете просмотреть созданные алерты, отфильтровав их по показателю **Сведения** – **Автоотправка в Sandbox**.

При включении автоматической отправки файлов на проверку компоненту Sandbox объем обрабатываемого компонентом трафика может значительно увеличиться. Если сервер с компонентом Sandbox не рассчитан на увеличение нагрузки, часть объектов из очереди запросов на обработку будет заменена запросами на обработку файлов, отправленных на проверку автоматически.

Чтобы избежать потери объектов из очереди запросов на обработку, вы можете выполнить следующие действия:

- Развернуть дополнительные серверы Sandbox.
- Отключить функцию автоматической отправки файлов на проверку компоненту Sandbox.
- Добавить в исключения правила TAA (IOA), по которым Kaspersky Anti Targeted Attack Platform наиболее часто отправляет файлы на проверку компоненту Sandbox.

  Информация о правилах, по которым Kaspersky Anti Targeted Attack Platform наиболее часто отправляет файлы на проверку компоненту Sandbox, отображается на виджете **Отправлено в Sandbox по правилам TAA**. Вы можете добавить этот виджет на текущую схему расположения виджетов.

  > При добавлении правила в исключения прекращается также разметка событий и создание алертов по этому правилу.

Список файлов, которые могут быть отправлены автоматически на проверку компоненту Sandbox, приведен в таблице ниже.

Список файлов, которые могут быть отправлены автоматически на проверку компоненту Sandbox

Тип события	Тип файла
Запущен процесс	Файл запущенного процесса и файл родительского процесса.
Загружен модуль	Файл загруженного модуля и файл родительского процесса.
Удаленное соединение	Файл родительского процесса.
Правило запрета	Файл приложения, запуск которого был заблокирован, и файл родительского процесса.
Заблокирован документ	Файл документа, запуск которого был заблокирован, и файл родительского процесса.
Изменен файл	Созданный, удаленный или измененный файл и файл родительского процесса.
Журнал событий ОС	Файл процесса (только для Linux).
Изменение в реестре	Файл родительского процесса.
Прослушан порт	Файл родительского процесса.
Загружен драйвер	Файл загруженного драйвера.
Обнаружение	Обнаруженный файл и файл родительского процесса (если есть).
Результат обработки обнаружения	Обнаруженный файл и файл родительского процесса (если есть).
AMSI-проверка	Файл процесса.
Интерпретированный запуск файла	Файла, который был запущен, и файл родительского процесса.
Интерактивный ввод команд в консоли	Файл родительского процесса.

> Информация о файлах, отправленных на проверку компоненту Sandbox, не отображаются в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

Включение и отключение автоматической отправки файлов с хостов с компонентом Endpoint Agent на проверку компоненту Sandbox

Чтобы включить или отключить автоматическую отправку файлов на проверку компоненту Sandbox по правилам TAA (IOA) "Лаборатории Касперского":

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Endpoint Agents**.
2. В блоке параметров **Автоматическая отправка файлов в Sandbox** выполните следующие действия:
   - Переместите переключатель **Отправлять файлы** в положение **Включено**, если хотите включить автоматическую отправку файлов.

     По умолчанию функция включена.
   - Переместите переключатель **Отправлять файлы** в положение **Выключено**, если хотите отключить автоматическую отправку файлов.

     Отключение функции не влияет на работу правил TAA (IOA): будет отключена только автоматическая отправка файлов.Отключение функции не влияет на работу правил TAA (IOA): будет отключена только автоматическая отправка файлов.
3. Нажмите на кнопку **Применить**.

Автоматическая отправка файлов на проверку компоненту Sandbox по правилам TAA (IOA) "Лаборатории Касперского" будет включена или отключена.

В режиме распределенного решения и мультитенантности параметры автоматической отправки файлов на проверку компоненту Sandbox по правилам TAA (IOA) "Лаборатории Касперского", заданные на сервере PCN, распространяются на подключенные к этому серверу PCN серверы SCN. При необходимости вы можете включить или отключить автоматическую отправку файлов на каждом выбранном сервере SCN отдельно.

Выбор операционных систем для проверки объектов в Sandbox

Пользователи с ролью **Старший сотрудник службы безопасности** могут выбрать набор операционных систем, на основе которого будут формироваться задачи на проверку объектов для компонента Sandbox. На сервере Sandbox должны быть установлены виртуальные машины, которые соответствуют выбранному набору.

Вы можете просматривать список серверов Sandbox и виртуальных машин, развернутых на сервере.

Пользователи с ролью **Аудитор** могут просматривать список серверов Sandbox и параметры набора операционных систем. Для пользователей с ролью **Сотрудник службы безопасности** этот раздел недоступен.

Просмотр таблицы серверов с компонентом Sandbox

Для пользователей с ролью **Сотрудник службы безопасности** просмотр таблицы серверов с компонентом Sandbox недоступен.

Пользователи с ролью **Старший сотрудник службы безопасности** могут просматривать таблицу серверов с компонентом Sandbox.

Чтобы просмотреть таблицу серверов с компонентом Sandbox:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Серверы Sandbox**.
2. Выберите закладку **Серверы**.

   Отобразится таблица со списком серверов Sandbox.

Таблица содержит следующую информацию:

- **IP и имя** – IP-адрес или полное доменное имя сервера с компонентом Sandbox.
- **Авторизация** – статус запроса на подключение к компоненту Sandbox.
- **Состояние** – состояние подключения к компоненту Sandbox.
- **Отпечаток сертификата** – отпечаток сертификата сервера с компонентом Sandbox.
- **Виртуальные машины** – список виртуальных машин, созданных на сервере.

Выбор операционных систем для проверки объектов в Sandbox

Чтобы выбрать набор операционных систем:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Серверы Sandbox**.
2. Выберите закладку **Параметры**.
3. В блоке параметров **Набор ОС** выберите один из вариантов:
   - **Windows 7, Windows 10**.
   - **CentOS 7.8, Windows 7, Windows 10**.
   - **Astra Linux 1.7, Windows 7, Windows 10**.
   - **Пользовательские**.

4. Если вы выбрали **Пользовательские**, в блоке параметров **Состав набора** установите флажки напротив операционных систем, которые вы хотите использовать в наборе.

   Пользовательские операционные системы отображаются в списке, если виртуальные машины с этими операционными системами были установлены на сервере Sandbox. Преднастроенные операционные системы всегда отображаются в списке, но если виртуальные машины с этими операционными системами не развернуты, рядом с названием операционной системы отображается статус **Неизвестно**.

Kaspersky Anti Targeted Attack Platform будет создавать задачи на проверку объектов в Sandbox в соответствии с выбранным набором.

Если набор операционных систем, установленных на сервере Sandbox, не совпадает с набором, выбранным на сервере Central Node, объекты не отправляются на проверку этому серверу Sandbox. При подключении к серверу Central Node нескольких серверов Sandbox приложение отправляет объекты на проверку тем серверам Sandbox, на которых установлены операционные системы, соответствующие выбранному на Central Node набору.

Вы можете изменить набор операционных систем в ходе эксплуатации приложения. В этом случае вам нужно убедиться, что конфигурация сервера Sandbox соответствует аппаратным требованиям.

В режиме распределенного решения и мультитенантности настройки набора операционных систем, заданные на сервере PCN, не распространяются на подключенные к нему серверы SCN. Вы можете выбрать набор операционных систем для каждого сервера PCN и SCN отдельно.

Работа с задачами

Пользователи с ролью **Старший сотрудник службы безопасности**, создающие задачи на сервере, обладают неограниченными правами (root) доступа для всех хостов с компонентом Endpoint Agent, подключенных к этому серверу.

При работе в веб-интерфейсе приложения пользователи с ролью **Старший сотрудник службы безопасности** могут работать с файлами и приложениями на хостах путем создания и удаления задач.

В режиме распределенного решения и мультитенантности задачи **Завершить процесс**, **Собрать форензику**, **Получить ключ реестра**, **Запустить YARA-проверку**, **Управлять службами**, **Запустить программу**, **Удалить файл**, **Восстановить файл из карантина**, **Поместить файл на карантин** могут быть одного из следующих типов:

- **Глобальный** – созданные на сервере PCN. Действие этих задач распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

- **Локальный** – созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

Задачи **Получить файл**, **Получить дамп памяти процесса**, **Получить метафайлы NTFS**, **Получить образ диска**, **Получить дамп памяти** выполняются только на указанном хосте, независимо от режима работы приложения.

Максимальное время выполнение задачи составляет 24 часа. Если за это время задача не успела завершиться, ее выполнение останавливается.

Пользователи с ролью **Старший сотрудник службы безопасности** могут работать со всеми задачами в рамках тех тенантов, к данным которых у них есть доступ.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Пользователи с ролью **Аудитор** могут просматривать таблицу задач и информацию о выбранной задаче.

Просмотр таблицы задач

Таблица задач содержит список созданных задач и находится в разделе **Задачи** окна веб-интерфейса приложения. Вы можете просматривать все задачи или только задачи, созданные вами (текущим пользователем).

Вы можете включить или отключить отображение задач, созданных вами с помощью переключателя **Только мои** в правом верхнем углу окна. По умолчанию отображение задач, созданных текущим пользователем, включено.

В таблице задач содержится следующая информация:

- **Время** – дата и время создания задачи.
- **Тип** – тип задачи в зависимости от режима работы приложения и сервера, на котором была создана задача.

  Задачи могут быть одного из следующих типов:

  - **Глобальный** – созданные на сервере PCN. Действие этих задач распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
  - **Локальный** – созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Имя** – название задачи.

  По ссылке с названием типа задачи раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Скопировать значение в буфер**.
- **Сведения** – полный путь к файлу или потоку данных, для которого создана задача, или путь к общему сетевому ресурсу.

По ссылке со сведениями о пути к файлу или потоку данных раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

- **Серверы** – имя сервера с ролью PCN или SCN, на котором выполняется задача.

  Поле отображается, если вы используете режим распределенного решения и мультитенантности.

- **Хосты** – имя хоста, на котором выполняется задача.

  Поле отображается, только если вы используете отдельный сервер Central Node.

- **Автор** – имя пользователя, создавшего задачу.

  > Если вы включили отображение задач, созданных только текущим пользователем, столбец не отображается.

- **Состояние** – статус выполнения задачи.

  Задача может иметь один из следующих статусов:

  - **Ожидает**.
  - **В обработке**.
  - **Завершено**.

Просмотр информации о задаче

Чтобы просмотреть информацию о задаче:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Выберите задачу, информацию о которой вы хотите просмотреть.

Откроется окно с информацией о задаче.

Окно может содержать следующую информацию в зависимости от типа задачи:

- **Состояние** – статус выполнения задачи.
- **Описание** – описание задачи.
- **Путь к файлу** – путь к файлу или потоку данных.
- **Тип информации** – тип собранных данных.

- **Путь к ключу реестра** – путь к ключу реестра, который требуется получить.
- **ID процесса** – идентификатор процесса.
- **Маска** – маска файлов, которые включены в список данных.
- **Метафайлы** – метафайлы NTFS, которые требуется получить.
- **Том** – имя диска, с которого требуется получить метафайлы, образ диска или дамп памяти.
- **Путь к общему ресурсу** – путь к общему сетевому ресурсу.
- **Сохраненный файл** – ссылка на файл, полученный в результате выполнения задачи.
- **Максимальный уровень вложенности** – максимальный уровень вложенности папок, в которых приложение ищет файлы.
- **Исключения** – папки, в которых запрещены поиск или проверка файлов.
- **Область проверки** – папки, в которых проводится проверка по правилам YARA.
- **Действие** – действие, которое было выполнено над службой.

  В приложении доступны следующие операции со службами:

  - **Запустить**.
  - **Остановить**.
  - **Приостановить**.
  - **Продолжить**.
  - **Удалить**.
  - **Изменить тип запуска**.
- **Максимальное время проверки** – максимальное время выполнения задачи, по истечении которого проверка завершается.
- **SHA256** – SHA256-хеш файла, который вы хотите получить.
- **Запущено от имени** – параметр запуска приложения от имени локальной системы.
- **Автор** – имя пользователя, создавшего задачу.
- **Тенант** – название тенанта. Отображается, только когда вы используете режим распределенного решения и мультитенантности.
- **Время создания** – время создания задачи.
- **Время завершения** – время завершения задачи.
- **Отчет** – результат выполнения задачи на выбранных хостах.

Создание задачи получения файла

Вы можете получить файл с выбранных хостов с компонентом Endpoint Agent. Для этого вам нужно создать задачу получения файла.

Размер файла, который требуется получить, не должен превышать 100 МБ. Если размер файла превышает 100 МБ, задача завершается ошибкой.

Чтобы создать задачу получения файла:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Файл**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу, который вы хотите получить.

      Если запрашиваемый файл связан с дополнительными потоками данных NTFS, в результате выполнения задачи вы получите все файлы потоков данных NTFS, с которыми связан запрашиваемый файл.

      Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае вы получите только файлы указанного потока.

      При создании задачи приложение не проверяет на корректность указанный путь к файлу, который вы хотите получить.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите получить. Поле не является обязательным.

   c. Если вы хотите отказаться от проверки файла, снимите флажок **Отправить на проверку**.

      По умолчанию флажок установлен.

   d. **Описание** – описание задачи. Поле не является обязательным.

   e. **Хост** – имя или IP-адрес хоста.

      Вы можете указать только один хост.

4. Нажмите на кнопку **Добавить**.

Будет создана задача получения файла. Задача запускается автоматически после создания.

Файл, полученный в результате выполнения задачи, будет помещен в Хранилище. Если задача получения файла завершилась успешно, вы можете скачать полученный файл на ваш локальный компьютер.

Если вы используете режим распределенного решения и мультитенантности, архив помещается в Хранилище того сервера Central Node, к которому подключен хост, указанный в поле **Хост**.

Вы также можете скачать полученный файл из окна с отчетом о выполнении задачи.

Чтобы скачать полученный файл из окна с отчетом о выполнении задачи:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Откройте задачу получения файла, который вы хотите скачать.

3. В разделе **Отчет** нажмите на имя или IP-адрес хоста.

   Откроется окно с информацией о файле.

4. Нажмите на кнопку **Скачать**.

Файл будет сохранен на ваш локальный компьютер в папку загрузки браузера.

Для пользователей с ролью **Аудитор** функция создания задачи получения файла недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи сбора форензики

Вы можете получить списки файлов, процессов и точек автозапуска с выбранных хостов с компонентом Endpoint Agent. Для этого нужно создать задачу сбора форензики.

Чтобы создать задачу сбора форензики:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Форензика**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Тип информации** – тип собираемых данных. Установите флажок напротив одного, нескольких или всех параметров:

   - **Список процессов**, если хотите получить список процессов, запущенных на хосте в момент выполнения задачи.

   - **Список точек автозапуска**, если хотите получить список точек автозапуска.

     В список точек автозапуска включаются данные о приложениях, добавленных в папку автозагрузки или зарегистрированных в разделах реестра Run, а также о приложениях, которые запускаются автоматически при загрузке хоста с компонентом Endpoint Agent и при входе пользователя в систему на указанных хостах.

Список поддерживаемых точек автозапуска

Kaspersky Endpoint Agent поддерживает сбор следующих точек автозапуска:

- Logon.
- Run.
- Explorer.
- Shell.
- Office.
- Internet Explorer®.
- Tasks.
- Services.
- Drivers.
- Telephony.
- Cryptography.
- Debuggers.
- COM.
- Session Manager.
- Network.
- LSA.
- Applications.
- Codecs.
- Shellex.
- WMI.
- Unspecified.

Kaspersky Endpoint Security поддерживает сбор перечисленных выше точек автозапуска и указанных далее:

- BootLog.
- Browsers.
- DriverLog.
- EfiLoader.

- GroupPolicy.
- Logon.
- OsLoader.
- OsUpdate.
- Printer.
- Process.
- Scheduler.

- **Список файлов**, если хотите получить список файлов, хранящихся в выбранной папке или во всех папках хоста в момент выполнения задачи.

b. Если вы установили флажок **Список файлов**, в блоке параметров **Тип источника** выберите один из вариантов:

- **Все локальные диски**, если вы хотите, чтобы в список файлов были включены файлы, хранящиеся во всех папках локальных дисков на момент выполнения задачи.
- **Директория**, если вы хотите, чтобы в список файлов были включены файлы, хранящиеся в указанной папке и следующих по пути папках диска на момент выполнения задачи.

c. Если вы выбрали **Директория**, в поле **Начальная директория** укажите путь к папке, с которой начнется поиск файлов.

Вы можете использовать следующие префиксы:

- Системные переменные окружения.
- Пользовательские переменные окружения.

  При использовании пользовательских переменных окружения в список файлов будет включена информация о файлах в папках всех пользователей, определивших указанные переменные окружения. Если пользовательские переменные окружения переопределяет системные, в список файлов будет включена информация о файлах в папках по значению системных переменных окружения.

d. **Хосты** – IP-адрес или имя хоста, на который хотите назначить задачу.

Вы можете указать несколько хостов.

e. При необходимости вы можете указать следующие параметры поиска файлов в папках:

- **Маска** – маска файлов, которые должны быть включены в список файлов.
- **Альтернативные потоки данных** – флажок, включающий запись информации об альтернативных потоках данных в список файлов.

  Если запрашиваемый файл связан с дополнительными потоками данных NTFS, в результате выполнения задачи вы получите все файлы потоков данных NTFS, с которыми связан запрашиваемый файл.

  По умолчанию флажок установлен.

- **Максимальный уровень вложенности** – максимальный уровень вложенности папок, в которых приложение будет искать файлы.
- **Исключения** – путь к папкам, в которых вы хотите запретить поиск информации о файлах.
- **Описание** – описание задачи.

4. Нажмите на кнопку **Добавить**.

Задача сбора форензики будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в Хранилище ZIP-архив, который содержит файл с выбранными данными. Если задача завершилась успешно, вы можете скачать архив на ваш локальный компьютер.

Для пользователей с ролью **Аудитор** функция создания задачи сбора форензики недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения ключа реестра

Вы можете получить ключ реестра с выбранных хостов с компонентом Endpoint Agent. Для этого нужно создать задачу получения ключа реестра.

Чтобы создать задачу получения ключа реестра:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Ключ реестра**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к ключу реестра** – путь к ключу реестра, который вы хотите получить.

   Вы можете указать путь к ключу реестра в одном из следующих форматов:

   - Корневой относительный путь.

     Например, \REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.

   - Относительный путь с указанием полного имени раздела.

     Например, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.

   - Относительный путь с аббревиатурой вместо полного имени раздела.

     Например, HKLM\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.

Если вы хотите получить данные из ветки HKEY_CURRENT_USER, вам требуется указать ветку HKEY_USERS и SID пользователя: HKEY_USERS\<SID пользователя>.

b. **Описание** – описание задачи. Поле не является обязательным.

c. **Хосты** – имя или IP-адрес хоста, на который вы хотите назначить задачу.

Вы можете указать несколько хостов.

4. Нажмите на кнопку **Добавить**.

Задача получения ключа реестра будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в Хранилище ZIP-архив, который содержит файл в формате .reg, содержащий список всех ключей реестра и их значений, расположенных по указанному при создании задачи пути. Вы можете скачать архив на ваш локальный компьютер.

Если при выполнении задачи произошел сбой, в файл архива записывается описание ошибки.

Для пользователей с ролью **Аудитор** функция создания этой задачи недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения метафайлов NTFS

Вы можете получить метафайлы NTFS с выбранных хостов с компонентом Endpoint Agent. Для этого нужно создать задачу получения метафайлов NTFS.

Чтобы создать задачу получения метафайлов NTFS:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Метафайлы NTFS**.

Откроется окно создания задачи.

3. Задайте значения следующих параметров:

a. **Метафайлы** – список метафайлов, которые вы можете получить с помощью задачи. Выберите требуемый метафайл, установив напротив него флажок.

Вы можете выбрать несколько метафайлов.

b. **Том** – имя диска, с которого вы хотите получить метафайлы.

По умолчанию в поле указан системный диск. Вы можете указать путь к другому диску в формате `<буква диска>:`.

c. **Описание** – описание задачи. Поле не является обязательным.

d. **Хост** – имя или IP-адрес хоста, на который вы хотите назначить задачу.

Вы можете указать только один хост.

4. Нажмите на кнопку **Добавить**.

Задача получения метафайлов NTFS будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в Хранилище ZIP-архив, который содержит выбранные метафайлы. Вы можете скачать архив на ваш локальный компьютер.

Если при выполнении задачи произошел сбой, в файл архива записывается описание ошибки.

Если вы используете режим распределенного решения и мультитенантности, архив помещается в Хранилище того сервера Central Node, к которому подключен хост, указанный в поле **Хост**.

Загрузка выбранных метафайлов может привести к заполнению Хранилища и ротации объектов в нем. Если размер метафайла превышает размер Хранилища, метафайл не загружается

Для пользователей с ролью **Аудитор** функция создания этой задачи недоступна. У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения дампа памяти процесса

Вы можете получить дамп памяти процесса с выбранных хостов с компонентом Endpoint Agent. Для этого нужно создать задачу получения дампа памяти процесса.

Чтобы создать задачу получения дампа памяти процесса:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Дамп памяти процесса**.

Откроется окно создания задачи.

3. Задайте значения следующих параметров:

a. **ID процесса** – идентификатор процесса, для которого вы хотите получить дамп памяти.

b. **MD5/SHA256** – MD5-, SHA256-хеш файла процесса, для которого вы хотите получить дамп памяти. Поле не является обязательным.

c. **Описание** – описание задачи. Поле не является обязательным.

d. **Хост** – имя или IP-адрес хоста, на который вы хотите назначить задачу.

Вы можете указать только один хост.

4. Нажмите на кнопку **Добавить**.

Задача получения дампа памяти процесса будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в Хранилище ZIP-архив, который содержит файл с информацией о процессе и файл дампа памяти процесса. Вы можете скачать архив на ваш локальный компьютер.

Если при выполнении задачи произошел сбой, в файл архива записывается описание ошибки.

Если вы используете режим распределенного решения и мультитенантности, архив помещается в Хранилище того сервера Central Node, к которому подключен хост, указанный в поле **Хост**.

Для пользователей с ролью **Аудитор** функция создания этой задачи недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения образа диска

Вы можете получить образ диска с выбранного хоста с компонентом Endpoint Agent для Windows. Для этого нужно создать задачу получения образа диска.

Файл, полученный в результате выполнения задачи, можно сохранить только в общем сетевом ресурсе.

Чтобы создать задачу получения образа диска:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Образ диска**.

Откроется окно создания задачи.

3. Задайте значения следующих параметров:

a. **Путь к общему ресурсу** – путь к общему сетевому ресурсу.

Вам нужно указать путь в формате Universal Naming Convention (UNC): `\\server\share\path`.

b. **Имя пользователя** – имя пользователя учетной записи для доступа к общему сетевому ресурсу.

c. **Пароль** – пароль учетной записи для доступа к общему сетевому ресурсу.

d. В блоке параметров **Тип диска** выберите один из вариантов:

- **Логический**.
- **Физический**.

e. Если вы выбрали **Логический**, в поле **Том** введите букву диска без двоеточия и слеша или переменную `%SystemDrive%`.

f. Если вы выбрали **Физический**, в поле **Физический диск** введите номер диска.

g. Установите флажок **Разбить файл на части**, если вы хотите, чтобы при сохранении файл был разделен на несколько частей.

h. Если вы установили флажок, в поле **Размер части, ГБ** укажите минимальный размер части сохраняемого файла.

Минимальный размер части должен быть более одного гигабайта.

i. **Описание** – описание задачи. Поле не является обязательным.

j. **Хост** – IP-адрес или имя хоста, на который хотите назначить задачу.

4. Нажмите на кнопку **Добавить**.

Задача получения образа диска будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в общий сетевой ресурс архив, который содержит файл или файлы в формате EWF или RAW. Вы можете конвертировать файлы из формата RAW в формат EWF.

Для пользователей с ролью **Аудитор** функция создания задач недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Конвертация файла из формата RAW в формат EWF

Kaspersky Endpoint Security сохраняет образ диска в формате RAW. Также файлы могут быть помещены в архив. Для конвертации файлов из формата RAW в формат EWF разработан специальный скрипт на языке Python. Скрипт постоянно выполняет поиск файлов в формате RAW в заданной папке. При обнаружении таких файлов скрипт автоматически конвертирует файлы в формат EWF.

Скрипт convert_to_ewf_monitor.py

Для работы скрипта на компьютере должно быть установлено следующее ПО:

- Библиотека для доступа к файлам Expert Witness Compression Format (EWF) – libewf.

  Библиотеке libewf является ПО с открытым кодом.

  Рекомендуется разместить файлы библиотеки и файл скрипта в одной папке.

- Интерпретатор Python.

Чтобы включить конвертацию файлов образов дисков:

1. Запустите интерпретатор командной строки.
2. Перейдите в папку, в которой расположен скрипт.
3. Выполните команду:

   ```
   py convert_to_ewf_monitor.py --source <full path to the source files folder>
   [additional settings]
   ```

   Параметры скрипта конвертации в EWF

Параметр	Описание
`--source <full path to folder>`	Полный путь к папке, в которой скрипт выполняет поиск исходных файлов. Скрипт также выполняет поиск файлов в подпапках по указанному пути. Это обязательный параметр.
`--destination <full path to folder>`	Полный путь к папке, в которую скрипт сохраняет сконвертированные файлы. При этом структура папок сохраняется. По умолчанию скрипт сохраняет сконвертированные файлы в папке, которая указана для параметра `source`.
`--delete`	Удаление исходных файлов после успешной конвертации. Если сконвертировать файлы не удалось, скрипт пропустит удаление исходных файлов, и вы сможете повторить попытку.
`--ewftool <full path to folder>`	Полный путь к файлу ewfacquirestream.exe. Путь следует указывать с названием файла. По умолчанию скрипт пытается обнаружить файл ewfacquirestream.exe в папке, в которой расположен сам скрипт.
`--name_mask <regular expressions>`	Регулярные выражения для поиска исходных файлов для конвертации. Вы можете использовать этот параметр, если вам нужно конвертировать отдельные файлы. По умолчанию скрипт выполняет поиск с помощью регулярного выражения `^diskdump_`.
`--convert_single_dump`	Поиск одного файла для конвертации. После успешной конвертации одного файла скрипт завершает свою работу.
`--workers_num <number of files>`	Максимальное количество исходных файлов, которое скрипт может конвертировать одновременно. С помощью этого параметра вы можете оптимизировать производительность скрипта. По умолчанию скрипт может конвертировать до четырех файлов одновременно.
`--log_level <log level>`	Уровень ведения журнала. По умолчанию скрипт ведет журнал DEBUG.
`--log_path <full path to folder>`	Полный путь для сохранения файлов журнала. Путь следует указывать с названием файла журнала. По умолчанию скрипт показывает события в консоли интерпретатора.

Пример:

```
PS D:\Folder\Script\> py convert_to_ewf_monitor.py --source E:/Folder --destination E:/EWF --delete --log_path
E:/Folder/Logs.txt
```

Создание задачи получения дампа оперативной памяти

Вы можете получить дамп оперативной памяти с выбранного хоста с компонентом Endpoint Agent. Для этого нужно создать задачу получения дампа памяти.

Файл, полученный в результате выполнения задачи, можно сохранить только в общем сетевом ресурсе.

Чтобы создать задачу получения дампа памяти:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Дамп памяти**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к общему ресурсу** – путь к общему сетевому ресурсу.

      Вам нужно указать путь в формате Universal Naming Convention (UNC): `\\server\share\path`.

   b. **Имя пользователя** – имя пользователя учетной записи для доступа к общему сетевому ресурсу.

   c. **Пароль** – пароль учетной записи для доступа к общему сетевому ресурсу.

   d. **Описание** – описание задачи. Поле не является обязательным.

   e. **Хост** – IP-адрес или имя хоста, на который хотите назначить задачу.

4. Нажмите на кнопку **Добавить**.

   Задача получения дампа оперативной памяти будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в общий сетевой ресурс файл в формате RAW или архив, который содержит файл в формате RAW.

Для пользователей с ролью **Аудитор** функция создания задач недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи завершения процесса

Если вы считаете, что запущенный на компьютере процесс может угрожать безопасности компьютера или локальной сети организации, вы можете завершить его.

Чтобы создать задачу завершения процесса:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Завершить процесс**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу процесса, который вы хотите завершить.

      Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае будут завершены только процессы указанного потока данных. Процессы остальных потоков этого файла будут выполняться.

   b. **MD5/SHA256** – MD5-, SHA256-хеш файла процесса, который вы хотите завершить. Поле не является обязательным.

   c. **Описание** – описание задачи. Поле не является обязательным.

d. **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создана задача завершения процесса. Задача запускается автоматически после создания.

Для пользователей с ролью **Аудитор** функция создания задачи завершения процесса недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи проверки хостов с помощью правил YARA

Вы можете проверять хосты компонентом Endpoint Agent с помощью правил YARA. Для этого требуется создать задачу **Запустить YARA-проверку**. Вы можете создать задачу следующими способами:

- В разделе **Задачи**.

  В этом случае при создании задачи вам потребуется выбрать правила YARA, с помощью которых вы хотите проверить хосты.
- В разделе **Пользовательские правила**, подразделе **YARA**.

  В этом случае создается задача для проверки хостов по выбранным правилам YARA.

*Чтобы создать задачу проверки хостов с компонентом Endpoint Agent с помощью правил YARA в разделе **Задачи**:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и выберите **Запустить YARA-проверку**.

   Откроется окно создания задачи.
3. Задайте значения следующих параметров:

   a. **Выбрать правила** – имя правила. Вы можете ввести название правила или несколько знаков из названия правила и выбрать правило в списке.

   Вы можете добавить несколько правил.

b. **Проверить** – область проверки. Выберите один из следующих вариантов:

- **ОЗУ**, если вы хотите проверить процессы, запущенные на момент выполнения задачи.

  Приложение не проверяет процессы с низким уровнем приоритета.

- **Точки автозапуска**, если вы хотите проверить точки автозапуска, полученные в результате выполнения задачи **Собрать форензику**.

  Для проверки точек автозапуска вам требуется указать хосты, для которых ранее была выполнена задача **Собрать форензику**.

- **Указанные директории**, если вы хотите проверить файлы, хранящиеся в указанной папке и во всех вложенных папках на момент выполнения задачи.

- **Все локальные диски**, если вы хотите проверить файлы, хранящиеся во всех папках локальных дисков на момент выполнения задачи.

  Проверка всех локальных дисков может создать повышенную нагрузку на хост.

c. Если вы выбрали **ОЗУ**, при необходимости выполните следующие действия:

- В поле **Процессы** укажите короткие имена процессов или маску файлов, которые хотите проверить.

  Приложение проверяет все запущенные на хосте процессы с одинаковыми именами.

  Если поле **Процессы** не заполнено, приложение проверяет все процессы, запущенные на момент выполнения задачи, кроме процессов с PID ниже 10 и процессов, указанных в поле **Исключения**.

- В поле **Исключения** укажите полные имена процессов или маску файлов, которые хотите исключить из проверки.

  Если на хосте запущено несколько процессов с одинаковыми именами, приложение исключит из проверки все эти процессы.

d. Если вы выбрали **Точки автозапуска**, в поле **Тип проверки** выберите тип проверки:

- **Быстрая**.

  В этом случае проверяются все точки автозапуска, кроме COM-объектов.

- **Полная**.

  В этом случае проверяются все точки автозапуска и связанные с ними файлы.

Если в качестве компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Security для Windows, вне зависимости от выбранного параметра выполняется полная проверка.

e. Если вы выбрали **Указанные директории**, выполните следующие действия:

- В поле **Указанные директории** укажите путь к директории в формате C:\<имя директории>*.

- В поле **Исключения** укажите путь к директории в формате C:\<имя директории>*.

f. **Максимальное время проверки** – максимальное время проверки.

По истечении указанного времени проверка завершится, даже если хосты были проверены не по всем правилам. В отчете о выполнении задачи указываются результаты, актуальные на момент завершения проверки.

g. **Описание** – описание задачи. Поле необязательно для заполнения.

h. **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

*Чтобы создать задачу проверки хостов с компонентом Endpoint Agent с помощью правил YARA в разделе **Пользовательские правила**, подразделе **YARA**:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.
2. Установите флажки слева от правил, с помощью которых вы хотите проверить хосты.

   В нижней части окна отобразится панель управления.
3. Нажмите на кнопку **Запустить YARA-проверку**.
4. Выполните шаг 3 инструкции, приведенной выше.

Создание задачи будет завершено. Задача запускается автоматически после создания.

Если по результатам проверки будут обнаружены угрозы, Kaspersky Anti Targeted Attack Platform создаст соответствующие алерты.

Для пользователей с ролью **Аудитор** создание задачи проверки хостов с помощью правил YARA недоступно.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи управления службами

Вы можете удаленно запускать, останавливать, приостанавливать и продолжать работу службы, а также удалить службу или изменить ее тип запуска на выбранных хостах с компонентом Endpoint Agent. Для этого нужно создать задачу управления службами.

Чтобы создать задачу управления службами:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Управлять службами**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Имя службы** – укажите имя службы.

   b. **MD5/SHA256** – MD5- или SHA256-хеш службы. Поле необязательно для заполнения.

      Если вы указали хеш службы, которая загружается из DLL, Kaspersky Anti Targeted Attack Platform сравнивает указанный хеш одновременно с хешем библиотеки службы DLL и хешем процесса svchost.

   c. **Действие** – выберите операцию, которую вы хотите произвести со службой.

      В приложении доступны следующие операции со службами:

      - **Запустить**.
      - **Остановить**.
      - **Приостановить**.
      - **Продолжить**.
      - **Удалить**.
      - **Изменить тип запуска**.

      При удалении службы процессы, которые были запущены этой службой, продолжают работать до перезагрузки системы или завершении работы процесса.

   d. Если вы выбрали **Изменить тип запуска**, в поле **Тип запуска** выберите тип запуска службы.

   e. **Описание** – описание задачи. Поле необязательно для заполнения.

f. **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Задача управления службами будет создана. Задача запускается автоматически после создания.

Настоятельно не рекомендуется останавливать, приостанавливать, а также удалять или изменять тип запуска служб, влияющих на работоспособность хоста.

Список служб, с которыми не рекомендуется проводить операции

- AVP*.
- BFE.
- CertPropSvc.
- CoreMessagingRegistrar.
- CryptSvc.
- DcomLaunch.
- Dhcp.
- DispBrokerDesktopSvc.
- EventLog.
- EventSystem.
- LanmanServer.
- LanmanWorkstation.
- LSM.
- mpssvc.
- Netlogon.
- Netman.
- PlugPlay.
- PolicyAgent.
- Power.
- ProfSvc.
- RasMan.
- RpcEptMapper.
- RpcSs.
- SamSs.
- SCardSvr.
- SecurityHealthService.
- SessionEnv.
- Spooler.
- SstpSvc.
- TermService.
- UmRdpService.
- UserManager.
- UsoSvc.
- VaultSvc.
- W32Time.
- WebClient.
- Winmgmt.

- WlanSvc.
- wscsvc.

Для пользователей с ролью **Аудитор** создание задачи управления службами недоступно.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи выполнения приложения

Вы можете создать задачу запуска приложения или выполнения команды.

Если при выполнении задачи файл стандартного вывода или файл вывода ошибок достигает размера 100 КБ, часть данных из файла удаляется. Файл будет содержать не все данные.

Чтобы создать задачу запуска приложения или выполнения команды:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Запустить программу**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. В полях **Путь к файлу** и **Рабочий каталог** ниже введите значения одним из следующих способов:

   - В поле **Путь к файлу** введите полный путь к исполняемому файлу (например, `C:\Windows\System32\ipconfig.exe`). Поле **Рабочий каталог** оставьте пустым.

     При создании задачи приложение не проверяет на корректность указанный путь к исполняемому файлу.

   - В поле **Путь к файлу** введите имя и расширение исполняемого файла (например, `ipconfig.exe`). В поле **Рабочий каталог** укажите рабочую директорию (например, `C:\Windows\System32\`).

   b. В поле **Аргументы** введите дополнительные параметры запуска файла или выполнения команды (например, аргумент `/all`).

   c. В поле **Описание** введите описание задачи. Поле не является обязательным.

d. Настройте параметр **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создана задача запуска приложения или выполнения команды. Задача запускается автоматически после создания.

Пример:
Чтобы выполнить команду `ipconfig /all` на хосте с IP-адресом `10.10.10.1`, выполните следующие действия:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.
   Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и выберите **Запустить программу**.
   Откроется окно создания задачи.
3. Задайте значения следующих параметров:
   a. В полях **Путь к файлу** и **Рабочий каталог** ниже введите значения одним из следующих способов:
      - В поле **Путь к файлу** введите `C:\Windows\System32\ipconfig.exe`. Поле **Рабочий каталог** оставьте пустым.
      - В поле **Путь к файлу** введите `ipconfig.exe`. В поле **Рабочий каталог** введите `C:\Windows\System32\`.

   b. В поле **Аргументы** введите `/all`.

   c. В поле **Описание** введите описание задачи.

   d. Выберите область применения задачи **Выбранных хостов**.

   e. В поле **Хосты** введите несколько символов IP-адреса `10.10.10.1`, и когда этот IP-адрес появится в раскрывающемся списке результатов поиска ниже, выберите его.
4. Нажмите на кнопку **Добавить**.

Для пользователей с ролью **Аудитор** функция создания задачи запуска приложения или выполнения команды недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи удаления файла

Чтобы создать задачу удаления файла:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Удалить файл**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу, который вы хотите удалить.

      Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае будет удален только указанный поток данных. Остальные потоки данных этого файла останутся без изменений.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите удалить. Поле не является обязательным.

   c. **Описание** – описание задачи. Поле не является обязательным.

d. **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создана задача удаления файла. Задача запускается автоматически после создания.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки хоста. Рекомендуется проверить успешность удаления файла после перезагрузки хоста.

Удаление файла с подключенного сетевого диска не поддерживается.

Для пользователей с ролью **Аудитор** создание задачи удаления файла недоступно.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи помещения файла на карантин

Если вы считаете, что на компьютере с компонентом Endpoint Agent находится зараженный или возможно зараженный файл, вы можете изолировать его, поместив на карантин.

Чтобы создать задачу помещения файла на карантин:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Поместить файл на карантин**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу, который вы хотите поместить на карантин.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите поместить на карантин. Поле не является обязательным.

c. **Описание** – описание задачи. Поле не является обязательным.

d. **Хосты** – имя или IP-адрес хоста, на который вы хотите назначить задачу.

Вы можете указать несколько хостов.

e. Нажмите на кнопку **Добавить**.

Будет создана задача помещения файла на карантин. Задача запускается автоматически после создания.

В результате выполнения задачи:

- Файл будет удален из папки компьютера, в которой он находится, и перемещен в директорию карантина на этом компьютере, указанную при настройке приложение, которое используется в качестве компонента Endpoint Agent.
- В списке задач раздела **Задачи** веб-интерфейса приложения появится информация о выполнении этой задачи.
- В списке файлов раздела **Хранилище** подраздела **Карантин** появится информация о помещении файла на карантин.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет помещен на карантин только после перезагрузки хоста. Рекомендуется проверить успешность выполнения задачи после перезагрузки хоста.

Задача помещения файла на карантин может завершиться с ошибкой **Доступ запрещен**, если вы пытаетесь поместить на карантин исполняемый файл и он запущен в настоящий момент.

Чтобы решить проблему, создайте задачу завершения процесса для этого файла, а затем повторите попытку создания задачи помещения файла на карантин.

Для пользователей с ролью **Аудитор** функция создания задачи помещения файла на карантин недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи восстановления файла из карантина

Если вы считаете, что изолированный ранее файл безопасен, вы можете восстановить его из карантина на хост.

Чтобы создать задачу восстановления файла из карантина:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Восстановить файл из карантина**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Описание** – описание задачи. Поле не является обязательным.

   b. **Поиск файлов** – имя файла, находящегося в карантине.

4. Нажмите на кнопку **Добавить**.

Будет создана задача восстановления файла из карантина. Задача запускается автоматически после создания.

После восстановления файла из карантина на хост метаданные о файле останутся в таблице объектов, помещенных в Хранилище.

В режиме распределенного решения и мультитенантности файл, помещенный на карантин сервера SCN, нельзя восстановить на сервере PCN. Вы можете восстановить файл на том сервере SCN, где была создана задача для помещения файла на карантин.

Для пользователей с ролью **Аудитор** функция создания задачи восстановления файла из карантина недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание копии задачи

Чтобы скопировать задачу:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Откройте задачу, которую вы хотите скопировать.

3. Нажмите на кнопку **Скопировать**.

   Откроется окно создания задачи. Все параметры задачи будут скопированы.

4. Если вы хотите изменить параметры задачи, внесите изменения для одного или нескольких параметров в зависимости от типа копируемой задачи.

5. Нажмите на кнопку **Добавить**.

Будет создана копия выбранной задачи.

Для пользователей с ролью **Аудитор** функция создания копии задачи недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Удаление задач

Если вы удалите задачу в процессе ее выполнения, результат выполнения задачи может не сохраниться.

Если вы удалите успешно выполненную задачу загрузки файла, файл будет удален.

Чтобы удалить задачу:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Откройте задачу, которую вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Задача будет удалена.

Чтобы удалить все или несколько задач:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Установите флажки напротив задач, которые вы хотите удалить.

   Вы можете выбрать все задачи, установив флажок в строке с заголовками столбцов.

3. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранные задачи будут удалены.

Для пользователей с ролью **Аудитор** функция удаления задачи недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Фильтрация задач по времени создания

Чтобы отфильтровать задачи по времени их создания:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Время** откройте меню фильтрации задач.

3. Выберите один из следующих периодов отображения задач:

   - **Все**, если вы хотите, чтобы приложение отображало в таблице все созданные задачи.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице задачи, созданные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице задачи, созданные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице задачи, созданные за указанный вами период.

4. Если вы выбрали период отображения задач **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения задач.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по типу

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать задачи по их типу.

Чтобы отфильтровать задачи по их типу:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Тип** откройте меню фильтрации задач.

3. Выберите один из следующих вариантов отображения задач:

   - **Все**, если вы хотите, чтобы отображались все задачи независимо от типа.
   - **Глобальный**, если вы хотите, чтобы отображались только задачи, созданные на сервере PCN. Действие этих задач распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
   - **Локальный**, если вы хотите, чтобы отображались только задачи, созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени

Чтобы отфильтровать задачи по имени:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Имя** откройте меню фильтрации задач.

3. Установите один или несколько флажков:

   - **Завершить процесс**.
   - **Запустить программу**.
   - **Собрать форензику**.
   - **Запустить YARA-проверку**.

- **Управлять службами**.
- **Получить файл**.
- **Удалить файл**.
- **Поместить файл на карантин**.
- **Восстановить файл**.

4. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени и пути к файлу

Вы можете фильтровать задачи по показателю **Сведения** – имя и путь к файлу или потоку данных.

Чтобы отфильтровать задачи по имени и пути к файлу или потоку данных:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Сведения** откройте окно настройки фильтрации задач.
3. В правом раскрывающемся списке выберите **Сведения**.
4. В левом раскрывающемся списке выберите один из следующих операторов фильтрации задач:
   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.
5. В поле ввода укажите один или несколько символов имени или пути к файлу.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по описанию

Вы можете фильтровать задачи по показателю **Описание** – описание задачи, которое было добавлено на этапе создания задачи.

Чтобы отфильтровать задачи по описанию:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Сведения** откройте окно настройки фильтрации задач.

3. В левом раскрывающемся списке выберите **Описание**.

4. В правом раскрывающемся списке выберите один из следующих операторов фильтрации задач:

   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.

5. В поле ввода укажите один или несколько символов имени или пути к файлу.

6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

7. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени сервера

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать задачи по серверам, на которые распространяется действие задач.

Чтобы отфильтровать задачи по серверам, на которые распространяется действие задач:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Серверы** откройте меню фильтрации задач.

3. Установите флажки рядом с именами тех серверов, задачи по которым вы хотите отобразить.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени пользователя, создавшего задачу

Фильтрация задач по имени пользователя, создавшего задачу, доступна только при отображении всех задач. Если вы включили отображение задач, созданных только текущим пользователем, фильтрация задач по имени пользователя недоступна.

Чтобы отфильтровать задачи по имени пользователя, создавшего задачу:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Автор** откройте меню фильтрации задач.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации задач:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов имени пользователя.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по состоянию обработки

Чтобы отфильтровать задачи по состоянию их обработки пользователем:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Состояние** откройте меню фильтрации задач.

3. Установите один или несколько флажков:

   - **Ожидает**.
   - **В обработке**.
   - **Завершено**.

4. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра задач

Чтобы сбросить фильтр задач по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Работа с политиками (правилами запрета)

При работе в веб-интерфейсе приложения пользователи с ролью **Старший сотрудник службы безопасности** могут управлять правилами запрета запуска файлов и процессов на выбранных хостах с помощью политик. Например, вы можете запретить запуск приложений, использование которых считаете небезопасным, на выбранном хосте с компонентом Endpoint Agent. Приложение идентифицирует файлы по их хешу с помощью алгоритмов хеширования MD5 и SHA256. Вы можете создавать, включать и отключать, удалять и изменять правила запрета. Кроме того, по ссылке с названием алгоритма хеширования в таблице правил запрета вы можете выполнять такие действия по поиску объектов, событий или алертов, по которым сработали правила запрета, как **Найти события**, **Найти алерты**, **Найти на Kaspersky TIP** или **Найти на virustotal.com**.

В режиме распределенного решения и мультитенантности правила запрета могут быть следующих типов:

- **Глобальный** – созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

- **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, редактировать, удалять, включать и отключать, а также импортировать правила запрета в рамках тех тенантов, к данным которых у них есть доступ.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к политикам.

Пользователи с ролью **Аудитор** могут просматривать таблицу правил запрета запуска файлов и процессов, а также информацию о выбранном правиле запрета без возможности редактирования.

Все изменения в правилах запрета применяются на хостах после установки авторизованного соединения с выбранными хостами. Если соединение с хостами отсутствует, на хостах продолжают действовать старые правила запрета. Изменения в правилах запрета не влияют на уже запущенные процессы.

Правила запрета могут быть созданы автоматически на основе предустановленных политик (далее также "предустановок"), добавленных по умолчанию. При включенных предустановках приложение создает правило запрета на основе обнаружения компонента Sandbox со средним или высоким уровнем важности. Созданное правило запрета блокирует запуск файла по его MD5-хешу. Пользователи с ролью **Старший сотрудник службы безопасности** могут включать и отключать предустановки.

Предустановки не поддерживаются в режиме распределенного решения и мультитенантности.

Для правил запрета, которые были созданы автоматически или импортированы, доступны такие же операции, что и для правил, созданных вручную.

На каждый хеш файла можно создать только одно правило запрета.

Максимальное поддерживаемое количество правил запрета в системе составляет 50 000.

Правила запрета действуют, только когда компонент Endpoint Agent запущен на хосте. Если попытка запуска файла будет совершена до запуска компонента или после завершения работы компонента на хосте, то запуск файла не будет заблокирован.

Управление правилами запрета запуска файлов и процессов на выбранных хостах с помощью политик доступно только при интеграции компонента Endpoint Agent с сервером Central Node и осуществляется только через веб-интерфейс Kaspersky Anti Targeted Attack Platform.

Если в роли компонента Endpoint Agent вы используете Kaspersky Endpoint Security для Windows, вам нужно учитывать, что приложение поддерживает запрет запуска определенного набора расширений файлов офисного формата и набора интерпретаторов скриптов.

Просмотр таблицы правил запрета

Таблица правил запрета находится в разделе **Политики** окна веб-интерфейса приложения.

В таблице содержится следующая информация:

1. **Тип** – тип правила в зависимости от режима работы приложения и роли сервера, на котором оно создано:

   - **Глобальный** – созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

   - **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

2. **Имя** – имя правила запрета.

3. **Автор** – имя пользователя, под учетной записью которого было создано правило.

4. **Хеш файла** – алгоритм хеширования, применяющийся для идентификации файла.

   Идентификация файла может осуществляться по одному из следующих алгоритмов хеширования:

   - **MD5**.

   - **SHA256**.

   По ссылке с названием алгоритма хеширования раскрывается список, в котором вы можете посмотреть хеш файла, а также выбрать одно из следующих действий:

   - **Добавить в фильтр**.

   - **Исключить из фильтра**.

   - **Найти на Kaspersky TIP**.

- **Найти на virustotal.com** (для SHA256).
- **Найти события**.

  В результате выполнения этого действия откроется раздел **Поиск угроз** с событиями, уже отфильтрованными по выбранному вами хешу.
- **Найти алерты**.

  В результате выполнения этого действия откроется раздел **Алерты** с обнаружениями, уже отфильтрованными по выбранному вами хешу.
- **Включить правило запрета**.
- **Отключить правило запрета**.
- **Удалить правило запрета**.
- **Скопировать значение в буфер**.

5. **Серверы** – имена серверов с ролью PCN или SCN, на которые распространяется правило запрета.

   Поле отображается, если вы используете режим распределенного решения и мультитенантности.
6. **Хосты** – имя сервера с компонентом Central Node, на хосты которого распространяется правило запрета.

   Поле отображается, только когда вы используете отдельный сервер Central Node.
7. **Состояние** – текущее состояние правила запрета.

   Правило запрета может находиться в одном из следующих состояний:

   - **Включено**.
   - **Выключено**.

Настройка отображения таблицы правил запрета

Вы можете настроить отображение столбцов, а также порядок их следования в таблице правил запрета.

Чтобы настроить отображение таблицы правил запрета:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. В заголовочной части таблицы нажмите на кнопку  .

   Отобразится окно **Настройка таблицы**.
3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку  и переместите строку с параметром в нужное место.
5. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.
6. Нажмите на кнопку **Применить**.

Отображение таблицы правил запрета будет настроено.

Просмотр правила запрета

Чтобы просмотреть правило запрета:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. Выберите правило запрета, которое вы хотите просмотреть.

Правило запрета содержит следующую информацию:

- **События** – ссылка, по которой открывается раздел **Поиск угроз** с условием поиска, содержащим выбранное вами правило запрета.
- **Состояние** – текущее состояние правила запрета.

  Правило запрета может находиться в одном из следующих состояний:

  - **Включено**.
  - **Выключено**.
- Закладка **Сведения** со следующей информацией:
  - **MD5/SHA256** – хеш файла, запрещенного к запуску.

    По ссылке **MD5/SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти на Kaspersky TIP**.
    - **Найти события**.
    - **Найти алерты**.
    - **Скопировать значение в буфер**.
  - **Имя** – имя правила запрета или файла, запрещенного к запуску.

- **Тип** – тип правила в зависимости от режима работы приложения и роли сервера, на котором оно создано:
  - **Глобальный** – созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
  - **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Уведомление** – состояние параметра **Показывать пользователю уведомление о блокировке запуска файла**.
- **Запрет для** – список хостов, на которые распространяется правило запрета.

  Если запрет действует на всех хостах, отображается надпись **Всех хостов**.

- Закладка **Журнал изменений** содержит список изменений запрета: время изменения, имя пользователя, изменившего запрет, и действия над запретом.

Создание правила запрета

При создании правила запрета для системного файла возможна некорректная работа хоста, на котором запрещается запуск этого файла. Приложение Kaspersky Anti Targeted Attack Platform не проверяет, для какого типа файлов создается правило запрета.

Чтобы создать правило запрета:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Нажмите на кнопку **Добавить**.
3. Выберите **Создать правило**.

   Откроется окно создания правила запрета.

4. Задайте значения следующих параметров:
   a. **Состояние** – состояние правила запрета:
      - Если вы хотите включить правило запрета, переведите переключатель в положение **Вкл**.
      - Если вы хотите отключить правило запрета, переведите переключатель в положение **Откл**.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла или потока данных, запуск которого вы хотите запретить.

   c. **Имя** – имя правила запрета.

d. Если вы хотите, чтобы приложение выводило уведомление о срабатывании правила запрета пользователю компьютера, на который распространяется запрет, установите флажок **Показывать пользователю уведомление о блокировке запуска файла**.

Если вы установили флажок **Показывать пользователю уведомление о блокировке запуска файла**, при попытке запуска запрещенного файла пользователю будет показано уведомление о том, что сработало правило запрета запуска этого файла.

e. **Запрет для** – область применения правила запрета:

- Если вы хотите применить правило запрета на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите применить правило запрета на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите применить правило запрета.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
- Если вы хотите применить правило запрета на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Security для Linux версии ниже 12.2, функция создания правила запрета недоступна. Если при создании правила запрета в качестве области применения правила вы выберете хост с приложением Kaspersky Endpoint Security для Linux или все хосты, правило запрета не будет применено или будет применено только к хостам с приложением Kaspersky Endpoint Security для Windows.

5. Нажмите на кнопку **Добавить**.

Будет создан запрет на запуск файла.

Вы также можете импортировать правила запрета.

Для пользователей с ролью **Аудитор** функция создания правила запрета на запуск файла недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета.

Импорт правил запрета

Вы можете импортировать файл с MD5- и SHA256-хешами файлов, запуск которых хотите запретить. Для каждого хеша Kaspersky Anti Targeted Attack Platform создаст отдельное правило запрета.

Максимальный размер импортируемого файла - 10 МБ. На одной строке должен располагаться только один хеш.

Чтобы импортировать правила запрета:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Нажмите на кнопку **Добавить**.

3. Выберите **Импортировать правила**.

   Откроется окно импорта правил запрета.

4. Задайте значения следующих параметров:

   a. **Состояние** – состояние правила запрета:

   - Если вы хотите включить все импортированные правила запрета, переведите переключатель в положение **Вкл**.
   - Если вы хотите отключить все импортированные правила запрета, переведите переключатель в положение **Откл**.

   b. Если вы хотите, чтобы приложение выводило уведомление о срабатывании правил запрета пользователю компьютера, на который распространяется запрет, установите флажок **Показывать пользователю уведомление о блокировке запуска файла**.

   Поле **Запрет для** недоступно для редактирования. По умолчанию правила запрета, созданные на сервере PCN, распространяются на все хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN (если вы используете режим распределенного решения и мультитенантности).

5. Загрузите файл с хешами файлов, для которых вы хотите создать правила запрета, с помощью кнопки **Обзор**.

   Откроется окно выбора файлов.

6. Выберите файл, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

7. Нажмите на кнопку **Добавить**.

Правила будут импортированы.

Для пользователей с ролью **Аудитор** функция импорта правил запрета на запуск файла недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета.

Включение и отключение правила запрета

Чтобы включить или отключить правило запрета:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. В строке с правилом запрета, которое вы хотите включить или отключить, в столбце **Состояние** выполните одно из следующих действий:

   - Если вы хотите включить правило запрета, переведите переключатель в положение **Включено**.

     Выбранное вами правило запрета будет включено.

   - Если вы хотите отключить правило запрета, переведите переключатель в положение **Выключено**.

     Выбранное вами правило запрета будет отключено.

Для пользователей с ролью **Аудитор** функция включения и отключения правил запрета недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета запуска файлов и процессов на выбранных хостах с помощью политик.

Включение и отключение предустановок

Чтобы включить или отключить предустановки:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Выберите закладку **Предустановки**.

3. В строке с предустановкой, которую вы хотите включить или отключить, в столбце **Состояние** переведите переключатель в положение **Включено** или **Выключено**.

Предустановка будет включена или отключена. При отключении предустановки все ранее автоматически созданные правила запрета сохранятся.

Удаление правил запрета

Вы можете удалить одно или несколько правил запрета, а также все правила запрета сразу.

Чтобы удалить одно правило запрета:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Нажмите на правило запрета, которое вы хотите удалить.

   Откроется окно сведений о правиле запрета.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Правило запрета будет удалено.

Чтобы удалить все или несколько правил запрета:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Установите флажки напротив правил запрета, которые вы хотите удалить.

   Вы можете выбрать все правила запрета, установив флажок в строке с заголовками столбцов.

3. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранные правила запрета будут удалены.

Для пользователей с ролью **Аудитор** функция удаления правил запрета недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета запуска файлов и процессов на выбранных хостах с помощью политик.

Фильтрация правил запрета по имени

Чтобы отфильтровать правила запрета по имени:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. По ссылке **Имя** откройте меню фильтрации запретов.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации запретов:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов имени правила запрета.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по типу

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать правила запрета по их типу.

Чтобы отфильтровать правила запрета по типу:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. По ссылке **Тип** откройте меню фильтрации правил запрета.

3. Выберите один из следующих вариантов отображения правил запрета:

   - **Все**, если вы хотите, чтобы отображались все правила запрета независимо от типа.
   - **Глобальный**, если вы хотите, чтобы отображались только правила запрета, созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
   - **Локальный**, если вы хотите, чтобы отображались только правила запрета, созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по хешу файла

Чтобы отфильтровать правила запрета по хешу файла:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. По ссылке **Хеш файла** откройте меню фильтрации правил запрета.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации запретов:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов хеша файла.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по имени сервера

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать правила запрета по серверам, на которые распространяется действие правил запрета.

Чтобы отфильтровать правила запрета по имени сервера:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. По ссылке **Серверы** откройте меню фильтрации правил запрета.

3. Установите флажки напротив тех серверов, по которым вы хотите отфильтровать правила запрета.

4. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил запрета

Чтобы сбросить фильтр правил запрета по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Нажмите на кнопку справа от того заголовка столбца таблицы правил запрета, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Работа с пользовательскими правилами

Вы можете настроить дополнительную защиту IT-инфраструктуры организации с помощью пользовательских правил TAA, IDS, IOC и YARA.

Пользователи с ролью **Старший сотрудник службы безопасности** могут работать с пользовательскими правилами **TAA**, **IDS**, **IOC** и **YARA**: загружать и удалять файлы правил, просматривать списки правил, редактировать выбранные правила.

Пользователи с ролью **Аудитор** могут просматривать списки пользовательских правил **TAA**, **IDS**, **IOC** и **YARA** и свойства выбранных правил без возможности редактирования.

Пользователи с ролью **Сотрудник службы безопасности** могут просматривать списки пользовательских правил **TAA**, **IOC** и **YARA** и свойства выбранных правил без возможности редактирования.

Об использовании индикаторов компрометации (IOC) и атаки (IOA) для поиска угроз

Kaspersky Anti Targeted Attack Platform использует для поиска угроз два типа индикаторов – *IOC* (Indicator of Compromise, или индикатор компрометации) и *IOA* (Indicator of Attack, или индикатор атаки).

Индикатор IOC – это набор данных о вредоносном объекте или действии. Kaspersky Anti Targeted Attack Platform использует IOC-файлы открытого стандарта описания индикаторов компрометации OpenIOC. IOC-файлы содержат набор индикаторов, при совпадении с которыми приложение считает событие обнаружением и создает алерт. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

Индикатор IOA – это правило (далее также "правило TAA (IOA)"), содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Kaspersky Anti Targeted Attack Platform проверяет базу событий приложения и отмечает события или последовательность событий, которые совпадают с поведением, описанным в правилах TAA (IOA). При проверке используется технология *потоковой проверки*, при которой события, получаемые с защищаемых устройств, проверяются непрерывно в режиме реального времени.

Правила TAA (IOA), сформированные специалистами "Лаборатории Касперского", используются в работе технологии TAA (Targeted Attack Analyzer) и обновляются вместе с базами приложения. Они не отображаются в интерфейсе приложения и не могут быть отредактированы.

Вы можете добавлять пользовательские правила IOC и TAA (IOA), используя IOC-файлы открытого стандарта описания OpenIOC, а также создавать правила TAA (IOA) на основе условий поиска по базе событий.

Сравнительные характеристики индикаторов компрометации (IOC) и атаки (IOA) приведены в таблице ниже.

Сравнительные характеристики индикаторов IOC и IOA

Сравнительная характеристика	Индикаторы IOC в пользовательских правилах IOC	Индикаторы IOA в пользовательских правилах TAA (IOA)	Индикаторы IOA в правилах TAA (IOA), сформированных специалистами "Лаборатории Касперского"
Область проверки	Компьютеры с компонентом Endpoint Agent	База событий приложения	База событий приложения
Механизм проверки	Периодическая проверка	Потоковая проверка	Потоковая проверка
Возможность добавить в исключения из проверки	Нет.	Не требуется. Пользователи с ролью **Старший сотрудник службы безопасности** могут изменить текст индикатора в пользовательских правилах TAA (IOA) согласно требуемым условиям.	Есть.

Если вы используете режим распределенного решения и мультитенантности, в разделе отображаются данные по выбранному вами тенанту.

Работа с пользовательскими правилами TAA (IOA)

Пользовательские правила TAA (IOA) создаются на основе условий поиска по базе событий. Например, если вы хотите, чтобы приложение Kaspersky Anti Targeted Attack Platform формировало алерты по событиям запуска приложения, которое вы считаете небезопасным, на компьютерах с компонентом Endpoint Agent, вы можете выполнить следующие действия:

1. Сформировать поисковый запрос по базе событий вручную или загрузить IOC-файл с индикаторами компрометации или YAML-файл с Sigma-правилом для обнаружения этого приложения.

   При создании IOC-файла ознакомьтесь со списком IOC-терминов, которые можно использовать для поиска событий в разделе **Поиск угроз**. Вы можете посмотреть список поддерживаемых IOC-терминов, скачав файл по ссылке ниже.

   IOC-термины для поиска событий в разделе **Поиск угроз**

2. Создать правило TAA (IOA) на основе условий поиска событий.

   При поступлении на сервер Central Node событий, соответствующих созданному правилу TAA (IOA), Kaspersky Anti Targeted Attack Platform сформирует алерты.

Вы также можете создать правило TAA (IOA) на основе условий из уже загруженного IOC-файла. Для этого вам требуется выполнить следующие действия:

1. Найти события, соответствующие условиям выбранного файла.

2. Создать на основе условий поиска событий из выбранного файла правило TAA (IOA).

В режиме распределенного решения и мультитенантности правила TAA (IOA) могут быть одного из следующих типов:

- **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе приложения.

- **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.

Различия между пользовательскими правилами и правилами "Лаборатории Касперского" представлены в таблице ниже.

Сравнительные характеристики правил TAA (IOA)

Сравнительная характеристика	Пользовательские правила TAA (IOA)	Правила TAA (IOA) "Лаборатории Касперского"
Наличие рекомендаций по реагированию на событие	Нет	Есть Вы можете посмотреть рекомендации в информации об алерте
Соответствие технике в базе MITRE ATT&CK	Нет	Есть Вы можете посмотреть описание техники по классификации MITRE в информации об алерте
Отображение в таблице правил TAA (IOA)	Да	Нет

Сравнительная характеристика	Пользовательские правила TAA (IOA)	Правила TAA (IOA) "Лаборатории Касперского"
Способ отключить проверку базы по этому правилу	Отключить правило	Добавить правило в исключения TAA
Возможность удалить или добавить правило	Вы можете удалить или добавить правило в веб-интерфейсе приложения	Правила обновляются вместе с базами приложения и не могут быть удалены пользователем
Поиск алертов и событий, в которых сработали правила TAA (IOA)	По ссылкам **Алерты** и **События** в окне с информацией о правиле TAA (IOA)	По ссылкам **Алерты** и **События** в окне с информацией об алерте

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, импортировать, удалять, включать и выключать правила TAA (IOA), а также добавлять правила TAA (IOA) "Лаборатории Касперского" в исключения из проверки. Пользователи с ролями **Сотрудник службы безопасности** и **Аудитор** могут использовать правила TAA (IOA) для поиска признаков целевых атак, зараженных и возможно зараженных объектов в базе событий и алертов, а также просматривать таблицу правил TAA (IOA) и информацию о правилах TAA (IOA).

Просмотр таблицы правил TAA (IOA)

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Таблица пользовательских правил TAA (IOA) содержит информацию о правилах TAA (IOA), используемых для проверки событий и создания алертов, и находится в разделе **Пользовательские правила**, подразделе **TAA** окна веб-интерфейса приложения.

В таблице содержится следующая информация:

1. – степень важности, которая будет присвоена алерту, произведенному с использованием этого правила TAA (IOA).

   Степень важности может иметь одно из следующих значений:

   - – **Низкая**.
   - – **Средняя**.
   - – **Высокая**.

2. **Тип** – тип правила в зависимости от режима работы приложения и роли сервера, на котором оно создано:

   - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе приложения.
   - **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.

3. **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний правила:

   - **Высокая**.
   - **Средняя**.
   - **Низкая**.

   Чем выше надежность, тем меньше вероятность ложных срабатываний

4. **Имя** – название правила.

5. **Серверы** – имя сервера с ролью PCN или SCN, на который распространяется правило.

   Столбец отображается, если вы используете режим распределенного решения и мультитенантности.

6. **Алерты** – требование сохранять информацию об алерте на основе совпадения события из базы с критериями правила.

   - **Включено** – для события создается запись в таблице алертов с указанием технологии Targeted Attack Analyzer (TAA).
   - **Выключено** – не отображается в таблице алертов.

7. **Состояние** – состояние использования правила при проверке событий:

   - **Включено** – правило используется.
   - **Выключено** – правило не используется.

Создание правила TAA (IOA) на основе условий поиска событий

Чтобы создать правило TAA (IOA) на основе условий поиска событий:

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.

2. Выполните поиск событий в режиме конструктора или режиме исходного кода.

3. Нажмите на кнопку **Сохранить как правило TAA (IOA)**.

   Откроется окно **Новое правило TAA (IOA)**.

4. В поле **Имя** введите имя правила.

5. Нажмите на кнопку **Сохранить**.

Условие поиска событий будет сохранено. В таблице правил TAA (IOA) раздела **Пользовательские правила**, в подразделе **TAA** веб-интерфейса отобразится новое правило с заданным именем.

Не рекомендуется в условиях поиска событий, сохраняемых как пользовательское правило TAA (IOA), использовать следующие поля:

- IOAId.
- IOATag.
- IOATechnique.
- IOATactics.
- IOAImportance.
- IOAConfidence.

На момент сохранения пользовательского правила TAA (IOA) в приложении может не быть событий, содержащих данные для этих полей. Когда события с этими данными появятся, пользовательское правило TAA (IOA), созданное ранее, не сможет разметить события по этим полям.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания правила TAA (IOA) на основе условий поиска событий недоступна.

Импорт правил TAA (IOA)

Вы можете импортировать правила TAA (IOA) из IOC-файла или YAML-файла с Sigma-правилом и использовать их для проверки событий и создания алертов Targeted Attack Analyzer.

Чтобы импортировать правило TAA (IOA):

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Нажмите на кнопку **Импортировать**.

   Откроется окно выбора файла на вашем локальном компьютере.

3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.

   Откроется окно **Новое правило TAA (IOA)**.

4. Переместите переключатель **Состояние** в положение **Включено**, если вы хотите включить использование правила при проверке базы событий.

5. На закладке **Сведения** в поле **Имя** введите имя правила.

6. В поле **Описание** введите любую дополнительную информацию о правиле.

7. В раскрывающемся списке **Важность** выберите степень важности, которая будет присвоена обнаружению, выполненному по этому правилу TAA (IOA):
   - **Низкая**.
   - **Средняя**.
   - **Высокая**.
8. В раскрывающемся списке **Надежность** выберите уровень надежности этого правила, по вашей оценке:
   - **Низкая**.
   - **Средняя**.
   - **Высокая**.
9. В блоке параметров **Область применения** установите флажки напротив тех серверов, на которых вы хотите применить правило.
10. На закладке **Запрос** проверьте заданные условия поиска. Если требуется, внесите изменения.
11. Нажмите на кнопку **Сохранить**.

Пользовательское правило TAA (IOA) будет импортировано в приложение.

Вы также можете добавить правило TAA (IOA), сохранив условия поиска по базе событий в разделе **Поиск угроз**.

Просмотр информации о правиле TAA (IOA)

Чтобы просмотреть информацию о правиле TAA (IOA):

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).
2. Выберите правило, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о правиле.

Окно содержит следующую информацию:

- **Алерты** – по ссылке в новой вкладке браузера откроется таблица алертов, отфильтрованных по технологии Targeted Attack Analyzer и имени правила TAA (IOA), с которым вы работаете.
- **События** – по ссылке в новой вкладке браузера откроется таблица событий, отфильтрованных по имени правила.
- **Запрос** – по ссылке в новой вкладке браузера откроется таблица событий, отфильтрованных по имени правила. В условиях поиска событий указаны данные из правила TAA (IOA), с которым вы работаете. Например, `EventType=Запущен процесс AND FileName CONTAINS <имя правила, с которым вы работаете>`. Вы можете отредактировать запрос для поиска событий.

- **IOA ID** – по ссылке открывается идентификатор, присваиваемый приложением каждому правилу.

  Изменение идентификатора недоступно. Вы можете скопировать идентификатор по кнопке **Скопировать значение в буфер**.

- **Состояние** – использование правила при проверке базы событий.

На закладке **Сведения** отображается следующая информация:

- **Имя** – имя правила, которое вы указали при добавлении правила.
- **Описание** – любая дополнительная информация о правиле, которую вы указали.
- **Важность** – оценка возможного влияния события на безопасность компьютеров или локальной сети организации, указанная пользователем при добавлении правила.
- **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний, заданный пользователем при добавлении правила.
- **Тип** – тип правила в зависимости от роли сервера, на котором оно создано:
  - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе приложения.
  - **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
- **Область применения** – имена серверов с компонентом Central Node, на которых применяется правило.

На закладке **Запрос** отображается исходный код запроса, по которому осуществляется проверка. По ссылке **Запрос** в верхней части окна вы можете перейти в раздел **Поиск угроз** и выполнить запрос для поиска событий.

Поиск алертов и событий, в которых сработали правила TAA (IOA)

Чтобы найти и просмотреть алерты и события, при создании которых сработало пользовательское правило TAA (IOA):

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выберите правило, результат срабатывания которого вы хотите просмотреть.

   Откроется окно с информацией о правиле.

3. Выполните одно из следующих действий:

   - Если вы хотите просмотреть алерты, при создании которых сработало правило TAA (IOA), по ссылке **Алерты** перейдите в базу алертов.

     Откроется новая вкладка браузера с таблицей найденных алертов.

- Если вы хотите просмотреть события, при создании которых сработало правило TAA (IOA), по ссылке **События** перейдите в базу событий.

  Откроется новая вкладка браузера с таблицей найденных событий.

Вы можете просмотреть алерты и события, при создании которых сработало пользовательское правило TAA (IOA).

Чтобы найти и просмотреть алерты и события, при создании которых сработало правило TAA (IOA) "Лаборатории Касперского":

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.

3. В раскрывающемся списке слева выберите **Содержит**.

4. В раскрывающемся списке справа выберите технологию **(TAA) Targeted Attack Analyzer**.

5. Нажмите на кнопку **Применить**.

   В таблице отобразятся алерты, выполненные технологией TAA на основе правил TAA (IOA).

6. Выберите алерт, для которого в столбце **Обнаружено** отображается название нужного правила.

   Откроется окно с информацией об алерте.

7. В блоке **Результаты проверки** по ссылке с названием правила откройте окно с информацией о правиле.

8. Выполните одно из следующих действий:

   - Если вы хотите просмотреть алерты, при создании которых сработало правило TAA (IOA), по ссылке **Алерты** перейдите в базу алертов.

     Откроется новая вкладка браузера с таблицей найденных алертов.

   - Если вы хотите просмотреть события, при создании которых сработало правило TAA (IOA), по ссылке **События** перейдите в базу событий.

     Откроется новая вкладка браузера с таблицей найденных событий.

Вы можете просмотреть алерты и события, при создании которых сработало правило TAA (IOA) "Лаборатории Касперского".

Фильтрация и поиск правил TAA (IOA)

Чтобы отфильтровать или найти правила TAA (IOA) по требуемым критериям:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выполните следующие действия в зависимости от критерия фильтрации:

- **По степени важности**

  a. По значку ≣ откройте окно настройки фильтрации IOA-правил.

  b. Установите флажки напротив тех степеней важности, которые вы хотите включить в критерии фильтрации:

  - **Низкая**.
  - **Средняя**.
  - **Высокая**.

  c. Нажмите на кнопку **Применить**.

- **По типу правила**

  a. По ссылке **Тип** откройте окно настройки фильтрации.

  b. Выберите один из следующих элементов:

  - **Все** – все правила.
  - **Глобальный** – правила, созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе приложения.
  - **Локальный** – правила, созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.

- **По уровню надежности**

  a. По ссылке **Надежность** откройте окно настройки фильтрации.

  b. Установите флажки напротив тех уровней надежности, которые вы хотите включить в критерии фильтрации:

  - **Низкая**.
  - **Средняя**.
  - **Высокая**.

  c. Нажмите на кнопку **Применить**.

- **По имени правила**

  a. По ссылке **Тег IOA** откройте окно настройки фильтрации.

  b. Введите один или несколько символов названия IOA-правила.

  c. Нажмите на кнопку **Применить**.

- **По имени сервера**

  a. По ссылке **Серверы** откройте окно настройки фильтрации.

  b. Установите флажки напротив тех тенантов или серверов внутри тенантов, которые вы хотите включить в критерии фильтрации.

  c. Нажмите на кнопку **Применить**.

- **по созданию алертов на основе правила**

  a. По ссылке **Алерты** раскройте список настройки фильтрации.

  b. Выберите один из следующих вариантов:

  - **Все**.
  - **Включено**.
  - **Выключено**.

- **По состоянию правила**

  a. По ссылке **Состояние** раскройте список настройки фильтрации.

  b. Выберите один из следующих вариантов:

  - **Все**.
  - **Включено**.
  - **Выключено**.

В таблице отобразятся только правила, соответствующие заданным условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил TAA (IOA)

Чтобы сбросить фильтр правил TAA (IOA) по одному или нескольким условиям фильтрации, выполните следующие действия:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Нажмите на кнопку справа от того заголовка столбца таблицы правил, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только правила, соответствующие заданным условиям.

Включение и отключение использования правил TAA (IOA)

Пользователи с ролью **Старший сотрудник службы безопасности** могут включить или отключить использование одного или нескольких правил, а также всех правил сразу.

Чтобы включить или отключить использование правила TAA (IOA) при проверке событий:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. В строке с нужным правилом в столбце **Состояние** включите или выключите переключатель.

Использование правила при проверке событий будет включено или отключено.

Чтобы включить или отключить использование всех или нескольких правил TAA (IOA) при проверке событий:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Установите флажки слева от правил, использование которых вы хотите включить или отключить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Включить** или **Отключить**, чтобы включить или отключить использование всех правил.

Использование выбранных правил при проверке событий будет включено или отключено.

В режиме распределенного решения и мультитенантности на сервере PCN доступно управление только глобальными правилами TAA (IOA). Управление локальными правилами TAA (IOA) доступно на серверах SCN тех тенантов, к которым у вас есть доступ.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** включение и отключение правил TAA (IOA) недоступно.

Изменение правила TAA (IOA)

Пользователи с ролью **Старший сотрудник службы безопасности** могут изменять пользовательские правила TAA (IOA). Изменение правил "Лаборатории Касперского" недоступно.

При работе в режиме распределенного решения и мультитенантности вы можете изменять только те правила TAA (IOA), которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно изменение только правил, созданных на PCN. В веб-интерфейсе SCN доступно изменение только правил, созданных на SCN.

Чтобы изменить правило TAA (IOA):

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выберите правило, которое вы хотите изменить.

   Откроется окно с информацией об этом правиле.

3. Внесите необходимые изменения.

4. Нажмите на кнопку **Сохранить**.

Параметры правила будут изменены.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения правила TAA (IOA) на основе условий поиска событий недоступна.

Удаление правил TAA (IOA)

Пользователи с ролью **Старший сотрудник службы безопасности** могут удалить одно или несколько пользовательских правил TAA (IOA), а также все правила сразу.

При работе в режиме распределенного решения и мультитенантности вы можете удалять только те правила TAA (IOA), которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно удаление только правил, созданных на PCN. В веб-интерфейсе SCN доступно удаление только правил, созданных на SCN.

Чтобы удалить пользовательское правило TAA (IOA):

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выберите правило, которое вы хотите удалить.

   Откроется окно с информацией об этом правиле.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Правило будет удалено.

Чтобы удалить все или несколько пользовательских правил TAA (IOA):

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Установите флажки слева от правил, которые вы хотите удалить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Вы не можете удалять правила TAA (IOA) "Лаборатории Касперского". Если вы не хотите использовать при проверке правило TAA (IOA) "Лаборатории Касперского", вам требуется добавить его в исключения.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения правила TAA (IOA) на основе условий поиска событий недоступна.

Работа с пользовательскими правилами IOC

Вы можете использовать IOC-файлы для поиска индикаторов компрометации по базе событий и на компьютерах с компонентом Endpoint Agent. Например, если вы получили из внешних источников информацию о распространении вредоносного приложения, вы можете выполнить следующие действия:

1. Создать IOC-файл с индикаторами компрометации для вредоносного приложения и загрузить его в веб-интерфейс Kaspersky Anti Targeted Attack Platform.
2. Найти события, соответствующие условиям выбранного IOC-файла.

   Вы можете просмотреть эти события и, если вы хотите, чтобы приложение Kaspersky Anti Targeted Attack Platform формировало алерты по выбранным событиям, вы можете создать правило TAA (IOA).

3. Включить автоматическое использование выбранного IOC-файла для поиска индикаторов компрометации на компьютерах с компонентом Endpoint Agent.

4. Если в результате проверки компьютеров компонент Endpoint Agent обнаружит индикаторы компрометации, приложение Kaspersky Anti Targeted Attack Platform сформирует алерт.

   Вы можете найти эти алерты в таблице алертов с помощью фильтра по названию технологии.

5. Настроить расписание поиска индикаторов компрометации с помощью IOC-файлов на компьютерах с компонентом Endpoint Agent.

В режиме распределенного решения и мультитенантности IOC-файлы могут быть следующих типов:

- **Локальный** – IOC-файлы, загруженные на сервер SCN. По этим IOC-файлам производится поиск индикаторов компрометации на хостах с программой Kaspersky Endpoint Agent, подключенных к этому серверу SCN.
- **Глобальный** – IOC-файлы, загруженные на сервер PCN. По этим IOC-файлам производится поиск индикаторов компрометации на хостах с программой Kaspersky Endpoint Agent, подключенных к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN.

IOC-файл представляет собой текстовый файл, сохраненный с расширением .ioc. При создании IOC-файла ознакомьтесь со списком IOC-терминов, поддерживаемых приложением, которое вы используете в роли компонента Endpoint Agent. Вы можете посмотреть список поддерживаемых IOC-терминов, скачав файлы по ссылкам ниже.

Kaspersky Endpoint Security для Windows

Kaspersky Endpoint Security 12 для Linux

Для корректной работы функционала необходимо, чтобы для IOC-терминов Indicator и IndicatorItem был задан атрибут id. Если атрибут отсутствует хотя бы в одном IOC-файле, приложение не создает алерты при обнаружении совпадений индикаторов компрометации не только для этого файла, но и для всех остальных IOC-файлов.

Kaspersky Endpoint Security 11.4 для Linux и Kaspersky Endpoint Security для Mac не поддерживают работу с IOC-файлами.

Пример IOC-файла для поиска файла по его хеш-сумме

```
<?xml version="1.0" encoding="us-ascii"?>

<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:xsd="http://www.w3.org/2001/XMLSchema"

id="уникальный идентификатор в формате UUID" last-modified="дата последнего изменения правила в формате ГГГГ-ММ-ДДТЧЧ:ММ:СС" xmlns="http://schemas.mandiant.com/2010/ioc">

<short_description>название правила</short_description>

<authored_by>имя правила</authored_by>

<authored_date>дата создания файла в формате ГГГГ-ММ-ДДТЧЧ:ММ:СС</authored_date>
```

```
<links />

<definition>

<Indicator operator="OR" id="уникальный идентификатор в формате UUID">

<IndicatorItem id="уникальный идентификатор в формате UUID" condition="is">

<Context document="FileItem" search="FileItem/Md5sum" type="mir" />

<Content type="md5">MD5-хеш файла</Content>

</IndicatorItem>

</Indicator>

</definition>

</ioc>
```

Один IOC-файл может содержать только одно правило. Правило может быть любой сложности.

Пользователи с ролью **Старший сотрудник службы безопасности** могут импортировать, удалять, скачивать IOC-файлы на компьютер, включать и отключать поиск индикаторов компрометации по IOC-файлам, а также настраивать расписание поиска индикаторов компрометации на компьютерах с компонентом Endpoint Agent.

Пользователи с ролью **Сотрудник службы безопасности** и **Аудитор** могут просматривать список IOC-файлов и информацию о выбранном файле, а также экспортировать IOC-файлы на компьютер.

Просмотр таблицы IOC-файлов

Если вы используете режим распределенного решения и мультитенантности, вам нужно выполнять действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Таблица IOC-файлов содержит информацию об IOC-файлах, используемых для проверки на компьютерах с компонентом Endpoint Agent, и находится в разделе **Пользовательские правила**, подразделе **IOC** окна веб-интерфейса приложения.

В таблице IOC-файлов содержится следующая информация:

1. – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла.

   Степень важности может иметь одно из следующих значений:

   - – низкая важность.
   - – средняя важность.
   - – высокая важность.

2. **Тип** – тип IOC-файла в зависимости от режима работы приложения и сервера, на который загружен IOC-файл:

   - **Локальный** – IOC-файлы, загруженные на сервер SCN. По этим IOC-файлам производится поиск индикаторов компрометации на хостах с компонентом Endpoint Agent, подключенных к этому серверу SCN.

   - **Глобальный** – IOC-файлы, загруженные на сервер PCN. По этим IOC-файлам производится поиск индикаторов компрометации на хостах с компонентом Endpoint Agent, подключенных к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN.

3. **Имя** – имя IOC-файла.

4. **Серверы** – имя сервера с ролью PCN или SCN, на который распространяется правило.

   Столбец отображается, если вы используете режим распределенного решения и мультитенантности.

5. **Автоматическая проверка** – использование IOC-файла при автоматической проверке хостов с компонентом Endpoint Agent.

   Проверка хостов с использованием этого IOC-файла может находиться в одном из следующих состояний:

   - **Включено**.

   - **Выключено**.

Просмотр информации об IOC-файле

Чтобы просмотреть информацию об IOC-файле:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Выберите IOC-файл, информацию о котором вы хотите просмотреть.

Откроется окно с информацией об IOC-файле.

Окно содержит следующую информацию:

- **Найти алерты** – по ссылке открывается раздел **Алерты** с условием фильтрации, содержащим имя выбранного вами IOC-файла.

- **Найти события** – по ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим индикаторы компрометации выбранного вами IOC-файла.

- **Скачать** – по ссылке открывается окно скачивания IOC-файла.

- **Автоматическая проверка** – использование IOC-файла при автоматической проверке хостов с компонентом Endpoint Agent.

- **Имя** – имя IOC-файла.

- **Важность** – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла.

Степень важности может иметь одно из следующих значений:

- – низкая важность.
- – средняя важность.
-  – высокая важность.

- **Область применения** – отображает название тенанта и имена серверов, к которым относятся события, проверяемые по этому IOC-файлу (в режиме распределенного решения и мультитенантности).
- **XML** – отображает содержимое IOC-файла в формате XML.

Загрузка IOC-файла

IOC-файлы со свойствами UserItem для доменных пользователей не поддерживаются.

Чтобы загрузить IOC-файл:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Нажмите на кнопку **Импортировать**.

   Откроется окно выбора файла на вашем локальном компьютере.

3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.

4. Укажите следующие параметры:

   a. **Автоматическая проверка** – использование IOC-файла при автоматической проверке хостов с компонентом Endpoint Agent:

      - **Включено**.
      - **Выключено**.

   b. **Имя** – имя IOC-файла.

   c. **Важность** – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла:

      - **Низкая**.
      - **Средняя**.
      - **Высокая**.

d. **Область применения** – название тенанта и имена серверов, которые вы хотите проверять с помощью этого IOC-файла (в режиме распределенного решения и мультитенантности).

5. Нажмите на кнопку **Сохранить**.

IOC-файл будет загружен в формате XML.

Скачивание IOC-файла на компьютер

Вы можете скачать ранее загруженный IOC-файл на компьютер.

Чтобы скачать IOC-файл на компьютер:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Выберите IOC-файл, который вы хотите скачать.

   Откроется окно с информацией об IOC-файле.

3. В зависимости от параметров вашего браузера, по ссылке **Скачать** сохраните файл в папку по умолчанию или укажите папку для сохранения файла.

IOC-файл будет сохранен на компьютер в папку загрузки браузера.

Включение и отключение автоматического использования IOC-файла при проверке хостов

Вы можете включить или отключить автоматическое использование IOC-файла для поиска индикаторов компрометации на хостах с компонентом Endpoint Agent.

Чтобы включить или отключить автоматическое использование IOC-файла для поиска индикаторов компрометации на хостах с компонентом Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. В строке с IOC-файлом, использование которого вы хотите включить или отключить, в столбце **Состояние** переведите переключатель в одно из следующих положений:

   - **Включено**.
   - **Выключено**.

Автоматическое использование IOC-файла для поиска индикаторов компрометации на хостах с компонентом Endpoint Agent будет включено или отключено.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция включения или отключения автоматического использования IOC-файла недоступна.

Удаление IOC-файла

Чтобы удалить IOC-файл:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Выберите IOC-файл, который вы хотите удалить.

   Откроется окно с информацией об IOC-файле.

3. Нажмите на кнопку **Удалить**.

IOC-файл будет удален.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления IOC-файла недоступна.

Поиск алертов по результатам IOC-проверки

Чтобы найти и просмотреть результаты проверки по выбранному IOC-файлу:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Выберите IOC-файл, для которого вы хотите просмотреть результаты проверки.

   Откроется окно с информацией об IOC-файле.

3. Перейдите в базу алертов по ссылке **Найти алерты**.

   Откроется новая вкладка браузера с таблицей найденных алертов.

Вы также можете просмотреть результаты проверки по всем IOC-файлам, отфильтровав алерты по названию технологии.

Поиск событий по IOC-файлу

Чтобы просмотреть события, найденные с помощью IOC-файла:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Выберите IOC-файл, который вы хотите использовать для поиска событий по базе событий.

   Откроется окно с информацией об IOC-файле.

3. Перейдите в базу событий по ссылке **Найти события**.

   Откроется новая вкладка браузера с таблицей найденных событий.

Фильтрация и поиск IOC-файлов

Чтобы отфильтровать или найти IOC-файлы по требуемым критериям:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.
2. Откроется таблица IOC-файлов. Выполните следующие действия в зависимости от критерия фильтрации:

   - **По степени важности**

     a. По значку ≣ откройте окно настройки фильтрации IOC-файлов.

     b. Выберите одну или несколько из следующих степеней важности:

     - **Низкая**.
     - **Средняя**.
     - **Высокая**.

     c. Нажмите на кнопку **Применить**.

   - **По имени файла**

     a. По ссылке **Имя** откройте окно настройки фильтрации IOC-файлов.

     b. Введите один или несколько символов имени IOC-файла.

     c. Нажмите на кнопку **Применить**.

   - **По состоянию автоматической проверки (включена / выключена)**

     a. По ссылке **Автоматическая проверка** откройте окно настройки фильтрации IOC-файлов.

     b. Выберите один из следующих вариантов:

     - **Включено**.
     - **Выключено**.

   В таблице IOC-файлов отобразятся только IOC-файлы, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра IOC-файлов

Чтобы сбросить фильтр IOC-файлов по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.
2. Откроется таблица IOC-файлов.Нажмите на кнопку справа от того заголовка столбца таблицы IOC-файлов, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице IOC-файлов отобразятся только IOC-файлы, соответствующие заданным вами условиям.

Настройка расписания IOC-проверки

Вы можете настроить расписание поиска индикаторов компрометации с помощью IOC-файлов на хостах с компонентом Endpoint Agent.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** недоступна функция настройки расписания поиска индикаторов компрометации с помощью IOC-файлов.

Чтобы настроить расписание поиска индикаторов компрометации с помощью IOC-файлов на хостах с компонентом Endpoint Agent:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Endpoint Agents**, блок параметров **Расписание IOC-проверки**.
2. В раскрывающихся списках **Время запуска** выберите время начала поиска индикаторов компрометации. Время указывается в часовом поясе сервера Central Node, на котором выполняется настройка.

   Если Endpoint Agent получит новое расписание проверки позже того времени, которое указано в разделе **Расписание IOC-проверки**, очередная проверка будет запущена на следующий день в указанное время.
3. В раскрывающемся списке **Максимальное время проверки** выберите ограничение по времени выполнения поиска индикаторов компрометации.
4. Нажмите на кнопку **Применить**.

Новое расписание поиска индикаторов компрометации с помощью IOC-файлов на хостах с компонентом Endpoint Agent начнет действовать сразу после сохранения изменений. Результаты поиска индикаторов компрометации отобразятся в таблице алертов.

Управление поиском индикаторов компрометации с помощью IOC-файлов ограничено возможностями, доступными в веб-интерфейсе Kaspersky Anti Targeted Attack Platform. Других способов управления поиском индикаторов компрометации не предусмотрено.

Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Security для Windows, убедитесь, что IOC-файлы соответствуют требованиям. Также вам нужно учитывать, что при добавлении типа данных RegistryItem в область поиска IOC приложение анализирует только некоторые разделы реестра.

Подробнее о требованиях к IOC-файлам и проверяемых разделах реестра см. в справке Kaspersky Endpoint Security для Windows:

- Область поиска IOC в реестре (RegistryItem).
- Требования к IOC-файлам.

Работа с пользовательскими правилами обнаружения вторжений

Для обнаружения вторжений в трафике сети вы можете использовать правила обнаружения вторжений и дополнительные методы обнаружения вторжений по встроенным алгоритмам. При обнаружении в трафике признаков атак Kaspersky Anti Targeted Attack Platform регистрирует события по технологии *Обнаружение вторжений*.

Для работы с пользовательскими правилами обнаружения вторжений требуется действующий лицензионный ключ KATA или KATA + NDR.

Правило обнаружения вторжений описывает аномалию трафика, которая может быть признаком атаки в сети. Правила содержат условия, по которым система обнаружения вторжений анализирует трафик.

Приложение применяет правила обнаружения вторжений, если включен метод обнаружения вторжений по правилам. Вы можете включать и выключать применение метода.

Вы можете использовать следующие типы наборов правил:

- Системные наборы правил. Эти наборы правил поставляются "Лабораторией Касперского" и предназначены для обнаружения признаков наиболее часто встречающихся атак или нежелательной сетевой активности. Системные наборы правил доступны сразу после установки приложения. Вы можете обновлять системные наборы правил, устанавливая обновления. При необходимости вы можете создать для этих правил исключения из проверки. См. подробнее разделы *Работа с исключениями из правил обнаружения вторжений* и *Работа с разрешающими правилами для событий NDR*.

- Пользовательские наборы правил. Эти наборы правил вы самостоятельно загружаете в приложение. Для загрузки нужно использовать файлы, в которых содержатся структуры данных, задающие правила обнаружения вторжений. Файлы для загрузки должны находиться в одной директории и иметь расширение rules. Имена пользовательских наборов правил совпадают с именами файлов, из которых были загружены эти наборы правил.

  Пользовательские наборы правил обнаружения вторжений отображаются в разделе **Пользовательские правила** → **Обнаружение вторжений**.

Приложение поддерживает применение не более чем 50 000 правил суммарно во всех загруженных наборах правил. Ограничение количества загруженных наборов правил – не более 100.

Правила, загружаемые из пользовательских наборов правил, могут содержать такие условия для анализа трафика, по которым приложение будет регистрировать слишком большое количество событий срабатывания этих правил. В этом случае вам нужно учитывать, что регистрация слишком большого количества событий может повлиять на производительность системы обнаружения вторжений.

Наборы правил обнаружения вторжений могут быть включены или выключены. Правила из включенного набора применяются при анализе трафика, если включен метод обнаружения вторжений по правилам. Если набор правил выключен, правила из этого набора не применяются.

При загрузке набора правил приложение выполняет проверку содержащихся в нем правил. Если в проверяемых правилах обнаружены ошибки, приложение блокирует применение таких правил. Если обнаружены ошибки во всех правилах набора или набор не содержит правил, приложение выключает этот набор правил.

При обнаружении в трафике условий, заданных в правиле из включенного набора, приложение регистрирует событие срабатывания правила. Для регистрации используются системные типы событий, которым присвоены следующие коды:

- 4000003000 – для события при срабатывании правила из системного набора правил;
- 4000003001 – для события при срабатывании правила из пользовательского набора правил.

Пользовательские наборы правил могут содержать правила, полученные из других систем обнаружения и предотвращения вторжений. При обработке таких правил приложение не выполняет заданные в них действия, применяющиеся по отношению к сетевым пакетам (например, действия `drop` и `reject`). В результате срабатывания правил обнаружения вторжений в Kaspersky Anti Targeted Attack Platform выполняется только регистрация событий.

Значения оценок событий Kaspersky Anti Targeted Attack Platform соответствуют значениям приоритетов в правилах обнаружения вторжений (см. таблицу ниже).

Соответствие приоритетов правил и значений оценок событий

Значения приоритетов в правилах обнаружения вторжений	Значения оценок событий Kaspersky Anti Targeted Attack Platform
4 и более	2.5
3	4.5
2	6.5
1	9

Настройка параметров регистрации событий обнаружения вторжений выполняется в разделе **Параметры → Типы событий**.

Вы можете просмотреть события обнаружения вторжений в таблице зарегистрированных событий.

В режиме распределенного решения и мультитенантности пользовательские правила обнаружения вторжений могут быть одного из следующих типов:

- Созданные на сервере PCN. По этим правилам производится проверка трафика на сервере PCN.
- Созданные на сервере SCN. По этим правилам производится проверка трафика на сервере SCN.

Пользователи с ролью **Старший сотрудник службы безопасности** могут загружать, включать и выключать пользовательские наборы правил обнаружения вторжений, а также добавлять правила обнаружения вторжений "Лаборатории Касперского" в исключения из проверки. Пользователи с ролью **Аудитор** могут просматривать пользовательские наборы правил обнаружения. У пользователей с ролью **Сотрудник службы безопасности** нет доступа к пользовательским правилам обнаружения вторжений.

Просмотр таблицы правил обнаружения вторжений

Таблица пользовательских правил обнаружения вторжений находится в разделе **Пользовательские правила**, подразделе **Обнаружение вторжений** окна веб-интерфейса приложения.

В таблице содержится следующая информация:

- **Набор правил** – имя набора правил.
- **Автор** – имя пользователя, под учетной записью которого был загружен файл с правилами.
- **Состояние** – текущее состояние правила. Правило может находиться в одном из следующих состояний: **Включено**, **Выключено**.
- **Правила** – статус правил, которые входят в набор. Может отображаться один из следующих статусов: *OK*, *Ошибки во всех правилах*, *Ошибки в некоторых правилах*.
- **Размер файла** – размер загруженного файла с правилами.
- **Последнее обновление** – дата загрузки файла.

При необходимости вы можете настроить отображение столбцов в таблице.

Настройка отображения таблицы правил обнаружения вторжений

Вы можете настроить отображение столбцов в таблице правил обнаружения вторжений.

Чтобы настроить отображение таблицы правил обнаружения вторжений:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Обнаружение вторжений**.
2. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.
3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, переместите строку с параметром в нужное место, используя кнопки и .

5. Закройте окно настройки таблицы.

Отображение таблицы правил обнаружения вторжений будет настроено.

Дополнительные методы обнаружения вторжений

Для обнаружения вторжений вы можете применять следующие дополнительные методы:

- Обнаружение признаков подмены адресов в ARP-пакетах (ARP-спуфинг).

  Если включено обнаружение признаков подмены адресов в ARP-пакетах, Kaspersky Anti Targeted Attack Platform проверяет указываемые адреса в ARP-пакетах и обнаруживает признаки атак низкого уровня типа "человек посередине" (Man in the middle, MITM). Этот тип атак в сетях с использованием протокола ARP характеризуется наличием в трафике поддельных ARP-сообщений.

  При обнаружении признаков подмены адресов в ARP-пакетах приложение регистрирует события по технологии Обнаружение вторжений. Для регистрации используются системные типы событий, которым присвоены следующие коды:

  - 4000004001 – для события обнаружения нескольких ARP-ответов, которые не связаны с ARP-запросами;
  - 4000004002 – для события обнаружения нескольких ARP-запросов с одного MAC-адреса разным получателям.

- Обнаружение аномалий в протоколе TCP.

  Если включено обнаружение аномалий в протоколе TCP, Kaspersky Anti Targeted Attack Platform проверяет TCP-сегменты потока данных в поддерживаемых протоколах прикладного уровня.

  При обнаружении пакетов, содержащих перекрывающиеся TCP-сегменты с различающимся содержимым, приложение регистрирует событие по технологии Обнаружение вторжений. Для регистрации используется системный тип события с кодом 4000002701.

- Обнаружение аномалий в протоколе IP.

  Если включено обнаружение аномалий в протоколе IP, Kaspersky Anti Targeted Attack Platform проверяет фрагментированные IP-пакеты.

  При обнаружении ошибок сборки IP-пакетов приложение регистрирует события по технологии Обнаружение вторжений. Для регистрации используются системные типы событий, которым присвоены следующие коды:

  - 4000005100 – для события обнаружения конфликта данных при сборке IP-пакета (IP fragment overlapped);
  - 4000005101 – для события обнаружения IP-пакета с превышением максимально допустимого размера (IP fragment overrun);
  - 4000005102 – для события обнаружения IP-пакета с размером начального фрагмента меньше ожидаемого (IP fragment too small);
  - 4000005103 – для события обнаружения несоответствия фрагментов IP-пакета (mis-associated fragments).

- Обнаружение атак подбора и сканирования.

Если включено обнаружение атак подбора и сканирования, Kaspersky Anti Targeted Attack Platform проверяет статистику сетевой активности с целью выявления признаков атак подбора учетных данных, отказа в обслуживании, сканирования, подмены сетевых сервисов и других аномалий.

Метод использует встроенные правила. При срабатывании правил приложение регистрирует событие по технологии Обнаружение вторжений. Для регистрации используется системный тип события, которому присвоен код 4000003002.

Вы можете включать и выключать применение методов. Применять дополнительные методы обнаружения вторжений можно независимо от наличия и состояния правил обнаружения вторжений. Для проверки по дополнительным методам используются встроенные алгоритмы.

Включение и выключение наборов правил обнаружения вторжений

Наборам правил обнаружения вторжений могут быть присвоены статусы *Включено* или *Выключено*. Если набор правил выключен, все правила этого набора не используются при обнаружении вторжений.

При включении или выключении выбранных наборов правил на всех компьютерах с установленными компонентами приложения (Central Node и Sensor) выполняется перезапуск системы обнаружения вторжений. Перезапуск необходим для применения изменений.

Изменять состояния наборов правил обнаружения вторжений могут только пользователи с ролью **Старший сотрудник службы безопасности**.

Чтобы изменить статус наборов правил обнаружения вторжений:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Обнаружение вторжений**.
2. Установите флажки рядом с наборами правил, для которых вы хотите изменить статус.
3. По правой кнопке мыши откройте контекстное меню.
4. В контекстном меню выберите один из следующих пунктов:
   - **Включить**, если вы хотите включить все выключенные наборы правил из числа выбранных.
   - **Выключить**, если вы хотите выключить все включенные наборы правил из числа выбранных.
   - **Поменять статусы выбранных наборов правил**, если для всех выбранных наборов правил вы хотите одновременно инвертировать их статусы. Этот вариант позволяет быстрее включить и выключить выбранные наборы правил с разными статусами на всех компьютерах с установленными компонентами приложения – для применения изменений будет выполнен только один перезапуск системы обнаружения вторжений на этих компьютерах.
5. В окне запроса подтверждения нажмите на кнопку **ОК**.

Статус наборов правил обнаружения вторжений будет изменен.

Загрузка и замена пользовательских наборов правил обнаружения вторжений

Вы можете загрузить в приложение наборы правил обнаружения вторжений из файлов. Для загрузки в приложение файлы с описаниями правил обнаружения вторжений должны находиться в одной папке и иметь расширение rules. Имена файлов не должны содержать следующие символы: `\ / : * ? , " < > |`

После загрузки из файла правила обнаружения вторжений сохраняются в приложении в качестве пользовательского набора правил. Имя набора правил совпадает с именем файла, из которого этот набор был загружен.

При загрузке наборов правил из файлов текущие пользовательские наборы правил удаляются из таблицы и заменяются новыми.

Загружать пользовательские наборы правил обнаружения вторжений могут только пользователи с ролью **Старший сотрудник службы безопасности**.

Чтобы загрузить и заменить пользовательские наборы правил обнаружения вторжений:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Обнаружение вторжений**.
2. В панели инструментов нажмите на кнопку **Заменить все пользовательские правила**.
3. В окне подтверждения нажмите на кнопку **OK**.

   Откроется окно загрузки файла.
4. Выберите папку, в которой содержатся нужные файлы, и нажмите на кнопку загрузки файлов из этой папки.

   В таблице с наборами правил отобразятся новые пользовательские наборы правил. Все наборы правил, в которых не обнаружены ошибки, будут включены.
5. Проверьте наличие ошибок в правилах загруженных наборов.

   Сведения об обнаруженных ошибках отображаются в столбце **Правила**. При отсутствии ошибок отображается статус *OK*. Если набор правил содержит ошибки, вы можете просмотреть подробные сведения о них по ссылке **Подробнее**.
6. При необходимости включите или выключите наборы правил (в том числе тех наборов, для которых отображается статус *Ошибки в некоторых правилах*).

Пользовательские наборы правил обнаружения вторжений будут загружены.

Удаление пользовательских наборов правил обнаружения вторжений

Вы можете удалить все пользовательские наборы правил обнаружения вторжений, которые были загружены в приложение из файлов. Возможность выборочного удаления пользовательских наборов правил недоступна. Если вы хотите использовать в приложении только некоторые из имеющихся наборов правил, вы можете скопировать файлы с этими наборами в отдельную папку и заменить все пользовательские наборы правил на наборы правил из этой папки.

Удалять пользовательские наборы правил обнаружения вторжений могут только пользователи с ролью **Старший сотрудник службы безопасности**.

Чтобы удалить пользовательские наборы правил обнаружения вторжений:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Обнаружение вторжений**.
2. В панели инструментов нажмите на кнопку **Удалить все пользовательские правила**.
3. В окне подтверждения нажмите на кнопку **OK**.

   Отобразится окно для выбора папки с файлами правил обнаружения вторжений.

Все пользовательские наборы правил обнаружения вторжений будут удалены из таблицы.

Работа с пользовательскими правилами YARA

Вы можете использовать правила YARA в качестве баз модуля YARA для проверки файлов и объектов, поступающих на Central Node, и для проверки хостов с компонентом Endpoint Agent.

В режиме распределенного решения и мультитенантности пользовательские правила YARA могут быть одного из следующих типов:

- **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер PCN и все серверы SCN, подключенные к этому серверу PCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
- **Локальный** – созданные на сервере SCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер SCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.

При работе в веб-интерфейсе приложения пользователи с ролью **Старший сотрудник службы безопасности** могут импортировать файл правил YARA в Kaspersky Anti Targeted Attack Platform через веб-интерфейс приложения.

Пользователи с ролями **Аудитор** и **Сотрудник службы безопасности** могут только просматривать правила YARA.

Просмотр таблицы правил YARA

Таблица пользовательских правил YARA содержит информацию о правилах YARA, используемых для проверки файлов, объектов и создания обнаружений, и отображается в разделе **Пользовательские правила**, подразделе **YARA** окна веб-интерфейса приложения.

В таблице содержится следующая информация:

- **Создано** – время создания правила.
- – важность алерта для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние этот алерт может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

  По умолчанию алертам, созданным в результате проверки по загруженным правилам YARA, присваивается высокая степень важности.
- **Тип** – тип правила в зависимости от режима работы приложения и роли сервера, на котором оно было создано:
  - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер PCN и все серверы SCN, подключенные к этому серверу PCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
  - **Локальный** – созданные на сервере SCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер SCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
- **Имя** – название правила.
- **Файл** – название файла, из которого было импортировано правило.
- **Автор** – имя пользователя, под учетной записью которого было импортировано правило.
- **Серверы** – имя сервера с ролью PCN или SCN, на который распространяется правило.

  Столбец отображается, если вы используете режим распределенного решения и мультитенантности.
- **Проверка трафика** – состояние использования правила при потоковой проверке файлов и объектов, поступающих на Central Node:
  - **Включено** – правило используется.
  - **Выключено** – правило не используется.

Настройка отображения таблицы правил YARA

Вы можете настроить отображение столбцов, а также порядок их следования в таблице.

Чтобы настроить отображение таблицы:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.
2. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.
3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку  и переместите строку с параметром в нужное место.
5. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.
6. Нажмите на кнопку **Применить**.

Отображение таблицы будет настроено.

Импорт правил YARA

Чтобы импортировать правила YARA:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.
2. Нажмите на кнопку **Загрузить**.
   Откроется окно выбора файлов.
3. Выберите файл правил YARA, который вы хотите загрузить, и нажмите на кнопку **Открыть**.
   Окно выбора файлов закроется, откроется окно **Импорт правил YARA**.

   Максимальный допустимый размер загружаемого файла – 20 МБ.

   В нижней части окна отображается отчет. В отчете содержится следующая информация:

   - Количество правил, которые могут быть успешно импортированы.
   - Количество правил, которые не будут импортированы (если такие есть).
     Для каждого правила, которое не может быть импортировано, указывается его название.
4. Установите флажок **Проверка трафика**, если вы хотите использовать импортированные правила при потоковой проверке объектов и данных, поступающих на Central Node.
5. При необходимости в поле **Описание** введите любую дополнительную информацию.

   Поле **Важность** недоступно для редактирования. По умолчанию обнаружениям, выполненным по загружаемым правилам YARA, будет присвоена высокая степень важности.

6. В блоке параметров **Область применения** установите флажки напротив тех серверов, на которых вы хотите применить правила. На серверах, не отмеченных флажком, проверка с помощью загружаемых правил выполняться не будет. Если снят флажок в строке тенанта (первая строка списка), то серверы этого тенанта, добавляемые в дальнейшем, также не будут проверяться с помощью загружаемых правил.

   Блок параметров **Область применения** отображается только когда вы используете режим распределенного решения и мультитенантности.

7. Нажмите на кнопку **Сохранить**.

Импортированные правила отобразятся в таблице YARA-правил.

Просмотр информации о правиле YARA

Чтобы просмотреть информацию о правиле YARA:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. Выберите правило, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о правиле.

Окно содержит следующую информацию:

- **Алерты** – по ссылке в новой вкладке браузера откроется таблица алертов, отфильтрованных по технологии Targeted Attack Analyzer и имени правила TAA (IOA), с которым вы работаете.
- **Запустить YARA-проверку** – по ссылке открывается окно создания задачи.
- **Скачать** – по ссылке скачивается файл с правилами YARA.
- **Правило** – имя правила, указанное в файле.
- **Проверка трафика** – использование правила при потоковой проверке файлов и объектов, поступающих на Central Node.
- **Тип** – тип правила в зависимости от роли сервера, на котором оно создано:
  - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер PCN и все серверы SCN, подключенные к этому серверу PCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
  - **Локальный** – созданные на сервере SCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер SCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
- **Важность** – степень важности, которая присваивается алерту, созданному в результате проверки по этому правилу.

  По умолчанию алертам, созданным в результате проверки по загруженным правилам YARA, присваивается высокая степень важности.

- **Описание** – любая дополнительная информация о правиле, которую вы указали.
- **Область применения** – имена серверов с компонентом Central Node, на которых применяется правило.

Фильтрация и поиск правил YARA

Чтобы отфильтровать или найти правила YARA по требуемым критериям:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. Выполните следующие действия в зависимости от критерия фильтрации:

   - **По времени создания**

     a. По ссылке **Создано** откройте окно настройки фильтрации.

     b. Выберите один из следующих вариантов:

     - **За все время**, если вы хотите, чтобы приложение отображало в таблице правила, созданные за все время.
     - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице правила, созданные за предыдущий час.
     - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице правила, созданные за предыдущий день.
     - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице правила, созданные за указанный вами период.

     c. Если вы выбрали **Пользовательский диапазон**, выберите даты начала и конца периода и нажмите на кнопку **Применить**.

   - **По имени правила**

     a. По ссылке **Правило** откройте меню фильтрации.

     b. В раскрывающемся списке выберите один из следующих операторов фильтрации:

     - **Содержит**.
     - **Не содержит**.

     c. В поле ввода введите название правила или несколько символов из названия правила.

     d. Нажмите на кнопку **Применить**.

- **По имени файла**

  a. По ссылке **Файл** откройте меню фильтрации.

  b. В раскрывающемся списке выберите один из следующих операторов фильтрации:

  - **Содержит**.
  - **Не содержит**.

  c. В поле ввода введите название файла или несколько символов из названия файла.

  d. Нажмите на кнопку **Применить**.

- **По имени пользователя, загрузившего файл с правилами**

  a. По ссылке **Автор** откройте меню фильтрации.

  b. В раскрывающемся списке выберите один из следующих операторов фильтрации:

  - **Содержит**.
  - **Не содержит**.

  c. В поле ввода введите имя пользователя или несколько символов из имени пользователя.

  d. Нажмите на кнопку **Применить**.

- **По состоянию правила**

  a. По ссылке **Проверка трафика** раскройте список настройки фильтрации.

  b. Выберите один из следующих вариантов:

  - **Все**.
  - **Включено**.
  - **Выключено**.

В таблице отобразятся только правила, соответствующие заданным условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил YARA

Чтобы сбросить фильтрацию правил YARA по одному или нескольким условиям:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.
   Откроется таблица правил YARA.

2. Нажмите на кнопку справа от того заголовка столбца таблицы правил, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу для каждого из условий.

Выбранные фильтры будут сброшены.

В таблице отобразятся только правила, соответствующие заданным условиям.

Включение и отключение использования правил YARA

Пользователи с ролью **Старший сотрудник службы безопасности** могут включить или отключить использование одного или нескольких правил, а также всех правил сразу.

При работе в режиме распределенного решения и мультитенантности вы можете включить или отключить использование правил YARA, которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно включение и отключение использования только правил, созданных на сервере PCN. В веб-интерфейсе SCN доступно включение и отключение использования только правил, созданных на сервере SCN.

Если на серверах PCN и SCN включено использование правил YARA с одинаковыми именами, при проверке файлов и объектов, поступающих на SCN, применяется правило, созданное на PCN.

Чтобы включить или отключить использование правила YARA при потоковой проверке файлов и объектов, поступающих на Central Node:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. В строке с нужным правилом в столбце **Проверка трафика** включите или отключите переключатель.

Использование правила при потоковой проверке файлов и объектов, поступающих на Central Node, будет включено или отключено.

Чтобы включить или отключить использование всех или нескольких правил YARA при потоковой проверке файлов и объектов, поступающих на Central Node:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.

2. Установите флажки слева от правил, использование которых вы хотите включить или отключить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Включить** или **Отключить**, чтобы включить или отключить использование всех правил.

Использование выбранных правил при потоковой проверке файлов и объектов, поступающих на Central Node, будет включено или отключено.

Удаление правил YARA

Чтобы удалить правило YARA:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.
   Откроется таблица правил YARA.
2. Выберите правило, которое вы хотите удалить.
   Откроется окно с информацией об этом правиле.
3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне подтверждения действия нажмите на кнопку **Да**.

Правило будет удалено.

Чтобы удалить все или несколько правил YARA:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.
   Откроется таблица правил YARA.
2. Установите флажки слева от правил, которые вы хотите удалить.
   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.
   В нижней части окна отобразится панель управления.
3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне подтверждения действия нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления правила YARA недоступна.

Работа с объектами в Хранилище и на карантине

В Хранилище помещаются файлы, которые нужно отправить на проверку, а также файлы, полученные в результате выполнения задач **Получить файл**, **Восстановить файл из карантина**, **Собрать форензику**, **Получить метафайлы NTFS**, **Получить ключ реестра**, **Получить дамп памяти процесса**.

Хранилище расположено на сервере Central Node.

Вы можете управлять объектами в Хранилище: удалять, скачивать, загружать, отправлять на проверку, а также фильтровать списки объектов.

Kaspersky Anti Targeted Attack Platform отображает объекты в Хранилище в виде таблицы объектов.

Если вы используете режим распределенного решения и мультитенантности, Хранилище расположено на серверах PCN и SCN. В веб-интерфейсе сервера PCN отображается информация о Хранилище всех подключенных SCN в рамках тех тенантов, к данным которых у пользователя есть доступ.

Пользователь с ролью **Старший сотрудник службы безопасности** может поместить копии объектов в Хранилище с помощью задач или загрузив объект в Хранилище через веб-интерфейс Kaspersky Anti Targeted Attack Platform на том сервере PCN или SCN, с которым он работает в рамках тех тенантов, к данным которых у него есть доступ.

Пользователь с ролью **Сотрудник службы безопасности** может работать только с файлами, полученными в результате выполнения задач, которые он сам создал на том сервере PCN или SCN, с которым он работает в рамках тех тенантов, к данным которых у него есть доступ.

Если вы считаете файл опасным, вы можете поместить его на карантин на компьютере с компонентом Endpoint Agent. Метаданные файла, помещенного на карантин, отобразятся в разделе **Хранилище**, подразделе **Карантин** веб-интерфейса Kaspersky Anti Targeted Attack Platform.

Карантин на сервере Kaspersky Anti Targeted Attack Platform – это область Хранилища серверной части решения Kaspersky Anti Targeted Attack Platform, предназначенная для хранения метаданных объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent, в разделе **Хранилище**, подразделе **Карантин** веб-интерфейса Kaspersky Anti Targeted Attack Platform.

Вы можете управлять объектами на карантине: восстанавливать объекты из карантина, а также загружать копии объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent, в Хранилище Kaspersky Anti Targeted Attack Platform.

Kaspersky Anti Targeted Attack Platform отображает информацию об объектах, помещенных на карантин, в виде таблицы.

Максимальный объем Хранилища определяется при настройке параметров масштабирования приложения. Как только объем Хранилища превышает заданное по умолчанию пороговое значение, приложение начинает удалять из Хранилища самые старые копии объектов. Когда объем Хранилища снова становится меньше порогового значения, приложение прекращает удалять копии объектов из Хранилища.

Максимальный размер объекта, который можно поместить в Хранилище, составляет 1 ГБ.

Реальный размер объекта может быть больше видимого размера объекта из-за метаданных, необходимых для восстановления объекта из карантина. При помещении на карантин учитывается реальный размер объекта. Зашифрованные файлы могут передаваться в расшифрованном виде (в зависимости от параметров шифрования), сжатые файлы передаются в исходном виде.

Просмотр таблицы объектов, помещенных в Хранилище

Таблица объектов, помещенных в Хранилище, находится в разделе **Хранилище**, подразделе **Файлы** веб-интерфейса приложения.

В таблице объектов, помещенных в Хранилище, содержится следующая информация:

1. **Тип** – способ, которым объект был помещен в Хранилище.

Возможны следующие способы:

- – объект помещен в хранилище одним из следующих способов:
  - выполнена задача **Получить файл**;
  - получена копия объекта, помещенного на карантин на хостах с компонентом Endpoint Agent (в разделе **Хранилище**, подразделе **Карантин** в меню, раскрывшемся по ссылке с директорией объекта, выбрано действие **Получить файл из карантина**).
- – объект помещен в хранилище одним из следующих способов:
  - выполнена задача **Собрать форензику**;
  - выполнена задача **Получить дамп памяти процесса**;
  - выполнена задача **Получить ключ реестра**;
  - выполнена задача **Получить метафайлы NTFS**.
- – объект загружен пользователем вручную в разделе **Хранилище**, подразделе **Файлы**.

2. **Объект** – информация об объекте. Например, имя файла или путь к файлу.

3. **Результаты проверки** – результат проверки объекта.

   Результат проверки отображается в виде одного из следующих значений:

   - **Не обнаружено** – в результате проверки приложение не обнаружила признаков целевой атаки, возможно зараженных объектов или подозрительной активности.
   - **Ошибка выполнения** – проверка объекта завершилась с ошибкой.
   - **Выполняется** – проверка объекта еще не завершилась.
   - **Не выполнялась** – объект не был отправлен на проверку.
   - **Обнаружено** – в результате проверки приложение обнаружило признаки целевой атаки, возможно зараженный объект или подозрительную активность.

4. **Серверы** – имя сервера с ролью PCN или SCN. К этому серверу подключен хост, с которого получен объект

   Столбец отображается, если вы используете режим распределенного решения и мультитенантности.

5. **Адрес источника** – IP-адрес или имя хоста, с которого получен объект, или имя учетной записи пользователя, загрузившего объект.

6. **Время** – дата и время помещения объекта в Хранилище.

7. **Действия** – действия, которые можно выполнить с объектом. Доступны следующие действия:

   - – удалить объект из Хранилища.
   - – отправить объект из Хранилища на проверку технологиями Anti-Malware Engine, YARA и Sandbox.
   - – скачать объект из Хранилища на компьютер.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скачать**.
- **Отправить файл на проверку**.
- **Найти события**:
  - **Путь к файлу**.
  - **MD5**.
  - **SHA256**.
- **Найти алерты**:
  - **Путь к файлу**.
  - **MD5**.
  - **SHA256**.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

Просмотр информации об объекте, загруженном в Хранилище через веб-интерфейс

Чтобы просмотреть информацию об объекте, загруженном в Хранилище вручную, выполните следующие действия:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. В таблице выберите объект со значком , информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- **Файл** – имя файла.
- **Размер** – размер файла.
- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Время загрузки** – время загрузки для объектов, загруженных пользователем вручную.
- **Имя пользователя** – имя учетной записи пользователя, загрузившего объект в Хранилище вручную.
- **Результаты проверки** – результат проверки объекта приложением.

Кнопка **Найти на Kaspersky TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

Кнопка **Создать правило запрета** позволяет запретить запуск файла.

Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

По ссылке с именем файла раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky TIP**.
- **Найти события**.
- **Найти алерты**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке с **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky TIP**.
- **Найти на virustotal.com**.
- **Найти события**.
- **Найти алерты**.

- Создать правило запрета.
- **Скопировать значение в буфер**.

Просмотр информации об объекте, помещенном в Хранилище по задаче получения файла

*Чтобы просмотреть информацию об объекте, помещенном в Хранилище по задаче **Получить файл** или **Получить файл из карантина**:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. В таблице выберите объект со значком , информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- Блок рекомендаций. Могут отображаться следующие рекомендации:
  - Задача – ссылка, по которой открывается задача, с помощью которой объект был помещен в Хранилище.
  - Алерт – ссылка, по которой открывается алерт, содержащий объект, помещенный в Хранилище.
  - **Объект на карантине** – ссылка, по которой открываются метаданные объекта на карантине.
- **Объект** – имя файла или путь к файлу.
- **Размер** – размер файла.
- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Время** – время помещения объекта в Хранилище.
- **Тенант** – название тенанта, к которому относится сервер Central Node, PCN или SCN.
- **Сервер** – имя сервера Central Node, PCN или SCN. К этому серверу подключен хост, с которого получен объект.
- **Хост** – имя хоста, с которого получен объект.
- **Результаты проверки** – результат проверки объекта приложением.

Кнопка **Sandbox-обнаружение** позволяет просмотреть подробную информацией о результатах исследования поведения файла.

> Результаты исследования поведения файла отображаются, только если для этого файла было выполнено обнаружение компонентом Sandbox. Если файл был загружен в систему и затем проверен в Sandbox, но компонент при этом не обнаружил угрозу, результаты исследования не отображаются.

Кнопка **Найти на Kaspersky TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

Кнопка **Создать правило запрета** позволяет запретить запуск файла.

Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

По ссылке с именем файла раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky TIP**.
- **Найти события**.
- **Найти алерты**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке с **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky TIP**.
- **Найти на virustotal.com**.
- **Найти события**.
- **Найти алерты**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Просмотр информации об объекте, помещенном в Хранилище по задаче получения данных

*Чтобы просмотреть информацию об объекте, помещенном в Хранилище по задачам **Собрать форензику**, **Получить дамп памяти процесса**, **Получить ключ реестра**, **Получить метафайлы NTFS**:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. В таблице выберите объект со значком , информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- **Объект** – имя файла или путь к файлу.
- **Размер** – размер файла.
- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Время** – время помещения объекта в Хранилище.
- **Хост** – имя хоста, с которого получен объект.

Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

По ссылке с именем файла раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky TIP**.
- **Найти события**.
- **Найти алерты**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке с **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky TIP**.
- **Найти на virustotal.com**.
- **Найти события**.
- **Найти алерты**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Скачивание объектов из Хранилища

Если вы считаете объект в Хранилище безопасным, вы можете скачать его на локальный компьютер.

Скачивание зараженных объектов может угрожать безопасности вашего локального компьютера.

Чтобы скачать объект из Хранилища:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. В правой части строки с именем объекта, который вы хотите скачать, нажмите на кнопку .

Объект будет сохранен на ваш локальный компьютер в папку загрузки браузера. Файл загружается в формате ZIP-архива, защищенного паролем infected.

Загрузка объектов в Хранилище

Если вам требуется запустить проверку определенного объекта, вы можете загрузить этот объект в Хранилище и отправить его на проверку.

Чтобы загрузить объект в Хранилище:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. В правом верхнем углу окна нажмите на кнопку **Загрузить**.

   Откроется окно выбора файла.

3. Выберите объект, который вы хотите загрузить в Хранилище.

4. Если вы хотите загрузить в Хранилище файл с расширением .lnk, выполните следующие действия:

   a. В поле **File name** введите *.lnk и нажмите на клавишу **Enter**.

   b. Выберите объект.

5. Нажмите на кнопку **Open**.

Объект будет загружен в Хранилище и отобразится в таблице объектов.

Для пользователей с ролью **Аудитор** функция загрузки объектов в Хранилище недоступна.

Отправка объектов из Хранилища на проверку

Вы можете проверить объекты, помещенные в Хранилище, компонентом Central Node с помощью технологий Anti-Malware Engine и YARA, а также компонентом Sandbox.

Рекомендуется отправлять объекты из Хранилища на проверку в следующих случаях:

- проверка при помещении в Хранилище была отключена;
- базы приложения были обновлены;
- объект был загружен в Хранилище вручную.

Чтобы отправить объект из Хранилища на проверку:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. Нажмите на объект, который вы хотите проверить.

   Откроется окно сведений об объекте.

3. Нажмите на кнопку **Проверить**.

   Запустится проверка объекта.

   После завершения проверки объекта его статус отобразится в таблице объектов.

Вы также можете отправить объект из Хранилища на проверку нажатием на кнопку в правой части строки с информацией об объекте в таблице объектов, помещенных в Хранилище.

Для пользователей с ролью **Аудитор** функция проверки объектов, помещенных в хранилище, недоступна.

Удаление объектов из Хранилища

Чтобы удалить объект из Хранилища:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. Нажмите на объект, который вы хотите удалить.

   Откроется окно сведений об объекте.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Объект будет удален из Хранилища.

Вы также можете удалить объект из Хранилища нажатием на кнопку в правой части строки с информацией об объекте в таблице объектов, помещенных в Хранилище.

Чтобы удалить все или несколько объектов из Хранилища:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. Установите флажки напротив объектов, которые вы хотите удалить из Хранилища.

   Вы можете выбрать все объекты, установив флажок в строке с заголовками столбцов.

3. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранные объекты будут удалены из Хранилища.

Для пользователей с ролью **Аудитор** функция удаления объектов, помещенных в хранилище, недоступна.

Фильтрация объектов в Хранилище по типу объекта

Чтобы отфильтровать объекты в Хранилище по их типу:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. По ссылке **Тип** откройте меню фильтрации объектов.

3. Установите один или несколько флажков:

   - **Загружен по задаче Получить файл**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные в Хранилище по задачам **Получить файл** и **Восстановить файл из карантина**.
   - **Загружен через веб-интерфейс**, если вы хотите, чтобы приложение отображало в таблице объекты, загруженные пользователем через веб-интерфейс Kaspersky Anti Targeted Attack Platform.
   - **Загружен по задаче получения данных**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные в Хранилище по задачам **Собрать форензику**, **Получить метафайлы NTFS**, **Получить ключ реестра**, **Получить дамп памяти процесса**.

4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по описанию объекта

Чтобы отфильтровать объекты в Хранилище по описанию объекта:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. По ссылке **Объект** откройте меню фильтрации объектов.
3. В раскрывающемся списке выберите один из следующих вариантов:

   - **Путь к файлу**.
   - **MD5**.
   - **SHA256**.

4. В раскрывающемся списке выберите один из следующих операторов фильтрации объектов:

   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.
   - **Соответствует шаблону**.
   - **Не соответствует шаблону**.

5. В поле ввода укажите один или несколько символов описания объекта.

6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

7. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по результатам проверки

Чтобы отфильтровать объекты в Хранилище по результатам проверки этих объектов:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. По ссылке **Результаты проверки** откройте меню фильтрации объектов.

3. Установите один или несколько флажков:

   - **Не обнаружено**.
   - **Ошибка выполнения**.
   - **Выполняется**.
   - **Не выполнялась**.
   - **Обнаружено**.

4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по имени сервера Central Node, PCN или SCN

Чтобы отфильтровать объекты в Хранилище по имени сервера Central Node, PCN или SCN:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. По ссылке **Серверы** откройте меню фильтрации объектов.

3. Установите один или несколько флажков напротив тех серверов, по которым вы хотите отфильтровать объекты в Хранилище.

4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по источнику объекта

Чтобы отфильтровать объекты в Хранилище по источнику, с которого они были получены:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. По ссылке **Адрес источника** откройте меню фильтрации объектов.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации объектов:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов IP-адреса, имени хоста или имени учетной записи пользователя, загрузившего объект вручную.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов по времени помещения в Хранилище

Чтобы отфильтровать объекты по времени помещения в Хранилище:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. По ссылке **Время** откройте меню фильтрации объектов.

3. Выберите один из следующих периодов отображения объектов:

   - **Все**, если вы хотите, чтобы приложение отображало в таблице все помещенные в Хранилище объекты.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные в Хранилище за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные в Хранилище за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные в Хранилище за указанный вами период.

4. Если вы выбрали период отображения объектов **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения объектов.

   b. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра объектов в Хранилище

Чтобы сбросить фильтр объектов в Хранилище по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. Нажмите на кнопку справа от того заголовка столбца таблицы объектов в Хранилище, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Просмотр таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent

Таблица объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent, находится в разделе **Хранилище**, подразделе **Карантин** веб-интерфейса приложения.

На сервере Kaspersky Anti Targeted Attack Platform хранятся метаданные объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent. Сами объекты хранятся в специальном хранилище на каждом компьютере, на котором был обнаружен опасный объект.

В таблице объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent, содержится следующая информация:

1. **Объект** – информация об объекте. Например, имя файла или путь к файлу.
2. **Адрес источника** – IP-адрес или имя хоста компьютера с компонентом Endpoint Agent, на карантине которого находится объект.
3. **Время** – дата и время помещения объекта на карантин.
4. **Состояние** – состояние объекта.

В правой части строки с информацией об объекте расположены кнопки:

- Кнопка позволяет удалить метаданные объекта на сервере Kaspersky Anti Targeted Attack Platform.
- Кнопка позволяет восстановить объект из карантина на компьютере с компонентом Endpoint Agent.
- Кнопка позволяет получить копию объекта из карантина на компьютере с компонентом Endpoint Agent на сервер Kaspersky Anti Targeted Attack Platform.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скачать**.
- **Отправить файл на проверку**.
- **Найти события**:
  - **Путь к файлу**.
  - **MD5**.
  - **SHA256**.
- **Найти алерты**:
  - **Путь к файлу**.
  - **MD5**.
  - **SHA256**.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

Просмотр информации об объекте на карантине

Чтобы просмотреть информацию об объекте, помещенном на карантин на компьютере с компонентом Endpoint Agent:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. В таблице выберите объект, информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- Блок рекомендаций. Может отображаться рекомендация **Задача** – ссылка, по которой открывается раздел **Задачи**, задача, с помощью которой объект был помещен на карантин.
- **Тип** – тип объекта, помещенного на карантин.

  Возможны следующие типы объектов:

  - – файл.
  - – дамп памяти процесса.
- **Объект** – имя файла или путь к файлу.
- **Состояние** – состояние файла (можно ли восстановить файл из карантина).
- **Адрес источника** – имя компьютера с компонентом Endpoint Agent, на карантине которого находится объект.
- **Время** – время помещения объекта на карантин.
- **Действия** – состояние файла (можно ли восстановить файл из карантина).

  Доступны следующие действия:

  - – удалить файл из карантина.
  - – получить копию файла на сервер Kaspersky Anti Targeted Attack Platform.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти алерты**.
- **Скопировать значение в буфер**.

Восстановление объекта из карантина

Чтобы восстановить объект из карантина на компьютере с компонентом Endpoint Agent:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. В таблице выберите объект, который вы хотите восстановить из карантина на компьютере с компонентом Endpoint Agent.

   Откроется окно сведений об объекте.

3. Нажмите на кнопку **Восстановить** в нижней части окна.

   Откроется раздел **Задачи**, задача **Восстановить файл из карантина**.

4. В поле **Описание** введите описание задачи.

5. Нажмите на кнопку **Добавить**.

Файл будет восстановлен из карантина.

Вы также можете запустить задачу восстановления файла из карантина нажатием на кнопку в правой части строки с информацией об объекте таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent.

В режиме распределенного решения и мультитенантности файл, помещенный на карантин сервера SCN, нельзя восстановить на сервере PCN. Вы можете восстановить файл на том сервере SCN, где была создана задача для помещения файла на карантин.

Для пользователей с ролью **Аудитор** функция восстановления объекта из карантина недоступна.

Получение копии объекта на карантине на сервер Kaspersky Anti Targeted Attack Platform

Размер объекта, копию которого требуется получить, не должен превышать 100 МБ. Если размер объекта превышает 100 МБ, задача завершается ошибкой.

Чтобы получить копию объекта, помещенного на карантин на компьютере с компонентом Endpoint Agent, на сервер Kaspersky Anti Targeted Attack Platform:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. В таблице выберите объект, который вы хотите восстановить из карантина на компьютере с компонентом Endpoint Agent.

   Откроется окно сведений об объекте.

3. Нажмите на кнопку **Получить файл** в нижней части окна.

   Будет создана задача получения копии объекта, помещенного на карантин на компьютере с компонентом Endpoint Agent. При успешном завершении задачи копия объекта загрузится на сервер Kaspersky Anti Targeted Attack Platform. Объект отобразится в разделе **Хранилище**, подразделе **Файлы** веб-интерфейса приложения в таблице объектов, помещенных в Хранилище.

   Информация о задаче отобразится в разделе **Задачи** веб-интерфейса.

Вы также можете получить копию объекта из карантина на компьютере с компонентом Endpoint Agent на сервер Kaspersky Anti Targeted Attack Platform нажатием на кнопку в правой части строки с информацией об объекте таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent.

Для пользователей с ролью **Аудитор** получение копии объекта из карантина недоступно.

Удаление информации об объекте, помещенном на карантин, из таблицы

Чтобы удалить информацию об объекте, помещенном на карантин на компьютере с компонентом Endpoint Agent, из таблицы Kaspersky Anti Targeted Attack Platform:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. Нажмите на объект, информацию о котором вы хотите удалить из таблицы.

   Откроется окно сведений об объекте.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

   Информация об объекте, помещенном на карантин на компьютере с компонентом Endpoint Agent, будет удалена из таблицы.

Вы также можете удалить информацию об объекте, помещенном на карантин на компьютере с компонентом Endpoint Agent, из таблицы нажатием на кнопку в правой части строки с информацией об объекте в таблице объектов, помещенных на карантин.

Для пользователей с ролью **Аудитор** удаление информации об объекте, помещенном на карантин, из таблицы недоступно.

Фильтрация информации об объектах, помещенных на карантин, по типу объекта

Чтобы отфильтровать информацию об объектах, помещенных на карантин, по их типу:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. По ссылке **Тип** откройте меню фильтрации объектов.

3. Установите один или несколько флажков:

   - **Файл**, если вы хотите, чтобы приложение отображало в таблице метаданные объектов, помещенных на карантин.
   - **Дамп памяти процесса**, если вы хотите, чтобы приложение отображало в таблице метаданные дампов, помещенных на карантин.

4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация информации об объектах, помещенных на карантин, по описанию объекта

Чтобы отфильтровать информацию об объектах, помещенных на карантин, по описанию объекта:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. По ссылке **Объект** откройте меню фильтрации объектов.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации объектов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов описания объекта.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация информации об объектах, помещенных на карантин, по имени хоста

Чтобы отфильтровать информацию об объектах, помещенных на карантин, по имени хоста, на котором они были помещены на карантин:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.
2. По ссылке **Адрес источника** откройте меню фильтрации объектов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации объектов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов имени хоста.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация информации об объектах, помещенных на карантин, по времени

Чтобы отфильтровать информацию об объектах, помещенных на карантин, по времени помещения на карантин:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. По ссылке **Время** откройте меню фильтрации объектов.

3. Выберите один из следующих периодов отображения объектов:

   - **Все**, если вы хотите, чтобы приложение отображало в таблице все объекты.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные на карантин за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные на карантин за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные на карантин за указанный вами период.

4. Если вы выбрали период отображения объектов **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения объектов.

   b. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра информации об объектах на карантине

Чтобы сбросить фильтр по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. Нажмите на кнопку справа от того заголовка столбца таблицы объектов на карантине, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Работа с отчетами

С помощью Kaspersky Anti Targeted Attack Platform пользователи с ролью **Старший сотрудник службы безопасности** могут управлять отчетами об обнаружениях приложения: создавать шаблоны отчетов, создавать отчеты по шаблону, просматривать и удалять отчеты и шаблоны отчетов.

Пользователи с ролью **Аудитор** могут просматривать отчеты и шаблоны отчетов и создавать отчеты по шаблону.

Доступны следующие виды отчетов:

- Общие отчеты. Шаблоны этих отчетов доступны в разделе **Отчеты**, подразделе **Шаблоны**. Сформированные отчеты доступны в разделе **Отчеты**, подразделе **Созданные отчеты**.

  Управление шаблонами отчетов и отчетами доступно во всех режимах работы приложения в соответствии с лицензией. Отчеты формируются на основе выборки обнаружений за указанный период. Если вы используете режим распределенного решения и мультитенантности, выборка данных осуществляется также по тенанту и серверам этого тенанта.

- Отчеты по функциональности NDR. Доступны в разделе **Отчеты**, подразделе **Отчеты (NDR)**.

  Управление шаблонами отчетов и отчетами доступно при добавлении лицензионного ключа KATA + NDR. Отчеты формируются на основе выборки обнаружений за указанный период по данным узла, на котором запущено формирование отчета.

Работа с общими отчетами

При работе в веб-интерфейсе приложения пользователи с ролью **Старший сотрудник службы безопасности** могут управлять отчетами KATA об обнаружениях приложения: создавать шаблоны отчетов, создавать отчеты по шаблону, просматривать и удалять отчеты и шаблоны отчетов.

Пользователи с ролью **Аудитор** могут просматривать отчеты KATA и шаблоны отчетов и создавать отчеты по шаблону.

Выполняйте действия по созданию отчета KATA в следующем порядке:

1. **Создайте шаблон отчета**
2. **Создайте отчет на основе шаблона**

Просмотр таблицы шаблонов и отчетов

Шаблоны и отчеты отображаются в разделе **Отчеты** окна веб-интерфейса приложения.

В подразделе **Созданные отчеты** отображается таблица отчетов. Таблица содержит следующую информацию:

- **Время создания** – дата и время создания отчета.
- **Имя отчета** – имя отчета, созданного по шаблону.
- **Период** – период, за который создан отчет.
- **Серверы** – имя сервера с ролью PCN или SCN, на который распространяется правило.
  Столбец отображается, если вы используете режим распределенного решения и мультитенантности.
- **Автор** – имя пользователя, создавшего отчет.
- **Состояние** – состояние отчета (можно ли скачать файл).

В подразделе **Шаблоны** отображается таблица шаблонов. Таблица содержит следующую информацию:

- **Время создания** – дата и время создания шаблона.
- **Время обновления** – дата и время последнего изменения шаблона.
- **Имя отчета** – имя шаблона.
- **Автор** – имя пользователя, создавшего шаблон.

Создание шаблона

При создании шаблона отчета вам нужно указать всю информацию, которую вы хотите отображать в отчете: имя отчета, его описание, наличие таблицы, графика или изображения. Также вы можете выбрать данные, которые вы хотите отображать в отчете и задать расположение элементов отчета.

Создание отчета в разделе **Отчеты**, подразделе **Созданные отчеты** интерфейса позволяет только выбрать шаблон для создания отчета и период отображения данных.

Новый шаблон отчета создается для каждой выборки данных.

Чтобы создать шаблон:

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.
   Откроется таблица шаблонов.

2. Нажмите на кнопку **Добавить**.

   Откроется окно создания шаблона. Окно содержит тело отчета и конструктор отчета в плавающем окне. Вы можете перемещать конструктор отчета по рабочей области окна веб-интерфейса.

3. В поле **Имя шаблона** в правом верхнем углу окна введите имя, которое вы хотите присвоить отчетам, создаваемым по этому шаблону. Например, **Алерты по технологии**.

   Это имя отобразится в таблице в разделе **Отчеты**, подразделе **Созданные отчеты** при создании всех отчетов на этом шаблоне.

4. Вместо текста **Заголовок отчета** введите имя отчета, которое отобразится в отчете после создания отчета. Если вы не хотите добавлять имя отчета, вы можете удалить текст **Заголовок отчета** и оставить этот раздел отчета пустым.

   Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.

5. Вместо текста **Описание отчета** введите описание отчета, которое отобразится в отчете после создания отчета. Если вы не хотите добавлять описание отчета, вы можете удалить текст **Описание отчета** и оставить этот раздел отчета пустым.

   Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.

6. Используя конструктор отчета, добавьте один или несколько элементов отчета:

   - **Таблица**.
   - **Диаграмма**.
   - **Изображение**.

7. Если вы выбрали добавление изображения, откроется окно **Изображение**. Выполните следующие действия:

   a. Нажмите на кнопку **Загрузить**.

   b. Загрузите изображение. Например, вы можете загрузить логотип вашей организации.

   c. В списке справа от кнопки загрузки выберите выравнивание изображения на странице отчета: **По левому краю**, **По правому краю** или **По центру**.

   d. Нажмите на кнопку **Применить**.

8. Если вы выбрали добавление диаграммы, откроется окно **Диаграмма по свойствам алертов**. Выполните следующие действия:

   a. В поле **Имя** введите имя диаграммы. Например, **Топ 5 алертов по технологии**. Вы также можете оставить поле пустым.

   b. В списке **Источник данных** выберите свойство алерта, по которому вы хотите создать диаграмму. Например, **Технологии**.

c. В поле **Количество секторов** укажите максимальное количество секторов диаграммы.

При создании отчета приложение выберет наиболее часто встречающиеся данные. Например, если вы указали 5 секторов и хотите создать диаграмму по технологии, приложение покажет диаграмму по 5 технологиям, в результате проверки которых было создано наибольшее количество алертов. Технологии, по которым было создано меньшее количество алертов, не отобразятся на диаграмме.

d. Нажмите на кнопку **Применить**.

9. Если вы выбрали добавление таблицы, откроется окно **Таблица алертов**. Выполните следующие действия:

a. В поле **Доступные столбцы** двойным щелчком мыши выберите свойства алертов, которые вы хотите добавить в таблицу отчета.

Выбранные свойства переместятся в поле **Выбранные столбцы**. Вы можете перетаскивать имена столбцов между полями **Доступные столбцы** и **Выбранные столбцы**, а также менять порядок столбцов таблицы отчета.

Например, если в поле **Выбранные столбцы** вы переместили свойства **Технологии, Обнаружено** и **Время создания**, в таблице созданного отчета отобразятся технологии, в результате проверки которыми были созданы алерты, список обнаруженных объектов и время создания алертов.

b. Если вы хотите отфильтровать алерты по свойству **Состояние**, установите флажки рядом с теми состояниями обработки алертов пользователем, данные по которым вы хотите отображать в отчете.

c. Если вы хотите отфильтровать алерты по свойству **Технологии**, установите флажки рядом с теми названиями модулей и компонентов приложения, данные по которым вы хотите отображать в отчете.

d. Если вы хотите отфильтровать алерты по свойству **Важность**, установите флажки рядом с теми степенями важности алертов, данные по которым вы хотите отображать в отчете.

e. Если вы хотите отфильтровать алерты по статусу **Статус VIP**, в списке выберите **VIP**. В отчете отобразятся только алерты со статусом VIP.

f. Нажмите на кнопку **Применить**.

10. Нажмите на кнопку **Сохранить** в правом верхнем углу окна.

Будет создан новый шаблон.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания шаблона отчета недоступна.

Создание отчета по шаблону

Чтобы создать отчет по шаблону:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

Откроется таблица отчетов.

2. Нажмите на кнопку **Добавить**.

Откроется окно **Новый отчет**.

3. Выполните следующие действия:

   a. В раскрывающемся списке **Шаблон** выберите один из шаблонов для создания отчета.

   b. В блоке параметров **Период** выберите один из следующих вариантов:

   - **Прошедший час**, если вы хотите, чтобы отчет содержал информацию о работе приложения за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы отчет содержал информацию о работе приложения за предыдущий день.
   - **Прошедшие 7 дней**, если вы хотите, чтобы отчет содержал информацию о работе приложения за предыдущую неделю.
   - **Прошедшие 30 дней**, если вы хотите, чтобы отчет содержал информацию о работе системы за предыдущий месяц.
   - **Пользовательские**, если вы хотите, чтобы отчет содержал информацию о работе системы за указанный вами период.

4. Если вы выбрали период отображения информации о работе приложения **Пользовательские**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода, за который будет создан отчет.

   b. Нажмите на кнопку **Применить**.

5. Если вы используете режим распределенного решения и мультитенантности, в блоке параметров **Серверы** установите флажки напротив тех тенантов и серверов, данные по которым вы хотите отображать в отчете.

6. Нажмите на кнопку **Создать**.

Созданный отчет отобразится в таблице отчетов. Вы можете загрузить отчет для просмотра на вашем компьютере.

Для пользователей с ролью **Сотрудник службы безопасности** функция создания шаблона отчета недоступна.

Просмотр отчета

Чтобы просмотреть отчет:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. Выберите отчет, который вы хотите просмотреть.

Отчет откроется в новой вкладке вашего браузера.

Скачивание отчета на локальный компьютер

Чтобы скачать отчет на ваш компьютер:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. В строке с отчетом, который вы хотите просмотреть, нажмите на значок .

   Отчет будет сохранен в формате HTML на ваш локальный компьютер в папку загрузки браузера.

   Для просмотра отчета вы можете использовать любое приложение для просмотра HTML-файлов (например, браузер).

Изменение шаблона

Чтобы изменить шаблон:

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.

2. Откроется таблица шаблонов. Выберите шаблон, который вы хотите изменить.

   Откроется окно изменения шаблона.

3. Вы можете изменить следующие параметры:

   - **Имя шаблона** – имя отчета, которое отобразится в таблице в разделе **Отчеты**, подразделе **Созданные отчеты** при создании всех отчетов по этому шаблону.
   - **Заголовок отчета** – имя отчета, которое отобразится в отчете после создания отчета.

     Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.
   - **Описание отчета** – описание отчета, которое отобразится в отчете после создания отчета.

     Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.
   - **Изображение**. Вы можете загрузить или удалить изображение.
   - **Диаграмма**. Вы можете изменить следующие параметры диаграммы:
     - **Имя**.
     - **Источник данных**.
     - **Количество секторов**.

     Нажмите на кнопку **Применить**.

- **Таблица**. Вы можете изменить следующие параметры таблицы:
  - **Выбранные столбцы**. Вы можете перетаскивать имена столбцов между полями **Доступные столбцы** и **Выбранные столбцы**, а также менять порядок столбцов таблицы отчета.
  - **Состояние**.
  - **Технологии**.
  - **Важность**.
  - **Статус VIP**.

4. Выберите один из следующих способов сохранения шаблона:
   - Если вы хотите применить изменения к текущему шаблону, нажмите на кнопку **Сохранить**.

     Шаблон будет изменен.
   - Если вы хотите создать новый шаблон, введите имя шаблона и нажмите на кнопку **Сохранить как**.

     Имя нового шаблона не должно совпадать с именем уже существующего шаблона.

     Новый шаблон будет сохранен.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения шаблона недоступна.

Фильтрация шаблонов по имени

Чтобы отфильтровать шаблоны по имени:

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. По ссылке **Имя отчета** откройте меню фильтрации шаблонов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации шаблонов:
   - **Содержит**.
   - **Не содержит**.
4. Введите один или несколько символов имени шаблона.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку + под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Фильтрация шаблонов по имени пользователя, создавшего шаблон

Чтобы отфильтровать шаблоны по имени пользователя, создавшего шаблон:

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. По ссылке **Автор** откройте меню фильтрации шаблонов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации шаблонов:
   - **Содержит**.
   - **Не содержит**.
4. Введите один или несколько символов имени пользователя.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку + под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Фильтрация шаблонов по времени создания

Чтобы отфильтровать шаблоны отчетов по времени создания:

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. По ссылке **Время создания** откройте меню фильтрации шаблонов.
3. Выберите один из следующих периодов отображения шаблонов:
   - **Все**, если вы хотите, чтобы приложение отображало в таблице все созданные шаблоны.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице шаблоны, созданные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице шаблоны, созданные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице шаблоны, созданные за указанный вами период.

4. Если вы выбрали период отображения шаблонов **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения шаблонов.

   b. Нажмите на кнопку **Применить**.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Сброс фильтра шаблонов

Чтобы сбросить фильтр шаблонов по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. Нажмите на кнопку справа от того заголовка столбца таблицы шаблонов, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Удаление шаблона

Чтобы удалить шаблон:

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. Установите флажок в строке с шаблоном, который вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Выбранный вами шаблон будет удален.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления шаблона недоступна.

Фильтрация отчетов по времени создания

Чтобы отфильтровать отчеты по времени их создания:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. По ссылке **Время создания** откройте меню фильтрации отчетов.

3. Выберите один из следующих периодов отображения отчетов:

   - **Все**, если вы хотите, чтобы приложение отображало в таблице все созданные отчеты.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице отчеты, созданные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице отчеты, созданные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице отчеты, созданные за указанный вами период.

4. Если вы выбрали период отображения отчетов **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения отчетов.

   b. Нажмите на кнопку **Применить**.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени

Чтобы отфильтровать отчеты по имени:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. По ссылке **Имя отчета** откройте меню фильтрации отчетов.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации отчетов:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов имени отчета.

5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку + под списком операторов фильтрации и повторите действия по вводу условий фильтрации.

6. Нажмите на кнопку **Применить**.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени сервера с компонентом Central Node

Чтобы отфильтровать отчеты по имени сервера с компонентом Central Node:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. По ссылке **Серверы** откройте меню фильтрации отчетов.

3. Установите флажки напротив тех серверов, по которым вы хотите отфильтровать отчеты.

4. Нажмите на кнопку **Применить**.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени пользователя, создавшего отчет

Чтобы отфильтровать отчеты по имени пользователя, создавшего отчет:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. По ссылке **Автор** откройте меню фильтрации отчетов.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации отчетов:

   - **Содержит**.
   - **Не содержит**.

4. Введите один или несколько символов имени пользователя.

5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку + под списком операторов фильтрации и повторите действия по вводу условий фильтрации.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Сброс фильтра отчетов

Чтобы сбросить фильтр отчетов по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. Нажмите на кнопку справа от того заголовка столбца таблицы отчетов, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Удаление отчета

Чтобы удалить отчет о работе приложения:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. Установите флажок в строке с отчетом, который вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранный отчет будет удален.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления отчета недоступна.

Работа с отчетами NDR

С помощью Kaspersky Anti Targeted Attack Platform вы можете получать отчеты с различными сведениями, сохраненными приложением. Kaspersky Anti Targeted Attack Platform формирует отчеты в виде файлов в формате PDF. Приложение может отправлять файлы с отчетами на адреса электронной почты.

Вы можете просматривать информацию о сформированных отчетах и экспортировать их в файлы в разделе **Отчеты**, подразделе **Отчеты (NDR)** на вкладке **Созданные отчеты**.

Шаблоны отчетов NDR могут быть следующих типов:

- Системные шаблоны – создаются автоматически при установке приложения. В таблице шаблонов отчетов системные шаблоны отображаются со значком . Вы не можете удалять системные шаблоны.

  Kaspersky Anti Targeted Attack Platform поддерживает следующие системные шаблоны для формирования отчетов:

  - Отчет об активах (Inventory report).

    Содержит информацию об устройствах и системных командах, а также используемых протоколах и обнаруженных рисках на устройствах.

  - Отчет о безопасности системы (System security report).

    Содержит информацию о состоянии безопасности устройств, зарегистрированных событиях, обнаруженных рисках и взаимодействиях с устройствами внешних сетей.

  - Краткий отчет (Executive summary).

    Содержит краткую информацию об устройствах и состоянии безопасности системы.

  - Полный отчет (Full report).

    Содержит полную информацию об устройствах и состоянии безопасности системы.

- Пользовательские шаблоны – создаются вручную путем дублирования шаблонов. Дублировать можно как системные, так и пользовательские шаблоны. Дублировать шаблоны могут только пользователи с ролью Старший сотрудник службы безопасности.

Данные в отчетах представлены в виде отдельных информационных блоков. Для каждого отчета Kaspersky Anti Targeted Attack Platform используется фиксированный набор и порядок расположения информационных блоков. Информационные блоки, которые используются в отчетах, и их описания приведены в таблице ниже.

Использование информационных блоков в отчетах

Название информационного блока	Отчет об активах	Отчет о безопасности системы	Краткий отчет	Полный отчет
Категории устройств	✓	–	✓	✓
Производители устройств	✓	–	✓	✓
Операционные системы на устройствах	✓	–	✓	✓
Устройства с наибольшим количеством рисков	✓	✓	–	✓
Ситуационная осведомленность	–	✓	✓	✓
Новые устройства в сети	✓	–	–	✓
Протоколы с наибольшим объемом трафика	✓	–	–	✓
Устройства с наибольшим количеством соединений с другими узлами	✓	–	–	✓
Объем сетевого трафика	✓	–	✓	✓
Протоколы общего применения	✓	–	✓	✓
Состояния безопасности устройств	–	✓	✓	✓

Название информационного блока	Отчет об активах	Отчет о безопасности системы	Краткий отчет	Полный отчет
Распределение устройств по статусам	—	✓	—	✓
Статистика по событиям	—	✓	—	✓
Распределение событий по технологиям обнаружения	—	✓	—	✓
Устройства с наибольшим количеством событий	—	✓	—	✓
Самые критичные события	—	✓	—	✓
Наиболее частые срабатывания правил обнаружения вредоносной активности	—	✓	—	✓
Устройства с признаками доступа к публичным ресурсам	—	✓	—	✓
Подключения по протоколам удаленного управления	—	✓	—	✓
Актуальные риски	—	✓	✓	✓

Просмотр таблицы шаблонов отчетов NDR

Вы можете просмотреть таблицу шаблонов отчетов в разделе **Отчеты**, подразделе **Отчеты (NDR)** на вкладке **Шаблоны отчетов** веб-интерфейса приложения.

Параметры шаблонов отчетов отображаются в следующих столбцах таблицы:

- **Имя**.

  Название шаблона отчета. Рядом с названиями системных шаблонов отчетов отображается значок .

- **Расписание**.

  Информация о расписании, по которому Kaspersky Anti Targeted Attack Platform автоматически запускает формирование отчета по шаблону. Информация о расписании отображается, если пользователь с ролью **Старший сотрудник службы безопасности** настроил параметры расписания в шаблоне отчета. Если параметры расписания не заданы, в столбце отображается значение **Выключено**.

- **Тип/пользователь**.

  Имя пользователя, внесшего последние изменения в шаблон отчета. Для системных шаблонов с параметрами по умолчанию отображается значение **Системный**.

- **Последний отчет**.

  Дата и время последнего запуска формирования отчета по шаблону отчета.

- **Получатели**.

  Значок, соответствующий наличию получателей отчетов по электронной почте. Предусмотрены следующие значки:

  - – получатели отчетов заданы.
  - – получатели отчетов не заданы.

Просмотр сведений о шаблоне отчета NDR

Чтобы просмотреть сведения о шаблоне отчета,

в разделе **Отчеты**, подразделе **Отчеты (NDR)** на вкладке **Шаблоны отчетов** выберите нужный шаблон.

В правой части окна веб-интерфейса появится область деталей. В области деталей отображаются все сведения, для которых заданы значения.

Подробные сведения о шаблоне отчета включают следующие поля:

- **Имя** – название шаблона отчета.
- **Тип/пользователь** – имя пользователя, внесшего последние изменения в шаблон отчета. Для системных шаблонов с параметрами по умолчанию отображается значение **Системный**.
- **Период** – период времени, за который Kaspersky Anti Targeted Attack Platform формирует отчет по шаблону.
- **Изменен** – время последнего изменения шаблона.
- **Последний отчет** – время последнего запуска формирования отчета по шаблону.
- **Следующий запуск (локальное время)** – время следующего запуска формирования отчета по шаблону. Этот параметр отображается, если для шаблона отчета заданы параметры расписания.
- **Расписание** – информация о расписании, по которому Kaspersky Anti Targeted Attack Platform автоматически запускает формирование отчета по шаблону. Этот параметр отображается, если для шаблона отчета заданы параметры расписания.

Адреса получателей – адреса электронной почту, на которые Kaspersky Anti Targeted Attack Platform отправляет сформированные отчеты. Этот параметр отображается, если для шаблона отчета заданы адреса получателей.

Просмотр таблицы отчетов NDR

Вы можете просмотреть таблицу отчетов в разделе **Отчеты**, подразделе **Отчеты (NDR)** на вкладке **Созданные отчеты** веб-интерфейса приложения.

Параметры отчетов отображаются в следующих столбцах таблицы:

- **ID**.

  Уникальный идентификатор отчета.

- **Имя отчета**.

  Название сформированного отчета.

- **Имя шаблона**.

  Название шаблона, по которому был сформирован отчет.

- **Запуск**.

  Дата и время запуска формирования отчета.

- **Статус**.

  Статус выполнения отчета. Предусмотрены следующие статусы выполнения отчета:

  Ожидание. Отчет находится в очереди на формирование. Отчет может иметь статус *В ожидании* при формировании нескольких отчетов одновременно.

  Формируется. Отчет находится в процессе формирования.

  Ошибка. При формировании отчета произошла ошибка.

  Готово. Формирование отчета завершено.

  Отменяется. Формирование отчета находится в процессе отмены.

  Отменено. Формирование отчета было отменено.

- **Пользователь**.

  Имя пользователя, запустившего формирование отчета или настроившего расписание запуска отчета по шаблону.

- **Тип запуска**.

  Тип запуска формирования отчета: вручную или по расписанию.

- **Завершен**.

  Дата и время завершения формирования отчета.

Формирование отчета NDR по шаблону вручную

Вы можете запустить формирование отчета по шаблону вручную.

Чтобы запустить формирование отчета:

1. Выберите раздел **Отчеты**, затем подраздел **Отчеты (NDR)**.

2. На вкладке **Шаблоны отчетов** выберите один или несколько шаблонов, по которым вы хотите сформировать отчеты.

   При выборе нескольких шаблонов приложение формирует по ним отчеты одновременно. Вы можете выбрать не более 10 шаблонов.

3. В панели инструментов, которая расположена над таблицей шаблонов отчетов, нажмите на кнопку **Получить отчеты**.

   Kaspersky Anti Targeted Attack Platform запустит формирование отчета.

Вы перейдете на вкладку **Созданные отчеты**, на которой отобразится статус выполнения запущенных отчетов. После завершения формирования отчетов Kaspersky Anti Targeted Attack Platform отправит файлы с отчетами в формате PDF на адреса электронной почты, указанные в шаблоне отчета. Если адрес электронной почты не задан в шаблоне отчета, вы можете экспортировать сформированные отчеты в файлы по отдельности вручную на вкладке **Созданные отчеты**. Максимальный размер файла отчета – 10 МБ.

Если требуется, вы можете отменить формирование отчета.

Дублирование шаблона отчета NDR

Вы можете создавать пользовательские шаблоны путем дублирования существующих шаблонов отчетов. Вы можете дублировать как системные, так и пользовательские шаблоны. При дублировании шаблона вы не можете изменять состав и расположение информационных блоков в отчете.

Максимальное количество шаблонов в приложении – 5000.

Чтобы дублировать шаблон отчета:

1. Выберите раздел **Отчеты**, затем подраздел **Отчеты (NDR)**.
2. На вкладке **Шаблоны отчетов** выберите нужный шаблон.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Создать новый шаблон**.
4. В поле **Имя** измените название шаблона отчета.

   Вы можете использовать буквы русского и латинского алфавитов, цифры, пробел, а также символы -, – и _.

   Название шаблона отчета должно удовлетворять следующим требованиям:

   - не совпадает с названием другого шаблона отчета (регистр символов не учитывается);
   - содержит до 100 символов.

   Названия отчетов, сформированные по обновленному шаблону, будут соответствовать новому названию шаблона.
5. В раскрывающемся списке **Период для данных** выберите период времени, за который вы хотите получить информацию о системе в отчете.

   Вы можете формировать отчеты с информацией, поступившей в приложение, за последние 24 часа, 7 дней, 30 дней, за последний год или задать период вручную.
6. Если требуется запускать формирование отчетов по расписанию, включите переключатель **Формирование отчета по расписанию** и настройте параметры расписания:

   a. В раскрывающемся списке **Периодичность** выберите, как часто требуется выполнять формирование отчета: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.

   b. В зависимости от выбранного варианта задайте значения параметров, чтобы уточнить время запуска формирования отчета.
7. Если требуется, в поле **Адреса получателей** введите адрес электронной почты, на которую вы хотите отправлять сформированные отчеты. Если требуется указать дополнительных получателей отчета, нажмите на кнопку **Добавить адрес получателя** и введите адрес электронной почты.

   Максимальное количество получателей отчета – 20.
8. Нажмите на кнопку **Сохранить**.

В таблице шаблонов отчетов отобразится новый шаблон отчета.

Изменение шаблона отчета NDR

Чтобы изменить параметры шаблона отчета:

1. Выберите раздел **Отчеты**, затем подраздел **Отчеты (NDR)**.
2. На вкладке **Шаблоны отчетов** выберите нужный шаблон.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.
4. В поле **Имя** измените название шаблона отчета.

   Вы можете использовать буквы русского и латинского алфавитов, цифры, пробел, а также символы -, – и _.

   Название шаблона отчета должно удовлетворять следующим требованиям:

   - не совпадает с названием другого шаблона отчета (регистр символов не учитывается);
   - содержит до 100 символов.

   Названия отчетов, сформированные по обновленному шаблону, будут соответствовать новому названию шаблона.
5. В раскрывающемся списке **Период для данных** выберите период времени, за который вы хотите получить информацию о системе в отчете.

   Вы можете формировать отчеты с информацией, поступившей в приложение, за последние 24 часа, 7 дней, 30 дней, за последний год или задать период вручную.
6. Если требуется запускать формирование отчетов по расписанию, включите переключатель **Формирование отчета по расписанию** и настройте параметры расписания:

   a. В раскрывающемся списке **Периодичность** выберите, как часто требуется выполнять формирование отчета: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.

   b. В зависимости от выбранного варианта задайте значения параметров, чтобы уточнить время запуска формирования отчета.
7. Если требуется, в поле **Адреса получателей** введите адрес электронной почты, на которую вы хотите отправлять сформированные отчеты. Если требуется указать дополнительных получателей отчета, нажмите на кнопку **Добавить адрес получателя** и введите адрес электронной почты.

   Максимальное количество получателей отчета – 20.
8. Нажмите на кнопку **Сохранить**.

Изменения отобразятся в соответствующих столбцах таблицы шаблонов отчетов.

Экспорт отчета NDR в файл

Вы можете экспортировать сформированный отчет в файл в формате PDF.

Чтобы экспортировать отчет в файл:

1. В разделе **Отчеты** выберите подраздел **Отчеты (NDR)**.
2. На вкладке **Созданные отчеты** выберите нужный отчет.

   Отчеты отфильтрованы по идентификаторам отчетов, запущенных последними в текущем сеансе подключения к Серверу. Для отображения всех сформированных отчетов сбросьте параметры фильтрации с помощью кнопки **Фильтр по умолчанию**. Если требуется, вы можете настроить фильтрацию по нужному периоду времени.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Экспорт**.

Браузер сохранит файл отчета. По умолчанию файл отчета имеет название в формате `<название отчета>_<дата и время формирования отчета>`. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Удаление шаблона отчета NDR

Вы можете удалять только пользовательские шаблоны отчетов.

Чтобы удалить шаблон отчета:

1. Выберите раздел **Отчеты**, затем подраздел **Отчеты (NDR)**.
2. На вкладке **Шаблоны отчетов** выберите один или несколько шаблонов отчетов, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Вы не можете удалить системные шаблоны отчетов. В таблице шаблонов отчетов системные шаблоны отображаются со значком .
4. В открывшемся окне запроса подтвердите удаление шаблонов отчетов.

Удаление отчета NDR

Чтобы удалить отчет:

1. Выберите раздел **Отчеты**, затем подраздел **Отчеты (NDR)**.
2. На вкладке **Созданные отчеты** выберите один или несколько отчетов, которые вы хотите удалить.

   Отчеты в таблице отчетов отфильтрованы по идентификаторам отчетов, запущенных последними в текущем сеансе подключения к Серверу. Для отображения всех сформированных отчетов сбросьте параметры фильтрации с помощью кнопки **Фильтр по умолчанию**. Если требуется, вы можете настроить фильтрацию по нужному периоду времени.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне запроса подтвердите удаление отчета.

Отмена формирования отчета NDR

Вы можете отменить формирование отчета только со статусом **Формируется**.

Чтобы отменить формирование отчета:

1. Выберите раздел **Отчеты**, затем подраздел **Отчеты (NDR)**.
2. На вкладке **Созданные отчеты** выберите отчет со статусом **Формируется**, формирование которого вы хотите отменить.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Отменить**.
4. В открывшемся окне запроса подтвердите отмену формирования отчета.

После выполнения запроса статус отчета изменится на **Отменено**.

Управление параметрами хранения файлов отчетов

Вы можете изменить ограничения максимального объема для хранения файлов отчетов.

Чтобы изменить параметры хранения файлов отчетов:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Серверы Sensor**.
3. Выберите карточку локального хоста (его IP-адрес 0.0.0.0).

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для изменения параметров сервера.
5. На вкладке **Общие** перейдите к блоку параметров **Отчеты** и задайте ограничение занимаемого объема для хранения файлов отчетов с помощью параметра **Макс. объем**.

   Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

   При изменении значения параметра вам нужно учитывать, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для узла.
6. При необходимости с помощью параметра **Время хранения (дней)** включите ограничение на минимальное время хранения файлов отчетов и укажите нужное количество дней для хранения.
7. Нажмите на кнопку **Сохранить**.

Работа с правилами присвоения алертам статуса VIP

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, удалять, изменять, импортировать и экспортировать список правил присвоения алертам статуса VIP.

Вы можете создавать правила одного из следующих типов:

- **IP**. Новым алертам, связанным с этим IP-адресом компьютера, будет присвоен статус VIP.
- **Имя хоста**. Новым алертам, связанным с этим именем хоста, будет присвоен статус VIP.
- **Адрес**. Новым алертам, связанным с этим адресом электронной почты, будет присвоен статус VIP.

Пользователи с ролью **Аудитор** могут просматривать и экспортировать список правил присвоения алертам статуса VIP.

Пользователям с ролью **Сотрудник службы безопасности** просмотр списка правил присвоения алертам статуса VIP недоступен.

Просмотр таблицы правил присвоения статуса VIP

Таблица правил присвоения статуса VIP находится в разделе **Параметры**, подразделе **Статус VIP** веб-интерфейса приложения.

В таблице содержится следующая информация:

- **Критерий** – критерий добавления записи в список правил.
- **Значение** – значение критерия.
- **Описание** – дополнительная информация, указанная при создании правила.

Создание правила присвоения статуса VIP

Чтобы добавить правило присвоения алерту статуса VIP:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. В правом верхнем углу окна веб-интерфейса приложения нажмите на кнопку **Добавить**.

   Откроется окно добавления правила.

3. В раскрывающемся списке **Критерий** выберите один из следующих типов правила:

   - **IP**, если вы хотите добавить правило для IP-адреса компьютера.
   - **Хост**, если вы хотите добавить правило для имени хоста.
   - **Адрес**, если вы хотите добавить правило для адреса электронной почты.

4. В поле **Значение** введите нужное значение.

   Например, если в списке **Критерий** вы выбрали **Адрес**, в поле **Значение** введите адрес электронной почты, для которого вы хотите добавить правило.

5. В поле **Описание** введите дополнительную информацию, если необходимо.

6. Нажмите на кнопку **Добавить**.

Правило будет добавлено. Новым алертам, связанным с добавленным IP-адресом, именем хоста или адресом электронной почты, будет присвоен статус VIP.

Для пользователей с ролью **Аудитор** функция создания правил для присвоения алертам статуса VIP недоступна.

Пользователям с ролью **Сотрудник службы безопасности** просмотр списка правил присвоения алертам статуса VIP недоступен.

Удаление правила присвоения статуса VIP

Чтобы удалить правило присвоения алертам статуса VIP:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.

2. Установите флажок слева от каждого правила, которое вы хотите удалить из списка.

3. Если вы хотите удалить все правила, установите флажок над списком.

4. В правом верхнем углу окна веб-интерфейса приложения нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения действия.

5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Для пользователей с ролью **Аудитор** функция удаления правил для присвоения алертам статуса VIP недоступна.

Пользователям с ролью **Сотрудник службы безопасности** просмотр списка правил присвоения алертам статуса VIP недоступен.

Изменение правила присвоения статуса VIP

Чтобы изменить правило присвоения алертам статуса VIP:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Выберите правило, которое вы хотите изменить.

   Откроется окно изменения правила.

3. Внесите необходимые изменения в поля **Критерий**, **Значение**, **Описание**.
4. Нажмите на кнопку **Сохранить**.

Правило будет изменено.

Для пользователей с ролью **Аудитор** функция изменения правил для присвоения алертам статуса VIP недоступна.

Пользователям с ролью **Сотрудник службы безопасности** просмотр списка правил присвоения алертам статуса VIP недоступен.

Импорт списка правил присвоения статуса VIP

Чтобы импортировать список правил присвоения алертам статуса VIP:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Нажмите на кнопку **Импортировать**.

   Отобразится подтверждение импорта списка.

Импортированный список правил присвоения алертам статуса VIP заменит текущий список правил присвоения алертам статуса VIP.

3. Нажмите на кнопку **Да**.

   Откроется окно выбора файлов.

4. Выберите файл формата JSON со списком правил, которые вы хотите импортировать, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Список будет импортирован.

Экспорт списка данных, исключенных из проверки

Чтобы экспортировать список исключений из проверки:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. В правом верхнем углу окна веб-интерфейса приложения нажмите на кнопку **Экспортировать**.

Файл в формате JSON с экспортированным списком исключений из проверки будет сохранен в папку загрузки браузера на вашем компьютере.

Фильтрация и поиск по типу правила присвоения статуса VIP

Чтобы отфильтровать или найти правила присвоения алертам статуса VIP по типу правила:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Критерий** откройте окно настройки фильтрации.
3. Установите один или несколько флажков рядом с типами правил:
   - **IP**.
   - **Хост**.
   - **Адрес**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск по значению правила присвоения статуса VIP

Чтобы отфильтровать или найти правила присвоения алертам статуса VIP по значению правила:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Значение** откройте окно настройки фильтрации.
3. Введите один или несколько символов значения правила.
4. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

   В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск по описанию правила присвоения статуса VIP

Чтобы отфильтровать или найти правила присвоения алертам статуса VIP по описанию:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Описание** откройте окно настройки фильтрации.
3. Введите один или несколько символов описания.
4. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

   В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил присвоения статуса VIP

Чтобы сбросить фильтр правил присвоения алертам статуса VIP по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Нажмите на кнопку справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Работа с разрешающими правилами для событий NDR

Kaspersky Anti Targeted Attack Platform может отслеживать сетевые взаимодействия устройств. Для определения разрешенных и неразрешенных сетевых взаимодействий используются *разрешающие правила*. Все сетевые взаимодействия, удовлетворяющие действующим разрешающим правилам, считаются разрешенными. При обнаружении разрешенных взаимодействий приложение не регистрирует события NDR и не создает алерты.

Вы можете просматривать, создавать, копировать, изменять, удалять, включать и отключать разрешающие правила.

Просмотр таблицы разрешающих правил

Чтобы просмотреть таблицу разрешающих правил:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**.
2. Перейдите на вкладку **Разрешающие правила**.

   Отобразится таблица разрешающих правил.

В таблице содержится следующая информация:

- **ID правила** – уникальный идентификатор правила.
- **Статус** (значок ◐) – текущий статус правила (*Включено* или *Выключено*).
- **Тип правила** – для правил, выключающих регистрацию событий, указан тип EVT.

- **Протоколы/Команды** – набор используемых протоколов.
- **Сторона 1** – имя устройства / адресная информация одной из сторон сетевого взаимодействия. Отображение адресов и портов адресной информации можно включать и выключать с помощью следующих параметров: **MAC-адрес**, **IP-адрес**, **Номер порта**. Если в приложение добавлены дополнительные адресные пространства, можно включать и выключать отображение имен адресных пространств с помощью следующих параметров:
  - **АП для MAC-адресов** – адресные пространства, к которым относятся MAC-адреса в правиле. Параметр может содержать имена только тех АП, в которых есть правила адресных пространств с выбранным уровнем модели OSI **Канальный (L2)**.
  - **АП для IP-адресов** – адресные пространства, к которым относятся IP-адреса в правиле. Параметр может содержать имена только тех АП, в которых есть правила адресных пространств с выбранным уровнем модели OSI **Сетевой (L3)**.
- **Сторона 2** – имя устройства / адресная информация другой стороны сетевого взаимодействия. Отображение адресной информации можно настраивать аналогично, как для столбца **Сторона 1**.
- **Комментарий** – дополнительная информация о правиле.
- **Создано** – дата и время создания правила.
- **Изменено** – дата и время последнего изменения правила.
- **Точка мониторинга** – имя точки мониторинга, которое должно быть указано в событии.
- **Тип события** – идентификатор и заголовок типа события.
- **Источник** – сведения об источнике правила.
- **SID системного правила IDS** – идентификатор системного правила IDS. Если при создании разрешающего правила идентификатор не был указан, отображается значение *Все правила*.

Создание разрешающего правила с изначально пустыми значениями или со значениями из шаблона

Чтобы создать разрешающее правило с изначально пустыми значениями или со значениями из шаблона:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**.
2. Перейдите на вкладку **Разрешающие правила**.
3. Нажмите на кнопку **Добавить правило**.
4. Если вы хотите задать значения параметров из шаблона, в области деталей нажмите на кнопку **Использовать шаблон**, в открывшемся окне выберите нужный шаблон и нажмите на кнопку **Применить**.
5. В поле **Протокол** укажите протокол для взаимодействия устройств.

   При выборе поля **Протокол** откроется окно с таблицей поддерживаемых протоколов, отображаемых в виде дерева стека протоколов. Вы можете управлять отображением элементов дерева с помощью кнопок **+** и **-** рядом с названиями протоколов, которые содержат протоколы следующих уровней.

   При необходимости воспользуйтесь поисковой строкой над таблицей, чтобы найти нужные протоколы.

Чтобы указать протокол, выполните следующие действия:

a. В таблице протоколов выберите протокол, который вы хотите указать для правила. Для выбора нужного протокола нажмите на кнопку, которая отображается в левом столбце таблицы протоколов.

b. Нажмите на кнопку **OK**.

Если выбран протокол, который приложение может определять по содержимому сетевых пакетов, под полем **Протокол** появится соответствующее предупреждение.

6. При необходимости введите дополнительную информацию о правиле в поле **Комментарий**.

7. В блоках параметров **Сторона 1** и **Сторона 2** укажите доступную для изменения адресную информацию для сторон сетевого взаимодействия. В зависимости от выбранного протокола (или набора протоколов), адресная информация может содержать MAC-адрес, IP-адрес и/или номер порта. Если в приложение добавлены дополнительные адресные пространства, вы можете указать имена адресных пространств для адресов.

   Для автоматического заполнения адресной информации стороны сетевого взаимодействия вы можете выбрать известные приложению устройства. Для этого выполните следующие действия:

   a. Откройте окно выбора устройств по ссылке **Указать адреса устройств**.

   b. В окне выбора устройств установите флажки напротив тех устройств, которые вы хотите использовать.

      Окно выбора устройств содержит таблицу, в которой можно настраивать отображение и порядок столбцов, выполнять фильтрацию, поиск и сортировку аналогично таблице устройств в разделе **Активы**.

   c. В окне выбора устройств нажмите на кнопку **OK**.

8. В поле **Тип события** укажите тип события, числовой код которого указывается в событиях.

   При выборе поля **Тип события** откроется окно со списком типов событий, которые могут быть указаны в разрешающих правилах. При необходимости воспользуйтесь поисковой строкой над списком, чтобы найти нужный тип события. Чтобы указать тип события, выберите его в списке и нажмите на кнопку **Применить**.

9. В поле **Точка мониторинга** укажите имя точки мониторинга, которое указывается в событиях.

   При выборе поля **Точка мониторинга** откроется окно со списком всех точек мониторинга на всех узлах с установленными компонентами приложения. При необходимости воспользуйтесь поисковой строкой над списком, чтобы найти имя нужной точки мониторинга. Чтобы указать имя точки мониторинга, выберите его в списке и нажмите на кнопку **Применить**.

10. Если вы хотите, чтобы приложение не проверяло сетевые соединения, подпадающие под условия этого разрешающего правила, по выбранному системному правилу IDS, укажите идентификатор этого правила в поле **SID системного правила IDS**. Вы можете посмотреть SID системного правила IDS в деталях IDS-алерта.

    Если SID не указан, приложение отключает проверку по всем системным правилам IDS для сетевых взаимодействий, подпадающих под условия этого разрешающего правила.

11. В области деталей нажмите на кнопку **Сохранить**.

Правило будет добавлено в таблицу разрешающих правил.

Создание разрешающего правила на основе зарегистрированного события

Чтобы создать разрешающее правило на основе зарегистрированного события:

1. В разделе **События в трафике сети** в таблице событий в таблице зарегистрированных событий выберите событие, на основе которого вы хотите создать разрешающее правило для событий.

2. В области деталей нажмите на кнопку **Создать разрешающее правило**.

   В окне браузера откроется раздел **Разрешающие правила**. В правой части окна веб-интерфейса появится область деталей в режиме изменения параметров правила. Для параметров нового правила будут заданы значения, полученные из сохраненных сведений о событии.

3. При необходимости измените параметры нового правила. Для этого выполните пункты 4–12, описанные в процедуре создания правила с изначально пустыми значениями параметров. Если изменять параметры нового правила не требуется, сохраните правило с помощью кнопки **Сохранить**.

Разрешающее правило на основе зарегистрированного события будет создано.

Копирование разрешающего правила

Чтобы создать правило контроля взаимодействия на основе имеющегося правила:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**.

2. Перейдите на вкладку **Разрешающие правила**.

3. Выберите правило, на основе которого вы хотите создать новое правило.

4. По правой кнопке мыши откройте контекстное меню.

5. В контекстном меню выберите пункт **Копировать правило**.

   В правой части окна веб-интерфейса появится область деталей в режиме изменения параметров правила. Для параметров нового правила будут заданы значения, полученные из параметров выбранного правила.

6. Измените нужные параметры. Для этого выполните пункты 4–12, описанные в процедуре создания правила.

Разрешающее правило будет скопировано.

Изменение параметров разрешающего правила

Вы можете изменять параметры включенного разрешающего правила. Для выключенных правил возможность изменения недоступна.

Чтобы изменить параметры разрешающего правила:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**.
2. Перейдите на вкладку **Разрешающие правила**.
3. Выберите правило, параметры которого хотите изменить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. Измените нужные параметры. Для этого выполните пункты 4–12, описанные в процедуре создания правила.
6. Нажмите на кнопку **Сохранить**.

Параметры правила будут изменены.

Включение и выключение разрешающих правил

Разрешающим правилам могут быть присвоены статусы *Включено* или *Выключено*. По умолчанию после создания правила включены.

Чтобы изменить статус разрешающих правил:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**.
2. Перейдите на вкладку **Разрешающие правила**.
3. В таблице правил выберите правила, для которых вы хотите изменить статус.
4. Включите или выключите правила с помощью кнопок **Включить** и **Выключить**. Каждая из этих кнопок отображается, если среди выбранных правил есть правила, с которыми можно выполнить соответствующую операцию.

Статус выбранных правил будет изменен.

Удаление разрешающих правил

Вы можете выборочно удалить одно или несколько разрешающих правил.

Чтобы удалить разрешающие правила:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**.
2. Перейдите на вкладку **Разрешающие правила**.
3. В таблице правил выберите разрешающие правила, которые вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

Откроется окно с запросом подтверждения. В зависимости от состояния выбранных правил, в запросе будут предложены следующие варианты действий:

- Если все выбранные правила включены, приложение предлагает удалить выбранные правила, выключить их или отменить операцию. Это условие не проверяется, если выбраны все правила, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных правил более 1000.

- Если среди выбранных правил присутствуют выключенные правила или выбраны все правила, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных правил более 1000, приложение предлагает удалить выбранные правила или отменить операцию.

5. В окне запроса подтвердите удаление правил.

Выбранные правила будут удалены.

Работа со списком исключений из проверки

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, импортировать и экспортировать список *исключений из проверки* – список данных, которые Kaspersky Anti Targeted Attack Platform будет считать безопасными и не будет отображать в таблице алертов. Вы можете создать правила исключений из проверки для следующих данных:

- **MD5**.
- **Формат**.
- **Маска URL**.
- **Адрес получателя**.
- **Адрес отправителя**.
- **IP или подсеть источника**.
- **IP или подсеть назначения**.
- **Агент пользователя**.

Пользователи с ролью **Аудитор** и **Сотрудник службы безопасности** могут просматривать список правил исключений из проверки, а также экспортировать его.

Просмотр таблицы данных, исключенных из проверки

Чтобы просмотреть таблицу с данными, исключенными из проверки:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **Проверка**.

   Отобразится таблица со списком данных, которые Kaspersky Anti Targeted Attack Platform будет считать безопасными и не будет создавать для них алерты. Вы можете фильтровать правила по ссылкам в названии столбцов.

В таблице содержится следующая информация:

- **Критерий** – критерий добавления записи в список разрешенных объектов.
- **Значение** – значение критерия.

Добавление правила исключения из проверки

Чтобы добавить правило исключения из проверки:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. В правом верхнем углу окна веб-интерфейса приложения нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
4. В раскрывающемся списке **Критерий** выберите один из следующих критериев добавления правила в список исключений из проверки:
   - **MD5**.
   - **Формат**.
   - **Маска URL**.
   - **Адрес получателя**.
   - **Адрес отправителя**.
   - **IP или подсеть источника**.
   - **IP или подсеть назначения**.
   - **Агент пользователя**.

5. Если вы выбрали **Формат**, в раскрывающемся списке **Значение** выберите формат файла, который вы хотите добавить.

   Например, вы можете выбрать формат **MSOfficeDoc**.

6. Если вы выбрали **MD5**, **Маска URL**, **Адрес получателя**, **Адрес отправителя**, **IP или подсеть источника**, **IP или подсеть назначения** или **Агент пользователя**, в поле **Значение** введите значение соответствующего критерия, которое вы хотите добавить в список исключений из проверки:

   - Если вы выбрали **MD5**, в поле **Значение** введите MD5-хеш файла.
   - Если вы выбрали **Маска URL**, в поле **Значение** введите маску URL-адреса.

     При формировании маски вы можете использовать следующие специальные символы:

     * – любая последовательность символов.

     > Пример:
     > Если вы введете маску `*abc*`, приложение будет считать безопасным любой URL-адрес, содержащий последовательность `abc`. Например, `www.example.com/download_virusabc`

     ? – любой один символ.

     > Пример:
     > Если вы введете маску `example_123?.com`, приложение будет считать безопасным любой URL-адрес, содержащий заданную последовательность символов и любой символ, следующий за `3`. Например, `example_1234.com`

     В случае, если символы `*` и `?` входят в состав полного URL-адреса, добавляемого в исключения из проверки, при вводе этих символов нужно использовать `\` – отмена одного из следующих за ним символов `*` или `?`, `\`.

     > Пример:
     > В качестве доверенного адреса требуется добавить следующий URL-адрес: `www.example.com/download_virus/virus.dll?virus_name=`
     > Чтобы приложение не восприняло `?` как специальный символ формирования маски, нужно поставить перед `?` знак `\`.
     > URL-адрес, добавляемый в список исключений из проверки, будет выглядеть следующим образом:
     > `www.example.com/download_virus/virus.dll\?virus_name=`

   - Если вы выбрали **Адрес получателя** или **Адрес отправителя**, в поле **Значение** введите адрес электронной почты.
   - Если вы выбрали **Агент пользователя**, в поле **Значение** введите заголовок **User agent HTTP-запросов**, содержащий информацию о браузере.
   - Если вы выбрали **IP или подсеть источника** или **IP или подсеть назначения**, в поле **Значение** введите адрес или подсеть (например, 255.255.255.0).

   В полях **Маска URL**, **Адрес получателя**, **Адрес отправителя** вы можете указывать доменные имена, содержащие символы кириллицы. В этом случае указанный адрес будет преобразован в Punycode и обработан в соответствии с параметрами приложения.

7. Нажмите на кнопку **Добавить**.

Правило будет добавлено в список исключений из проверки.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция добавления правила исключения из проверки недоступна.

Удаление правила исключения из проверки

Чтобы удалить одно или несколько правил из списка исключений из проверки:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. Установите флажок слева от каждого правила, которое вы хотите удалить из списка исключений из проверки.

   Если вы хотите удалить все правила, установите флажок над списком.
4. В нижней части окна нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены из списка исключений из проверки.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления записи в списке исключений из проверки недоступна.

Изменение правила, добавленного в исключения из проверки

Чтобы изменить правило в списке исключений из проверки:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. Выберите правило, которое вы хотите изменить.

   Откроется окно **Изменить правило**.
4. Внесите необходимые изменения в поля **Критерий** и **Значение**.
5. Нажмите на кнопку **Сохранить**.

Правило будет изменено.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения правила в списке исключений из проверки недоступна.

Экспорт списка данных, исключенных из проверки

Чтобы экспортировать список исключений из проверки:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. В правом верхнем углу окна веб-интерфейса приложения нажмите на кнопку **Экспортировать**.

Файл в формате JSON с экспортированным списком исключений из проверки будет сохранен в папку загрузки браузера на вашем компьютере.

Фильтрация правил в списке исключений из проверки по критерию

Чтобы отфильтровать записи в списке исключений из проверки по типу правила:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. По ссылке **Критерий** откройте окно настройки фильтрации.
4. Установите один или несколько флажков рядом с критериями, по которым вы хотите отфильтровать правила:
   - **MD5**.
   - **Формат**.
   - **Маска URL**.
   - **Адрес получателя**.
   - **Адрес отправителя**.
   - **IP или подсеть источника**.
   - **IP или подсеть назначения**.
   - **Агент пользователя**.
5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В списке исключений из проверки отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Поиск правил в списке исключений из проверки по значению

Чтобы найти правила в списке исключений из проверки по значению:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. По ссылке **Значение** откройте окно настройки фильтрации.
4. Введите символы значения.
5. Нажмите на кнопку **Применить**.

В списке исключений из проверки отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил в списке исключений из проверки

Чтобы сбросить фильтр записей в списке исключений по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. Нажмите на кнопку справа от того заголовка столбца таблицы записей в списке исключений из проверки, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В списке исключений из проверки отобразятся только правила, соответствующие заданным вами условиям.

Работа с исключениями из правил обнаружения вторжений

Пользователи с ролью **Старший сотрудник службы безопасности** могут добавлять правила обнаружения вторжений "Лаборатории Касперского" в исключения из проверки. Kaspersky Anti Targeted Attack Platform не будет создавать алерты при проверке по правилам обнаружения вторжений, добавленным в исключения. При этом приложение продолжает регистрировать события NDR по технологии *Обнаружение вторжений* (IDS).

Если вы хотите создать точечное исключение, например, чтобы приложение не регистрировало события NDR и не создавало по ним алерты для выбранного адреса источника, вам нужно добавить разрешающее правило.

Вы можете добавить в исключения только правила обнаружения вторжений "Лаборатории Касперского". Если вы не хотите применять при проверке пользовательское правило обнаружения вторжений, вы можете отключить это правило или удалить его.

Пользователи с ролью Аудитор могут просматривать список правил обнаружения вторжений, добавленных в исключения, и свойства выбранного правила.

Пользователям с ролью Сотрудник службы безопасности список правил обнаружения вторжений, добавленных в исключения, недоступен.

Просмотр таблицы правил обнаружения вторжений, добавленных в исключения

Чтобы просмотреть таблицу правил обнаружения вторжений, добавленных в исключения:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **IDS**.

   Отобразится таблица правил IDS, добавленных в исключения. Вы можете фильтровать правила по ссылкам в названии столбцов.

В таблице содержится следующая информация:

- **Время создания** – дата и время добавления правила обнаружения вторжений в исключения.
- **Правило** – имя правила обнаружения вторжений.
- **ID правила** – идентификатор правила обнаружения вторжений (SID, или signature ID) в формате Suricata.
- **Описание** – описание правила обнаружения вторжений.
- **Автор** – имя пользователя, под учетной записью которого правило обнаружения вторжений было добавлено в исключения.

Добавление правила обнаружения вторжений в исключения

Вы можете добавлять правила обнаружения вторжений "Лаборатории Касперского", по которым созданы алерты средней и высокой степени важности, в исключения из проверки событий.

Вы можете добавить в исключения только правила обнаружения вторжений "Лаборатории Касперского". Если вы не хотите применять при проверке событий пользовательское правило обнаружения вторжений, вы можете отключить это правило или удалить его.

Чтобы добавить правило обнаружения вторжений в исключения:

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.

3. В раскрывающемся списке слева выберите **Содержит**.

4. В раскрывающемся списке справа выберите технологию **(IDS) Intrusion Detection System**.

5. Нажмите на кнопку **Применить**.

6. Если вы хотите отфильтровать обнаружения, по значку раскройте список параметров фильтрации и выберите нужный фильтр.

7. Выберите алерт, для которого в столбце **Обнаружено** отображается название нужного правила обнаружения вторжений.

   Откроется окно с информацией об алерте.

8. В правой части окна в блоке **Рекомендации** в разделе **Оценка** выберите **Добавить в исключения**.

   Откроется окно **Добавить правило IDS в исключения**.

9. В поле **Описание** введите описание правила обнаружения вторжений.

10. Нажмите на кнопку **Добавить**.

Правило обнаружения вторжений будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса приложения, подразделе **Исключения** на закладке **IDS**. Это правило не будет применяться при создании алертов.

Для пользователей с ролью **Аудитор** функция изменения записи в списке разрешенных объектов недоступна.

Пользователи с ролью **Сотрудник службы безопасности** не имеют доступа к списку правил обнаружения вторжений, добавленных в исключения.

Редактирование описания правила обнаружения вторжений, добавленного в исключения

*Чтобы отредактировать описание правила обнаружения вторжений, добавленного в исключения, из раздела **Алерты**:*

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.

3. В раскрывающемся списке слева выберите **Содержит**.

4. В раскрывающемся списке справа выберите технологию **(IDS) Intrusion Detection System**.

5. Нажмите на кнопку **Применить**.

6. Если вы хотите отфильтровать обнаружения, по значку раскройте список параметров фильтрации и выберите нужный фильтр.

7. Выберите алерт, для которого в столбце **Обнаружено** отображается название нужного правила обнаружения вторжений.

   Откроется окно с информацией об алерте.

8. В правой части окна в блоке **Рекомендации** в разделе **Оценка** выберите **Изменить исключение IDS**.

   Откроется окно **Изменить исключение IDS**.

   В поле **Описание** измените описание правила.

   Нажмите на кнопку **Сохранить**.

Описание правила обнаружения вторжений, добавленного в исключения, будет изменено. Это правило не будет применяться при создании алертов.

Для пользователей с ролью **Аудитор** функция редактирования описания правила обнаружения вторжений недоступна.

Пользователи с ролью **Сотрудник службы безопасности** не имеют доступа к списку правил обнаружения вторжений, добавленных в исключения.

Удаление правил обнаружения вторжений из исключений

Вы можете удалить из исключений одно или несколько правил обнаружения вторжений, а также все правила сразу.

Чтобы удалить правило обнаружения вторжений из исключений:

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Исключения** и перейдите на закладку **IDS**.
2. Отобразится список правил обнаружения вторжений, добавленных в исключения.
3. Выберите правило, которое вы хотите удалить из исключений.

   Откроется окно с информацией о правиле.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Правило будет удалено из исключений. Правило будет применяться при создании алертов.

Чтобы удалить все или несколько правил IDS из исключений:

1. В окне веб-интерфейса приложения выберите раздел **Параметры** → **Исключения** и перейдите на закладку **IDS**.
2. Отобразится список правил обнаружения вторжений, добавленных в исключения.
3. Установите флажки напротив правил, которые вы хотите удалить из исключений.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.
4. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены из исключений. Правила будут применяться при создании алертов.

Для пользователей с ролью **Аудитор** функция удаления правила обнаружения вторжений из исключений недоступна.

Пользователи с ролью **Сотрудник службы безопасности** не имеют доступа к списку исключений из правил обнаружения вторжений.

Работа с TAA-исключениями

Правила TAA (IOA), сформированные специалистами "Лаборатории Касперского", содержат признаки подозрительного поведения объекта в IT-инфраструктуре организации. Kaspersky Anti Targeted Attack Platform проверяет базу событий приложения и создает алерты для событий, которые совпадают с поведением, описанным в правилах TAA (IOA). Если вы хотите, чтобы приложение не создавало алерты для событий, сформированных в результате нормальной для вашей организации активности хоста, вы можете добавить правило TAA (IOA) в исключения.

В приложении предусмотрены следующие режимы работы правил TAA (IOA), добавленных в исключения:

- Правило исключается всегда.

  В этом случае Kaspersky Anti Targeted Attack Platform не отмечает события как соответствующие правилу TAA (IOA) и не создает алерты по этому правилу.

- Правило дополняется условием.

  В этом случае правило TAA (IOA) дополняется условиями в виде поискового запроса. Kaspersky Anti Targeted Attack Platform не отмечает события, подходящие под заданные условия, как соответствующие правилу TAA (IOA). Для событий, которые соответствуют правилу TAA (IOA), но не соответствуют условиям примененного исключения, приложение отмечает события и создает алерты.

Если вы используете режим распределенного решения и мультитенантности, исключения TAA могут быть следующих типов:

- **Локальный** – созданные на сервере SCN. Действие исключений распространяется только на хосты, подключенные к этому серверу SCN. Исключения относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.

- **Глобальный** – созданные на сервере PCN. Действие исключений распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Исключения относятся к тенанту, в рамках которой пользователь работает в веб-интерфейсе приложения.

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, редактировать, удалять исключения в рамках тех тенантов, к данным которых у них есть доступ.

Пользователи с ролью **Аудитор** и **Сотрудник службы безопасности** могут только просматривать список исключений TAA и свойства выбранного исключения.

Для каждого правила TAA (IOA) можно создать только одно локальное или глобальное исключение.

Если для одного правила TAA (IOA) созданы исключения на сервере SCN и PCN, Kaspersky Anti Targeted Attack Platform обрабатывает события в соответствии с параметрами, заданными для исключения на сервере PCN.

Просмотр таблицы правил TAA (IOA), добавленных в исключения

Чтобы просмотреть таблицу правил TAA (IOA), добавленных в исключения:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.

2. Перейдите закладку **TAA (IOA)**.

   Отобразится таблица правил TAA (IOA), добавленных в исключения. Вы можете фильтровать правила по ссылкам в названии столбцов.

В таблице содержится следующая информация:

- – степень важности алерта, созданного в результате проверки по этому правилу TAA (IOA).

  Степень важности может иметь одно из следующих значений:

  - – **Низкая**.
  - – **Средняя**.
  - – **Высокая**.

- **Тип** – тип правила в зависимости от роли сервера, на котором оно создано:

  - **Локальный** – созданные на сервере SCN. Действие исключений распространяется только на хосты, подключенные к этому серверу SCN. Исключения относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
  - **Глобальный** – созданные на сервере PCN. Действие исключений распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Исключения относятся к тенанту, в рамках которой пользователь работает в веб-интерфейсе приложения.

- **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний правила:

  - **Высокая**.
  - **Средняя**.
  - **Низкая**.

  Чем выше уровень надежности, тем меньше вероятность ложных срабатываний.

- **Исключать правило** – режим работы правила, добавленного в исключения.

  - **Всегда** – правило исключается всегда. В этом случае Kaspersky Anti Targeted Attack Platform не отмечает события как соответствующие правилу TAA (IOA) и не создает обнаружения по этому правилу.
  - **При условии** – правило исключается при добавлении условия. В этом случае правило TAA (IOA) дополняется условиями в виде поискового запроса. Kaspersky Anti Targeted Attack Platform не отмечает события, подходящие под заданные условия, как соответствующие правилу TAA (IOA). Для событий, которые соответствуют правилу TAA (IOA), но не соответствуют условиям примененного исключения, программа отмечает события и создает обнаружения.

- **Имя** – имя правила.

Добавление правила TAA (IOA) в исключения

Вы можете добавить в исключения только правила TAA (IOA) "Лаборатории Касперского". Если вы не хотите применять при проверке событий пользовательское правило TAA (IOA), вы можете отключить это правило или удалить его.

*Чтобы добавить правило TAA (IOA) в исключения из раздела **Алерты**:*

1. В окне веб-интерфейса приложения выберите раздел **Алерты**.

   Откроется таблица алертов.

2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.

3. В раскрывающемся списке слева выберите **Содержит**.

4. В раскрывающемся списке справа выберите технологию **(TAA) Targeted Attack Analyzer**.

5. Нажмите на кнопку **Применить**.

   В таблице отобразятся алерты, выполненные технологией TAA на основе правил TAA (IOA).

6. Выберите алерт, для которого в столбце **Обнаружено** отображается название нужного правила.

   Откроется окно с информацией об алерте.

7. В блоке **Результаты проверки** по ссылке с названием правила откройте окно с информацией о правиле.

8. Справа от названия параметра **Исключение TAA (IOA)** нажмите на кнопку **Добавить в исключения**.

   Откроется окно добавления правила TAA (IOA) в исключения.

9. В поле **Исключать правило** выберите режим работы исключения:

   - **Всегда**, если вы хотите, чтобы приложение не создавало обнаружения для событий, соответствующих выбранному правилу TAA (IOA).

   - **При условии**, если вы хотите, чтобы приложение не создавало обнаружения только для событий, подходящих под заданные условия. Для событий, которые соответствуют правилу TAA (IOA) при заданных условиях исключения, приложение создаст обнаружения.

     Если вы выбрали **При условии**, выполните следующие действия:

     a. По ссылке **Настройка дополнительных условий** откройте форму поиска событий.

     b. Если вы используете режим распределенного решения и мультитенантности и хотите включить отображение событий по всем тенантам, включите переключатель **Искать по всем тенантам**.

     c. Выполните поиск событий в режиме конструктора.

        Отобразится таблица событий, соответствующих правилу TAA (IOA) при заданных условиях исключения.

        Если вы используете режим распределенного решения и мультитенантности, отобразятся уровни группировки найденных событий: Сервер – Названия тенантов – Имена серверов.

     d. Нажмите на имя того сервера, события которого вы хотите просмотреть.

        Отобразится таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей.

        > При необходимости вы можете изменить условия поиска событий.

     e. Нажмите на кнопку **Добавить исключение**.

10. Если вы используете режим распределенного решения и мультитенантности, в поле **Применить к серверам*** установите флажки напротив тенантов и серверов, к которым будет применяться правило.

11. Нажмите на кнопку **Добавить**.

Правило TAA (IOA) будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса приложения, подразделе **Исключения** на закладке **TAA (IOA)**. Это правило не будет применяться при создании обнаружений.

*Чтобы добавить правило TAA (IOA) в исключения из раздела **Поиск угроз**:*

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.

2. Задайте условия поиска и нажмите на кнопку **Найти**. Например, вы можете выбрать критерии для поиска событий в группе **Свойства TAA** в режиме конструктора.

   Отобразится таблица событий, удовлетворяющих условиям поиска.

3. Выберите событие.

4. Справа от названия параметра **Теги IOA** нажмите на имя правила.

   Откроется окно с информацией о правиле.

5. Справа от названия параметра **Исключение TAA (IOA)** нажмите на кнопку **Добавить в исключения**.

   Откроется окно добавления правила TAA (IOA) в исключения.

6. В поле **Исключать правило** выберите режим работы исключения:

   - **Всегда**, если вы хотите, чтобы приложение не создавало обнаружения для событий, соответствующих выбранному правилу TAA (IOA).

   - **При условии**, если вы хотите, чтобы приложение не создавало обнаружения только для событий, подходящих под заданные условия. Для событий, которые соответствуют правилу TAA (IOA) при заданных условиях исключения, приложение создаст обнаружения.

     Если вы выбрали **При условии**, выполните следующие действия:

     a. По ссылке **Настройка дополнительных условий** откройте форму поиска событий.

     b. Если вы используете режим распределенного решения и мультитенантности и хотите включить отображение событий по всем тенантам, включите переключатель **Искать по всем тенантам**.

     c. Выполните поиск событий в режиме конструктора.

        Отобразится таблица событий, соответствующих правилу TAA (IOA) при заданных условиях исключения.

        Если вы используете режим распределенного решения и мультитенантности, отобразятся уровни группировки найденных событий: Сервер – Названия тенантов – Имена серверов.

     d. Нажмите на имя того сервера, события которого вы хотите просмотреть.

        Отобразится таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей.

При необходимости вы можете изменить условия поиска событий.

e. Нажмите на кнопку **Добавить исключение**.

7. Нажмите на кнопку **Добавить**.

Правило TAA (IOA) будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса приложения, подразделе **Исключения** на закладке **TAA (IOA)**. Это правило не будет применяться при проверке событий.

При создании поискового запроса, сохраняемого как условия исключения, не рекомендуется использовать следующие поля:

- IOAId.
- IOATag.
- IOATechnique.
- IOATactics.
- IOAImportance.
- IOAConfidence.

Перечисленные поля отображаются только после того, как Kaspersky Anti Targeted Attack Platform отмечает события как подходящие под правила TAA (IOA).

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция добавления правила TAA (IOA) в исключения недоступна.

Просмотр правила TAA (IOA), добавленного в исключения

Чтобы просмотреть правило TAA (IOA), добавленное в исключения:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения** и перейдите на закладку **TAA (IOA)**.

   Отобразится таблица правил TAA (IOA), добавленных в исключения.

2. Выберите правило, которое вы хотите просмотреть.

   Откроется окно с информацией о правиле.

Окно содержит следующую информацию:

- **Правило TAA (IOA)** – по ссылке открывается окно с описанием техники MITRE, соответствующей этому правилу, рекомендациями по реагированию на событие и данными о вероятности ложных срабатываний.
- **ID** – идентификатор, присваиваемый приложением каждому правилу.

- **Имя** – имя правила, которое вы указали при добавлении правила.
- **Важность** – оценка возможного влияния события на безопасность компьютеров или локальной сети организации, по оценке специалистов "Лаборатории Касперского".
- **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний, по оценке специалистов "Лаборатории Касперского".
- **Исключать правило** – режим работы правила, добавленного в исключения.
  - **Всегда** – правило исключается всегда. В этом случае Kaspersky Anti Targeted Attack Platform не отмечает события как соответствующие правилу TAA (IOA) и не создает обнаружения по этому правилу.
  - **При условии** – правило исключается при добавлении условия. В этом случае правило TAA (IOA) дополняется условиями в виде поискового запроса. Kaspersky Anti Targeted Attack Platform не отмечает события, подходящие под заданные условия, как соответствующие правилу TAA (IOA). Для событий, которые соответствуют правилу TAA (IOA), но не соответствуют условиям примененного исключения, программа отмечает события и создает обнаружения.
- **Настройка дополнительных условий** – по ссылке открывается форма поиска событий с условиями поискового запроса.

  Поле отображается, если при добавлении правила TAA (IOA) в исключения вы выбрали режим работы правила **При условии** и задали условия поискового запроса.
- Условия поискового запроса в формате `<IOA ID> AND NOT <условия поискового запроса>`.

  Условия поискового запроса отображаются, если при добавлении правила TAA (IOA) в исключения вы выбрали режим работы правила **При условии** и задали условия поискового запроса.
- **Применить к серверам*** – хосты, к которым применяется исключение.

  Поле отображается в режиме распределенного решения и мультитенантности.

Удаление правил TAA (IOA) из исключений

Вы можете удалить из исключений одно или несколько правил TAA (IOA), а также все правила сразу.

Чтобы удалить правило TAA (IOA) из исключений, выполните следующие действия:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения** и перейдите на закладку **TAA (IOA)**.

   Отобразится таблица правил TAA (IOA), добавленных в исключения.
2. Выберите правило, которое вы хотите удалить из исключений.

   Откроется окно с информацией о правиле.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Правило будет удалено из исключений. Правило будет применяться при создании обнаружений и при проверке событий.

Чтобы удалить все или несколько правил TAA (IOA) из исключений, выполните следующие действия:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения** и перейдите на закладку **TAA (IOA)**.
2. Отобразится таблица правил TAA (IOA), добавленных в исключения.
3. Установите флажки напротив правил, которые вы хотите удалить из исключений.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.
4. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены из исключений. Правила будут применяться при создании обнаружений и при проверке событий.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления из исключений правил TAA (IOA) недоступна.

Работа с ICAP-исключениями

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать список ICAP-исключений – список данных, которые Kaspersky Anti Targeted Attack Platform не будет проверять. Вы можете создать правила ICAP-исключений для следующих данных:

- **Формат**.
- **Агент пользователя**.
- **MD5**.
- **Маска URL**.
- **IP или подсеть источника**.

Пользователи с ролью **Аудитор** и **Сотрудник службы безопасности** могут просматривать список правил ICAP-исключений.

В режиме распределенного решения ICAP-исключения, созданные на SCN, распространяются на все компоненты Sensor, подключенные к этой SCN. ICAP-исключения, созданные на PCN, распространяются на SCN, установленную на одном устройстве с PCN, и все подключенные к этой SCN компоненты Sensor.

Просмотр таблицы ICAP-исключений

Чтобы просмотреть таблицу ICAP-исключений:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.

   Отобразится таблица данных, которые Kaspersky Anti Targeted Attack Platform не будет проверять. Вы можете фильтровать правила по ссылкам в названии столбцов.

В столбцах таблицы содержится следующая информация:

- **Значение** – значение критерия.
- **Критерий** – критерий добавления записи в список разрешенных объектов.
- **Состояние** – состояние правила.

Добавление правила в ICAP-исключения

Правила ICAP-исключения обрабатываются в том случае, если правило с данными не было ранее добавлено в правила исключений из проверки.

Чтобы добавить правило в ICAP-исключения:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.
3. В правом верхнем углу окна веб-интерфейса приложения нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
4. Установите переключатель **Состояние** в нужное положение.

   По умолчанию переключатель находится в положении **Включено**.
5. В раскрывающемся списке **Критерий** выберите один из следующих критериев добавления правила в список ICAP-исключений:
   - **Формат**.
   - **Агент пользователя**.
   - **MD5**.
   - **Маска URL**.
   - **IP или подсеть источника**.

6. В зависимости от выбранного критерия укажите в поле **Значение** следующую информацию:

- Если вы выбрали **Формат**, в раскрывающемся списке выберите формат файла, который вы хотите добавить.

  При добавлении правила ICAP-исключения по формату содержимое веб-страниц соответствующего формата будет загружаться без проверки, а также не нарушится отображение веб-страниц.

- Если вы выбрали **Агент пользователя**, введите заголовок `User agent HTTP-запросов`, содержащий информацию о браузере.

- Если вы выбрали **MD5**, введите MD5-хеш файла.

- Если вы выбрали **Маска URL**, введите маску URL-адреса.

  При формировании маски вы можете использовать следующие специальные символы:

  * – любая последовательность **символов**.

  Пример:
  Если вы введете маску `*abc*`, приложение не будет проверять любой URL-адрес, содержащий последовательность `abc`. Например, `www.example.com/download_virusabc`

  ? – любой один **символ**.

  Пример:
  Если вы введете маску `example_123?.com`, приложение не будет проверять любой URL-адрес, содержащий заданную последовательность символов и любой символ, следующий за `3`. Например, `example_1234.com`

  Если символы `*` и `?` входят в состав полного URL-адреса, добавляемого в исключения из проверки, при вводе этих символов нужно использовать `\` – отмена одного из следующих за ним **символов** `*` или `?`, `\`.

  Пример:
  В качестве доверенного адреса требуется добавить следующий URL-адрес:
  `www.example.com/download_virus/virus.dll?virus_name=`
  Чтобы приложение не восприняло `?` как специальный символ формирования маски, нужно поставить перед `?` знак `\`.
  URL-адрес, добавляемый в список исключений из проверки, будет выглядеть следующим образом:
  `www.example.com/download_virus/virus.dll\?virus_name=`

  В поле **Маска URL** вы можете указывать доменные имена, содержащие символы кириллицы. В этом случае указанный адрес будет преобразован в Punycode и обработан в соответствии с параметрами приложения.

- Если вы выбрали **IP или подсеть источника**, введите адрес или подсеть (например, 255.255.255.0).

7. Нажмите на кнопку **Добавить**.

Правило будет добавлено в список ICAP-исключений.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция добавления правила

ICAP-исключений недоступна.

Удаление правил из ICAP-исключений

Чтобы удалить одно или несколько правил из списка ICAP-исключений:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.
3. Установите флажок слева от каждого правила, которое вы хотите удалить из списка ICAP-исключений.

   Если вы хотите удалить все правила, установите флажок над списком.
4. В нижней части окна нажмите на кнопку **Удалить**.
5. В открывшемся окне подтвердите удаление правил, нажав на кнопку **Да**.

Выбранные правила будут удалены из списка ICAP-исключений. Данные, которые находились в правилах ICAP-исключений, будут проверяться Kaspersky Anti Targeted Attack Platform.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления записи в списке ICAP-исключений недоступна.

Изменение и выключение правила в списке ICAP-исключений

Чтобы изменить правило в списке ICAP-исключений:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.
3. Выберите правило, которое вы хотите изменить.

   Откроется окно **Изменить правило**.
4. Внесите необходимые изменения в поля **Состояние**, **Критерий** и **Значение**.
5. Нажмите на кнопку **Сохранить**.

Правило будет изменено.

Чтобы выключить правило в списке ICAP-исключений:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.

3. Справа от правила, которое вы хотите выключить в списке ICAP-исключений, в столбце **Состояние** переведите переключатель в положение **Выключено**.

4. В открывшемся окне подтвердите выключение правила, нажав на кнопку **Да**.

Правило будет выключено.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения и выключения правила в списке ICAP-исключений недоступна.

Фильтрация правил в списке ICAP-исключений по критерию

Чтобы фильтровать записи в списке ICAP-исключений по критерию:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.

2. Откройте вкладку **ICAP**.

3. По ссылке **Критерий** откройте окно настройки фильтрации.

4. Установите один или несколько флажков рядом с критериями, по которым вы хотите отфильтровать правила:

   - **Формат**.
   - **Агент пользователя**.
   - **MD5**.
   - **Маска URL**.
   - **IP или подсеть источника**.

5. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

В списке ICAP-исключений отобразятся только правила, соответствующие заданным условиям фильтрации. Вы можете одновременно выполнять фильтрацию по столбцам **Значение** и **Состояние**.

Фильтрация правил в списке ICAP-исключений по значению

Чтобы фильтровать правила в списке ICAP-исключений по значению:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.

2. Откройте вкладку **ICAP**.

3. По ссылке **Значение** откройте окно настройки фильтрации.

4. Введите значение.

5. Нажмите на кнопку **Применить**.

В списке ICAP-исключений отобразятся только правила, соответствующие заданным условиям поиска. Вы можете одновременно выполнять фильтрацию по столбцам **Критерий** и **Состояние**.

Фильтрация правил в списке ICAP-исключений по состоянию

Чтобы фильтровать правила в списке ICAP-исключений по состоянию:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.

2. Откройте вкладку **ICAP**.

3. По ссылке **Состояние** откройте окно настройки фильтрации.

4. Установите флажок напротив одного из значений:

   - **Включено**.
   - **Выключено**.

5. Нажмите на кнопку **Применить**.

В списке ICAP-исключений отобразятся только правила, соответствующие заданным условиям поиска. Вы можете одновременно выполнять фильтрацию по столбцам **Критерий** и **Значение**.

Сброс условий фильтрации правил в списке ICAP-исключений

Чтобы сбросить условия фильтрации правил в списке ICAP-исключений:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.

2. Откройте вкладку **ICAP**.

3. Нажмите на кнопку справа от того заголовка столбца таблицы **Значение**, **Критерий** или **Состояние**, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные условия фильтрации будут сброшены. В списке ICAP-исключений отобразятся только правила, соответствующие заданным условиям.

Работа с зеркалированным трафиком со SPAN-портов

При работе в веб-интерфейсе приложения пользователи с ролью **Старший сотрудник службы безопасности** могут выгружать дампы зеркалированного трафика со SPAN-портов в формате PCAP с серверов с компонентом Sensor и проводить расследование для обнаружения подозрительной активности.

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия на том сервере PCN или SCN, к которому подключен сервер с компонентом Sensor.

Чтобы выгрузить зеркалированный трафик со SPAN-портов:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.
3. Нажмите на кнопку **Скачать трафик**.

   Отобразится окно настройки параметров выгрузки.

   В разделе **Внутреннее хранилище** в поле **Самый старый пакет** отображается дата и время первого сохраненного дампа во внутреннем хранилище. В поле **Занято / максимально** первое число обозначает занятое пространство во внутреннем хранилище, а второе число обозначает общий размер внутреннего хранилища. В разделе **Внешнее хранилище** отображается статус хранилища: **Подключено** или **Не подключено**.
4. Выполните следующие действия:

   - В поле **Период трафика для скачивания** задайте границы, в рамках которых вы хотите выгрузить дампы трафика.

     Если вы выберете период, за который отсутствует записанный трафик, при нажатии кнопки **Скачать трафик** Kaspersky Anti Targeted Attack Platform предложит выбрать вам период всего от первого записанного дампа сетевого трафика до последнего. В случае, если записанные дампы отсутствуют, отобразится предупреждение об отсутствии данных за указанный период.

   - В поле **Ограничение объема скачивания** вы можете указать максимальный объем для выгрузки трафика.

     Если объем загружаемого трафика превысит заданное ограничение, будет отброшен более поздний трафик.

   - При необходимости включите фильтрацию в блоке **Фильтрация по точкам мониторинга** и укажите точки мониторинга, с которых вы хотите получить трафик.

   - При необходимости включите фильтрацию в блоке **Фильтрация с использованием BPF** и введите выражение для фильтрации с использованием технологии BPF (Berkeley Packet Filter). Для написания выражения фильтрации BPF используется формат libpcap. Подробнее об описании синтаксиса см. в Руководстве pcap-filter.

     Пример выражения для фильтрации:
     ```
     tcp port 102 or tcp port 502
     ```

- При необходимости включите фильтрацию в блоке **Фильтрация с использованием регулярных выражений** и введите выражение для фильтрации по данным, составляющим полезную нагрузку в трафике.

  Пример выражения для фильтрации:
  `^test.+xABxCD`

5. Нажмите на кнопку **Скачать трафик**.

Дампы зеркалированного трафика со SPAN-портов будут выгружены в формате PCAP.

Рекомендация по выполнению поочередных запросов на выгрузку трафика

Рекомендуется учитывать длительность выполнения предыдущего запроса на выгрузку трафика, прежде чем отправлять очередной запрос.

Если очередной запрос на выгрузку трафика поступает раньше, чем завершился предыдущий, может сложиться ситуация, когда файлы дампов не скачиваются, но сообщение об ошибке при этом не появляется.

Длительность запроса зависит от различных факторов: диапазон поиска, объем выгружаемого трафика, скорость связи между Sensor, сервером и компьютером клиента.

Объем выгружаемого трафика зависит от потребностей клиента; выгрузка небольших объемов выполняется за секунды. Если пользователь попытается загрузить весь доступный трафик, сработает ограничение на скорость выгрузки трафика в 50 Мбит/с. Такое ограничение предохраняет систему от перегрузки, вызванной выгрузкой большого объема трафика. На скорости 50 Мбит/с выгрузка 1 ГБ трафика занимает примерно 20 секунд, а 1 ТБ выгружается приблизительно за 5,5 часов.

Создание списка паролей для архивов

Приложение не проверяет архивы, защищенные паролем. Вы можете создать список наиболее часто встречающихся паролей для архивов, которые используются при обмене файлами в вашей организации. В этом случае при проверке архива приложение будет проверять пароли из списка. Если какой-либо из паролей подойдет, архив будет разблокирован и проверен.

Список паролей, заданный в параметрах приложения, также передается на сервер с компонентом Sandbox.

Чтобы создать список паролей для архивов:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пароли к архивам**.
2. В поле **Пароли к архивам** введите пароли, которые приложение будет использовать для архивов, защищенных паролем.

   Вводите каждый пароль с новой строки. Вы можете ввести до 50 паролей.
3. Нажмите на кнопку **Применить**.

Список паролей для архивов будет создан. При проверке файлов формата PDF, а также файлов приложений Microsoft Word, Excel®, PowerPoint®, защищенных паролем, приложение будет подбирать пароли из заданного списка.

Пользователи с ролью **Аудитор** могут просматривать список паролей для архивов без возможности редактирования.

Пользователи с ролью **Сотрудник службы безопасности** не имеют доступа к этому разделу веб-интерфейса.

Работа с информацией о серверах с компонентами Central Node и Sensor

Пользователям с ролью **Аудитор** доступен просмотр информации о серверах с компонентами Central Node и Sensor.

Информация о серверах с компонентами Central Node и Sensor отображается в разделе **Серверы Sensor** окна веб-интерфейса приложения.

В разделе отображаются карточки компонентов (слева) и карточки сетевых интерфейсов, обнаруженных на этих компонентах (справа от каждого компонента).

Над карточкой компонента Sensor отображается карточка компонента Central Node, к которому подключен Sensor.

Если компонент Central Node развернут со встроенным компонентом Sensor, для этого компонента Sensor в карточке отображается имя Embedded Sensor.

На карточке сетевого интерфейса отображаются следующие сведения:

- Имя сетевого интерфейса.
- MAC-адрес сетевого интерфейса.
- IP-адрес сетевого интерфейса.
- Пропускная способность сетевого интерфейса.

Если на сетевой интерфейс добавлена точка мониторинга, на карточке сетевого интерфейса отображаются следующие сведения о точке мониторинга:

- Имя точки мониторинга.
- **Режим технологий** – состояние функции наследования технологий. Может иметь значение **Включено** или **Выключено**.

Вы можете просмотреть подробную информацию о компонентах Central Node и Sensor и сетевых интерфейсах, обнаруженных на этих компонентах.

Чтобы просмотреть подробную информацию о компоненте или сетевом интерфейсе,

наведите курсор мыши на его карточку и нажмите на нее левой кнопкой мыши.

На вкладке **Параметры** для компонентов Central Node и Sensor отображаются следующие сведения:

- **Статус** – текущий статус компонента в виде значка и текстового описания.
- **Тип узла** – компонент приложения: **Сервер** (компонент Central Node) или **Сенсор** (компонент Sensor).
- **Текущий объем данных программы** – пространство на диске, занятое файлами приложения. Включает в себя установленные файлы и файлы, созданные в процессе работы приложения.
- **Максимально возможный объем данных программы** – пространство на диске, которое могут занять файлы приложения. Включает в себя установленные файлы и сумму всех заданных ограничений по объему в правилах хранения данных. Значение не может превышать объем доступного пространства на диске.
- **Занято на диске** – пространство на диске, занятое всеми файлами. Включает в себя файлы приложения, файлы операционной системы и других приложений. Объем пространства рассчитывается на диске, который содержит директорию /var/ в файловой системе компонента.
- **Свободно на диске** – пространство на диске, не занятое файлами. Объем пространства рассчитывается на диске, который содержит директорию /var/ в файловой системе компонента.
- **Объем диска** – общий объем пространства на диске, который содержит директорию /var/ в файловой системе компонента.
- **BPF-фильтрация** – признак включенной или выключенной фильтрации с использованием технологии BPF (Berkeley Packet Filter) по адресным параметрам в сетевых пакетах.
- **Внешнее хранилище для файлов дампа трафика** – статус подключения внешнего хранилища. Могут отображаться следующие статусы: **Подключено**, **Не подключено**.
- **Правила хранения** – текущие и максимальные значения объема, количества элементов и времени хранения данных приложения.

Для компонента Sensor, кроме вкладки **Параметры**, также отображаются вкладки **Внешнее хранилище**, **Другое**, **ICAP-интеграция**, **POP3-интеграция**, **SMTP-интеграция**.

- На вкладке **Внешнее хранилище** отображается информация о параметрах внешнего хранилища для записи зеркалированного SPAN-трафика.
- На вкладке **Другое** отображается следующая информация:
  - Максимальный размер проверяемого файла – текущее ограничение на размер файлов, проверяемых компонентом.
  - Запись HTTP body – признак включенной или выключенной записи содержимого HTTP-пакета.
- На вкладке **ICAP-интеграция** отображаются параметры интеграции с прокси-сервером по протоколу ICAP.
- На вкладке **POP3-интеграция** отображаются параметры интеграции с почтовым сервером по протоколу POP3.
- На вкладке **SMTP-интеграция** отображаются параметры интеграции с почтовым сервером по протоколу SMTP.

Для сетевого интерфейса, на который не добавлена точка мониторинга, в области деталей отображаются следующие сведения:

- **Сетевой интерфейс** – имя сетевого интерфейса в операционной системе.
- **Подключение** – значок подключения сетевого кабеля к Ethernet-порту сетевого интерфейса:
  - – сетевой кабель подключен;
  - – сетевой кабель отключен.

  Значок мигает при включенном режиме индикации Ethernet-порта.
- **MAC-адрес** – MAC-адрес сетевого интерфейса.
- **IP-адрес** – IP-адрес сетевого интерфейса. Если на сетевом интерфейсе обнаружено несколько IP-адресов, то в области деталей отображаются не более 16 IP-адресов.

Если на сетевой интерфейс добавлена точка мониторинга, в карточке сетевого интерфейса отображаются следующие сведения:

- **Статус** – текущий статус точки мониторинга в виде значка и текстового описания:
  - *OK*. Точка мониторинга доступна.
  - *Переключение*. Происходит переключение режима работы точки мониторинга.
  - *Ошибка*. Обнаружена ошибка при переключении режима работы точки мониторинга.
- **Подключение** – значок подключения сетевого кабеля к Ethernet-порту сетевого интерфейса:
  - – сетевой кабель подключен;
  - – сетевой кабель отключен.

Значок мигает при включенном режиме индикации Ethernet-порта.

- **Сетевой интерфейс** – имя сетевого интерфейса в операционной системе.
- **Режим** – текущий режим работы точки мониторинга:
  - *Включена*.
  - *Выключена*.
- На вкладке **Параметры**:
  - **Наследование технологий** – признак включенного или выключенного наследования технологий сервера.
  - **MAC-адрес** – MAC-адрес сетевого интерфейса.
  - **IP-адрес** – IP-адрес сетевого интерфейса.

Просмотр параметров сервера

Пользователям с ролью **Аудитор** доступен просмотр настроек сервера Central Node и PCN в режиме распределенного решения и мультитенантности.

Настройки сервера располагаются в разделе **Параметры** окна веб-интерфейса. В этом разделе вы можете просмотреть следующую информацию:

- **Пользователи**:
  - **Пользователи** – список учетных записей пользователей
  - **Интеграция с Active Directory** – параметры интеграции с Active Directory.
- **Общие параметры**:
  - **Обновление баз** – обновление баз данных.
  - **Мониторинг** – максимальное допустимое значение заполнения жесткого диска серверов Central Node и Sensor.
  - **SNMP** – параметры соединения с протоколом SNMP.
- **Политики аутентификации** – параметры политик аутентификации.
- **Сертификаты** – состояние сертификатов сервера и компьютеров с компонентом Endpoint Agent.
- **Дата и время** – настройки даты и времени сервера.
- **Endpoint Agents** – функции приложения, доступные при интеграции с компонентом Endpoint Agent.
  - **Телеметрия** – настройка объема принимаемых данных от компонента Endpoint Agent.
  - **Расписание IOC-проверки** – настройки расписания IOC-проверки.

- **Автоматическая отправка файлов в Sandbox** – автоматическая отправка файлов на проверку компоненту Sandbox.
- **Индикаторы активности** – показатели активности компонента Endpoint Agent.
- **Автоматическое удаление неактивных хостов** – автоматическое удаление неактивных хостов из таблицы Endpoint Agents.
- **Отправка файлов с хостов на анализ в Sandbox вручную** – ручная отправка файлов на проверку компоненту Sandbox.
- **Использование правил TAA (IOA) для цепочек событий –** использование правил TAA (IOA), проверяющие цепочки событий. По умолчанию функция выключена.

- **Проверка трафика ICAP** – параметры интеграции с прокси-сервером по протоколу ICAP.
- **Серверы подключений** – серверы, выполняющие роль серверов интеграции для компонента Endpoint Agent.
- **Коннекторы** – параметры коннекторов.
- **Секреты** – параметры секретов.
- **Типы событий** – параметры типов событий.
- **Типы рисков** – параметры типов рисков.
- **KSN/KPSN и MDR** – настройки участия в Kaspersky Security Network и Kaspersky Private Security Network и включение интеграции с MDR.
- **Репутационная база KPSN** – настройки использования репутационной базы KPSN.
- **Уведомления** – настройки отправки уведомлений.
- **SIEM-система** – настройки интеграции с SIEM-системой.
- **Статус VIP** – список правил присвоения обнаружениям статуса VIP.
- **Исключения** – список разрешенных объектов и списки исключений из правил TAA и IDS.
- **Сетевые параметры** – настройки параметров сетевого интерфейса.
- **Разрешающие правила** – правила контроля взаимодействий устройств в сети.
- **Пароли к архивам** – список паролей для архивов.
- **Лицензия** – состояние ключа лицензии.

Просмотр таблицы серверов с компонентом Sandbox

Пользователи с ролью **Аудитор** могут просматривать таблицу серверов с компонентом Sandbox.

Таблица серверов с компонентом Sandbox находится в разделе **Серверы Sandbox**, на закладке **Серверы** окна веб-интерфейса приложения.

В поле **Отпечаток сертификата** отображается отпечаток TLS-сертификата сервера Central Node.

Таблица **Список серверов** содержит следующую информацию:

- **IP и имя** – IP-адрес или полное доменное имя сервера с компонентом Sandbox.
- **Отпечаток сертификата** – отпечаток сертификата сервера с компонентом Sandbox.
- **Авторизация** – статус запроса на подключение к компоненту Sandbox.
- **Состояние** – состояние подключения к компоненту Sandbox.

Для пользователей с ролью **Сотрудник службы безопасности** просмотр таблицы серверов с компонентом Sandbox недоступен.

Просмотр параметров набора операционных систем для проверки объектов в Sandbox

Пользователи с ролью **Аудитор** могут просматривать параметры набора операционных систем, на основе которого будут формироваться задачи на проверку объектов для компонента Sandbox. На сервере Sandbox должны быть установлены виртуальные машины, которые соответствуют выбранному набору.

Информация о параметрах набора операционных систем для проверки объектов в Sandbox находится в разделе **Серверы Sandbox**, на закладке **Параметры** окна веб-интерфейса приложения.

В блоке параметров **Набор ОС** отображаются наборы операционных систем, в которых компонент Sandbox может проверять объекты.

В блоке параметров **Состав набора** отображаются операционные системы, которые входят в состав выбранного набора.

Просмотр таблицы внешних систем

Пользователи с ролью **Аудитор** могут просматривать таблицу внешних систем.

Таблица внешних систем находится в разделе **Внешние системы** окна веб-интерфейса приложения.

В поле **Отпечаток сертификата** отображается отпечаток TLS-сертификата сервера Central Node.

В таблице **Список серверов** содержится следующая информация:

- **Sensor** – IP-адрес или доменное имя сервера внешней системы.
- **Тип** – тип внешней системы (почтовый сенсор или другая система).

- **Имя** – название интегрированной внешней системы, не являющейся почтовым сенсором.

  Для почтового сенсора в этой столбце отображается прочерк.

- **ID** – идентификатор внешней системы.

- **Отпечаток сертификата** – отпечаток TLS-сертификата сервера с внешней системой, с помощью которого устанавливается шифрованное соединение с сервером Central Node.

  Отпечаток сертификата сервера с компонентом Central Node отображается в верхней части окна в поле **Отпечаток сертификата**.

- **Состояние** – состояние запроса на интеграцию.

Для пользователей с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** просмотр таблицы внешних систем недоступен.

Работа с пользовательскими правилами Sandbox

Пользовательские правила Sandbox для проверки файлов и URL-адресов позволяют отправлять объекты на проверку в пользовательских виртуальных машинах. Если правила не добавлены, объекты в пользовательских виртуальных машинах не проверяются. При этом для отправки объектов на проверку в преднастроенных виртуальных машинах правила создавать не требуется. Kaspersky Anti Targeted Attack Platform по умолчанию отправляет на проверку объекты, которые требуется проверить.

Создание правил доступно только при наличии пользовательских виртуальных машин.

Пользователи с ролями **Старший сотрудник службы безопасности** и **Администратор** могут создавать правила для проверки файлов и URL-адресов, редактировать, удалять, включать и отключать правила. Правила для проверки файлов можно также импортировать и экспортировать.

В режиме распределенного решения вам нужно создать правила для проверки файлов в пользовательских виртуальных машинах на каждом сервере PCN и SCN, с которого вы хотите отправлять файлы на проверку.

Пользователи с ролью **Аудитор** могут просматривать список правил. Для пользователей с ролью **Сотрудник службы безопасности** просмотр раздела недоступен.

Просмотр таблицы пользовательских правил Sandbox

Чтобы просмотреть таблицу пользовательских правил Sandbox:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы** или **URL-адреса**.

   Отобразится таблица пользовательских правил Sandbox для проверки файлов или URL-адресов.

В таблице пользовательских правил для проверки файлов содержится следующая информация:

- **Создано** – время создания правила.
- **Виртуальная машина** – имя виртуальной машины, на которую отправляются файлы для проверки.
- **Маска** – маска файлов, отправляемых на проверку.
- **Исключение по маске** – маска файлов, которые исключены из проверки.
- **Категория файла** – категории файлов, отправляемых на проверку.
- **Состояние** – состояние правила. Может иметь значения **Включено** и **Выключено**.

В таблице пользовательских правил для проверки URL-адресов содержится следующая информация:

- **Создано** – время создания правила.
- **Виртуальная машина** – имя виртуальной машины, на которую отправляются файлы для проверки.
- **Состояние** – состояние правила. Может иметь значения **Включено** и **Выключено**.

Настройка отображения таблицы правил Sandbox

Вы можете настроить отображение столбцов, а также порядок их следования в таблице.

Чтобы настроить отображение таблицы:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы** или **URL-адреса**.

   Отобразится таблица пользовательских правил Sandbox для проверки файлов или URL-адресов.
3. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.
4. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.
5. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.
6. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.
7. Нажмите на кнопку **Применить**.

Отображение таблицы правил будет настроено.

Фильтрация и поиск правил Sandbox

Чтобы отфильтровать или найти правила Sandbox по требуемым критериям:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы** или **URL-адреса**.

3. Выполните следующие действия в зависимости от критерия фильтрации:

   - **По времени создания**

     a. По ссылке **Создано** откройте окно настройки фильтрации.

     b. Выберите один из следующих вариантов:

     - **За все время**, если вы хотите, чтобы приложение отображало в таблице правила, созданные за все время.
     - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице правила, созданные за предыдущий час.
     - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице правила, созданные за предыдущий день.
     - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице правила, созданные за указанный вами период.

     c. Если вы выбрали **Пользовательский диапазон**, выберите даты начала и конца периода и нажмите на кнопку **Применить**.

   - **По названию виртуальной машины**

     a. По ссылке **Виртуальная машина** откройте окно настройки фильтрации.

     b. Введите один или несколько символов имени виртуальной машины.

     c. Нажмите на кнопку **Применить**.

   В таблице отобразятся только правила, соответствующие заданным условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил Sandbox

Чтобы сбросить фильтрацию правил Sandbox по одному или нескольким условиям:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы** или **URL-адреса**.
3. Нажмите на кнопку справа от того заголовка столбца таблицы правил, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу для каждого из условий.

   Выбранные фильтры будут сброшены.

   В таблице отобразятся только правила, соответствующие заданным условиям.

Просмотр информации о пользовательском правиле Sandbox

Чтобы просмотреть информацию о пользовательском правиле Sandbox:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы** или **URL-адреса**.
3. Выберите правило, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о правиле.

Окно с информацией о пользовательском правиле для проверки файлов содержит следующую информацию:

- **Состояние** – состояние правила запрета.
- **Виртуальная машина** – виртуальная машина, на которой проверяются файлы по этому правилу.
- **Маска** – маска файлов, которые отправляются на проверку.
- **Исключение по маске** – маска файлов, которые исключены из проверки.
- **Категория файла** – категории файлов, которые отправляются на проверку.
- **Размер файла** – размер проверяемых файлов.

Окно с информацией о пользовательском правиле для проверки URL-адресов содержит следующую информацию:

- **Виртуальная машина** – виртуальная машина, на которой проверяются URL-адреса.
- **Состояние** – состояние правила запрета.

Создание пользовательского правила Sandbox для проверки файлов

Чтобы добавить пользовательское правило Sandbox для проверки файлов:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы**.
3. Нажмите на кнопку **Добавить**.
4. Выберите **Создать правило**.

   Откроется окно создания правила.

5. Задайте значения следующих параметров:

   a. **Состояние** – состояние правила запрета. Установите флажок, если вы хотите включить правило.

   b. **Виртуальная машина** – виртуальная машина, на которой будут проверяться файлы по этому правилу.

      Для выбора доступны только виртуальные машины с пользовательскими образами операционных систем. Эти виртуальные машины должны входить в набор операционных систем, выбранных на сервере Central Node.

   c. Укажите хотя бы одно из значений: маску или категорию файла. Если вы заполните все поля, то правило сработает для файлов, которые подпадают под условия по категории и размеру или по маске и размеру и при этом не являются исключениями.

      - **Маска** – маска файлов, которые вы хотите отправлять на проверку. Вы можете указать несколько значений.

        Чтобы указать маску, используйте метасимволы * и ?. Другие метасимволы не поддерживаются.

      - **Исключение по маске** – маска файлов, которые требуется исключить из проверки. Вы можете указать несколько значений.

        Чтобы указать исключения по маске, используйте метасимволы * и ?. Другие метасимволы не поддерживаются.

      - **Категория файла** – категории файлов, которые вы хотите отправлять на проверку. Вы можете указать несколько категорий.

        Вы можете посмотреть полный список расширений для каждой категории в разделе Список расширений для категорий файлов.

      - **Размер файла** – размер проверяемых файлов.

      - Если вы хотите задать несколько интервалов, нажмите на кнопку **Добавить размер файла**.

6. Нажмите на кнопку **Добавить**.

Правило будет создано.

Если вы хотите отправлять на проверку архив, вам нужно учитывать особенности проверки архивов.

Проверка архивов осуществляется следующим образом:

1. Kaspersky Anti Targeted Attack Platform распаковывает архив.

2. Файлы из архива, соответствующие правилу, отправляются на проверку.

Файлы с расширением MSI проверяются так же, как архивы.

Создание пользовательского правила Sandbox для проверки URL-адреса

Чтобы добавить пользовательское правило Sandbox для проверки URL-адресов:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **URL-адреса**.
3. Нажмите на кнопку **Добавить**.
4. Выберите **Создать правило**.

   Откроется окно создания правила.
5. Задайте значения следующих параметров:

   a. **Виртуальная машина** – виртуальная машина, на которой будут проверяться URL-адреса.

   Для выбора доступны только виртуальные машины с пользовательскими образами операционных систем. Эти виртуальные машины должны входить в набор операционных систем, выбранных на сервере Central Node.

   b. **Состояние** – состояние правила запрета. Установите флажок, если вы хотите включить правило.
6. Нажмите на кнопку **Добавить**.

Правило будет создано.

Копирование пользовательского правила Sandbox

Чтобы копировать пользовательское правило Sandbox:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы** или **URL-адреса**.
3. Выберите нужное правило.
4. В окне просмотра правила нажмите на кнопку **Скопировать**.

Правило будет скопировано со всеми параметрами. Вы можете изменить значения параметров при необходимости.

Импорт пользовательских правил Sandbox для проверки файлов

Чтобы импортировать пользовательские правила Sandbox для проверки файлов:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы**.
3. Нажмите на кнопку **Добавить**.
4. Выберите **Импортировать правила**.
5. Откроется окно загрузки файла.
6. Выберите файл, который вы хотите импортировать.
7. Нажмите на кнопку **Open**.

Файл будет импортирован.

Изменение пользовательского правила Sandbox

Чтобы изменить пользовательское правило Sandbox:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы** или **URL-адреса**.

   Отобразится таблица пользовательских правил Sandbox для проверки файлов или URL-адресов.
3. Выберите правило.

Откроется окно редактирования правила.

Для редактирования доступны следующие поля:

- В пользовательских правилах Sandbox для проверки файлов:
  - **Состояние** – состояние правила запрета. Установите флажок, если вы хотите включить правило.
  - **Виртуальная машина** – виртуальная машина, на которой будут проверяться файлы по этому правилу.

    Для выбора доступны только виртуальные машины с пользовательскими образами операционных систем. Эти виртуальные машины должны входить в набор операционных систем, выбранных на сервере Central Node.

- Укажите хотя бы одно из значений: маску или категорию файла. Если вы заполните все поля, то правило сработает для файлов, которые подпадают под условия по категории и размеру или по маске и размеру и при этом не являются исключениями.

  - **Маска** – маска файлов, которые вы хотите отправлять на проверку. Вы можете указать несколько значений.

    Чтобы указать маску, используйте метасимволы * и ?. Другие метасимволы не поддерживаются.

  - **Исключение по маске** – маска файлов, которые требуется исключить из проверки. Вы можете указать несколько значений.

    Чтобы указать исключения по маске, используйте метасимволы * и ?. Другие метасимволы не поддерживаются.

  - **Категория файла** – категории файлов, которые вы хотите отправлять на проверку. Вы можете указать несколько категорий.

    Вы можете посмотреть полный список расширений для каждой категории в разделе Список расширений для категорий файлов.

  - **Размер файла** – размер проверяемых файлов.

    Если вы хотите задать несколько интервалов, нажмите на кнопку **Добавить размер файла**.

- В пользовательских правилах Sandbox для проверки URL-адресов:

  - **Виртуальная машина** – виртуальная машина, на которой будут проверяться URL-адреса.

    Для выбора доступны только виртуальные машины с пользовательскими образами операционных систем. Эти виртуальные машины должны входить в набор операционных систем, выбранных на сервере Central Node.

  - **Состояние** – состояние правила запрета. Установите флажок, если вы хотите включить правило.

Включение и отключение пользовательских правил Sandbox

Чтобы включить или отключить использование правила Sandbox:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы** или **URL-адреса**.

   Отобразится таблица пользовательских правил Sandbox для проверки файлов или URL-адресов.
3. В строке с нужным правилом в столбце **Состояние** включите или выключите переключатель.

Использование правила будет включено или отключено.

Чтобы включить или отключить использование всех или нескольких правил Sandbox:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы** или **URL-адреса**.

   Отобразится таблица пользовательских правил Sandbox для проверки файлов или URL-адресов.

3. Установите флажки слева от правил, использование которых вы хотите включить или отключить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

4. Нажмите на кнопку **Включить** или **Отключить**, чтобы включить или отключить использование выбранных правил.

Использование выбранных правил будет включено или отключено.

Экспорт пользовательских правил Sandbox для проверки файлов

Чтобы экспортировать пользовательские правила Sandbox для проверки объектов:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы**.
3. Нажмите на кнопку **Экспортировать**.

Файл с правилами будет сохранен на ваш локальный компьютер. Файл загружается в формате JSON.

Удаление пользовательских правил Sandbox

Пользователи с ролью **Старший сотрудник службы безопасности** могут удалить одно или несколько пользовательских правил Sandbox, а также все правила сразу.

Чтобы удалить пользовательское правило Sandbox:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы** или **URL-адреса**.

   Отобразится таблица пользовательских правил Sandbox для проверки файлов или URL-адресов.

3. Выберите правило, которое вы хотите удалить.

   Откроется окно с информацией об этом правиле.

4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

5. Нажмите на кнопку **Да**.

Правило будет удалено.

Чтобы удалить все или несколько пользовательских правил Sandbox:

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **Sandbox**.
2. Откройте вкладку **Файлы** или **URL-адреса**.

   Отобразится таблица пользовательских правил Sandbox для проверки файлов или URL-адресов.
3. Установите флажки слева от правил, которые вы хотите удалить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Список расширений для категорий файлов

Список расширений для категорий файлов приведен в таблице ниже.

Расширения для категорий файлов

Категория	Расширения
1C	.epf, .ert, .erf, .cf, .dt, .deb, .bsl, .os, .ertx, .xls, .xml, .html, .txt, .cfu, .rptdesign, .xdt, .xslt, .wsdl
Adobe Flash Player	.swf, .fla, .flv, .f4v, .f4p, .f4a, .f4b, .mxml, .as, .asc, .ascs, .asv, .fxp, .fxpl, .xfl, .swc, .cfx, .spl, .dcr, .dir, .dxr, .aam, .swz
Java	.jar, .class, .war, .ear, .jad, .jnlp, .ser, .jsp, .jspx, .properties, .policy
Html	.html, .htm, .shtml, .xhtml, .xml, .svg, .mathml, .rss, .atom, .json, .mht, .mhtml, .webarchive
Сетевой пакет	.pcap, .pcapng, .cap, .netcap, .etl, .erf, .pkts, .pkt, .tcpdump, .snoop, .ngc, .dump, .cat, .smb, .vpcap, .dmp, .shb, .npl, .nfcapd, .wcap, .arpd, .pc, .tr1, .tr2, .trace
SAP	.abap, .adt, .bak, .cct, .cdp, .cpf, .dsc, .erd, .glo, .grc, .lis, .log, .lsa, .msg, .olap, .pgm, .prd, .sap, .sd, .se, .so, .spf, .tpz, .trc, .trex, .ttx, .wri, .xlf
XML	.xml, .xsl, .xslt, .rdf, .rss, .opf, .svg, .wsdl, .xhtml, .xjb, .xmi, .xpl, .xsl-fo, .xquery, .xsd, .dtd, .xht, .atom, .mathml, .mml, .plist, .xul, .fodt, .fo, .mxf, .xspf, .gpx, .unity, .ac, .ad, .aw, .ccxml, .csd, .dms, .epub, .fxml, .glb, .glTF, .glTF-Binary, .gml, .iif, .imdi, .jelly, .kml, .mrc, .msh, .mshxml, .mtl, .nib, .nws, .nzb, .osdx, .owl, .pbix, .plistxml, .ptx, .qti, .rdfxml, .rl, .rng, .ros, .rpj, .scml, .scxml, .shex, .sketch, .soap, .srdf, .srx
Архив	.snb, .apk, .mht, .crx, .dd, .r01, .mpkg, .pup, .tbz, .ace, .arj, .bin, .cab, .cbr, .deb, .exe, .gzip, .one, .pak, .pkg, .ppt, .rpm, .sh, .sib, .sis, .sisx, .sit, .sitx, .spl, .tar-gz, .xar, .zipx, .zip, .rar, .7z, .tar, .gz, .bz2, .xz, .tgz, .tbz2, .txz, .z, .jar, .war, .ear, .iso, .img
Аудио	.a52, .adt, .dct, .dss, .dvf, .iklax, .ivs, .rm, .rmvb, .8svx, .amb, .avr, .cdda, .cvs, .cvsd, .cvu, .dts, .dvms, .fap, .fssd, .gsrt, .hcom, .htk, .ima, .ircam, .maud, .nist, .paf, .prc, .pvf, .sd2, .smp, .snd, .sndr, .sndt, .sou, .sph, .spx, .tta, .txw, .vms, .voc, .vox, .w64, .wv, .wve, .ac3, .aob, .asf, .aud, .bin, .bwg, .cdr, .gpx, .ics, .m, .m3u, .mod, .mpp, .msc, .msv, .mts, .nkc, .ps, .sdf, .sib, .sln, .spl, .srt, .temp, .vb, .wave, .wm, .wpd, .xsb, .xwb, .mpc, .aac, .flac, .m4a, .mmf, .mp3, .ogg, .wav, .wma, .mid, .amr, .ape, .au, .caf, .gsm, .oma, .qcp, .vqf, .ra, .aif, .mp2, .m4p, .awb, .m4r, .ram, .asx, .mpga, .aiff, .koz, .m4b, .kar, .iff, .midi, .3ga, .opus, .aup, .xspf, .aifc, .rta, .cda, .m3u8, .mpa, .aa, .aax, .oga, .nfa, .adpcm, .cdo, .flp, .aimppl, .4mp, .mui
Видео	.drc, .f4a, .f4b, .f4p, .gifv, .mng, .mp2, .mpe, .mpv, .nsv, .roq, .svi, .3gp2, .3gpp2, .asx, .bin, .dat, .drv, .gtp, .moov, .spl, .stl, .vcd, .vid, .wm, .yuv, .hevc, .m2v, .mjpeg, .wtv, .avi, .mpeg, .m4v, .mov, .mp4, .wmv, .mpg, .swf, .3gp, .3g2, .mkv, .ogv, .webm, .asf, .ts, .mxf, .rm, .thp, .mts, .rmvb, .f4v, .mod, .vob, .h264, .flv, .3gpp, .divx, .qt, .amv, .dvsd, .m2ts, .ifo, .mswmm, .srt, .cpi, .wlmp, .vpj, .ced, .vep, .veg, .264, .dav, .pds, .dir, .arf, .mepx, .xesc, .bik, .nfv, .tvs, .imoviemobile, .rcproject, .esp3, .vproj, .aep, .camproj, .camrec, .cmproj, .cmrec, .modd, .mproj, .osp, .trec, .g64, .vro, .braw, .mse, .pz

Категория	Расширения
Документ	.sxi, .odg, .svg, .vsd, .eps, .cwk, .wp, .ott, .asp, .cdd, .cpp, .dotm, .gpx, .indd, .kdc, .kml, .mdb, .mdf, .mso, .one, .pkg, .pl, .pot, .potm, .potx, .ppsm, .ps, .sdf, .sgml, .sldm, .xar, .xlt, .xltm, .xltx, .pdf, .txt, .doc, .odt, .xps, .chm, .rtf, .sxw, .docx, .wpd, .wps, .docm, .hwp, .pub, .xml, .log, .oxps, .vnt, .dot, .pages, .m3u, .dotx, .shs, .msg, .odm, .pmd, .vmg, .eml, .tex, .wp5, .csk, .fdxt, .adoc, .afpub, .tcr, .acsm, .opf, .mbp, .apnx, .cbt, .vbk, .kfx, .lrf, .snb, .odp, .ppt, .pptx, .pps, .ppsx, .pptm, .key, .flipchart, .epub, .mobi, .azw, .azw3, .fb2, .djvu, .cbz, .cbr, .ibooks, .lit, .pdb, .prc, .tr2, .tr3, .ods, .xls, .xlsx, .csv, .wks, .xlsm, .xlsb, .xlr, .wk3, .numbers
Изображение	.dib, .pdf, .mrw, .icns, .wdp, .fig, .epsf, .cur, .erf, .fts, .heif, .jfif, .jpe, .jps, .mng, .pam, .pbm, .pes, .pfm, .picon, .pnm, .ppm, .ras, .rw2, .sgi, .x3f, .xbm, .xpm, .xwd, .art, .arw, .bmp, .cr2, .crw, .dcm, .dds, .djvu, .dng, .exr, .fpx, .gif, .ico, .jpg, .jp2, .jpeg, .nef, .orf, .pcd, .pcx, .pef, .pgm, .pict, .png, .psd, .raf, .sfw, .tga, .tiff, .wbmp, .xcf, .yuv, .kdc, .pct, .sr2, .tif, .hdr, .webp, .nrw, .plist, .ithmb, .thm, .pspimage, .mac, .heic, .rwl, .flif, .avif, .raw, .pictclipping, .jxr, .emf, .eps, .svg, .wpg, .ai, .svgz, .wmf, .odg, .cdr, .vsd, .std, .pd, .emz, .mix, .otg, .cvs, .gvdesign
Исполняемый файл Android	.apk, .aab, .dex, .so, .jar, .aar, .class, .obb, .odex, .vdex, .vmx, .vmem, .img
Исполняемый файл Windows	.cgi, .ds, .air, .cpp, .gadget, .hta, .jar, .msu, .paf.exe, .pwz, .thm, .vbs, .exe, .msi, .bat, .cmd, .com, .pif, .scr, .vb, .vbe, .js, .jse, .ws, .wsf, .wsh, .ps1, .psm1, .psd1, .ps1xml, .psc1, .scf, .lnk
Исполняемый файл	.rc, .p, .d, .asc, .bas, .cbl, .vbp, .iwb, .pb, .yml, .pika, .s19, .xt, .suo, .fsproj, .pbj, .pbxuser, .pyw, .xq, .cd, .sb, .sb2, .ise, .kv, .cod, .nib, .pwn, .b, .hpp, .apa, .bet, .bluej, .erb, .fxc, .m4, .owl, .sma, .trx, .vc, .def, .xap, .o, .pas, .qpr, .resources, .vbproj, .vbx, .xib, .md, .ccc, .wwp, .ss, .asf, .asm, .asp, .cfm, .dot, .dtd, .fla, .ged, .gv, .icl, .jse, .lua, .m, .mb, .mdf, .mod, .msp, .obj, .pkg, .po, .pot, .pub, .rss, .sln, .so, .vbe, .vbs, .vc4, .vcproj, .vcxproj, .wsc, .xcodeproj, .xsd, .c, .class, .cpp, .cs, .css, .go, .h, .htaccess, .html, .java, .json, .kml, .sql, .swift, .vb, .yaml, .sh, .bat, .cmd, .ps1, .py, .pl, .rb, .js, .ts, .php, .jsp, .aspx, .cgi, .jar
Образ диска	.img, .cue, .dsk, .vmdk, .vhd, .vhdx, .tc, .crypt, .dmgpart, .sparsebundle, .xva, .cif, .pqi, .udf, .fvd, .arc, .fcd, .gi, .giz, .ima, .udif, .vdi, .vim, .wim, .b5t, .b6t, .bin, .bwi, .bwt, .ccd, .cdi, .cdr, .dmg, .i00, .i01, .i02, .iso, .isz, .md0, .md1, .md2, .mdf, .mds, .nrg, .pdi, .po, .rom, .sub, .tib, .toast, .vc4, .vcd
Журнал событий Windows	.evt, .evtx, .log, .txt, .xml
Файл реестра Windows	.reg, .dat, .pol, .hiv, .srd
Шрифт	.bin, .ps, .sfd, .fnt, .afm, .ttf, .otf, .woff, .woff2, .eot, .svg, .dfont, .pfa, .pfb, .pfm, .fon, .suit, .bdf, .pcf, .snf, .ufo, .lib, .cff
Файл базы данных	.bup, .csv, .json, .xml, .myi, .sqlplan, .abs, .abx, .ac, .accdb, .accdc, .accde, .accdr, .accdt, .accdw, .accft, .adb, .ade, .adf, .adn, .adp, .alf, .anb, .approj, .aq, .ask, .bacpac, .bak, .btr, .caf, .cat, .cdb, .chck, .ckp, .cma, .cpd, .crypt, .dab, .dacpac, .dad, .daschema, .db, .db-journal, .db-shm, .db-wal, .db2, .db3, .dbc, .dbf, .dbs, .dbt, .dbv, .dbx, .dcb, .dct, .dcx, .ddl, .dlis, .dp1, .dqy, .dsk, .dsn, .dtsx, .dxl, .eco, .ecx, .edb, .epim, .erx, .exb, .fcd, .fdb, .fic, .frm, .ftb, .gdb, .grdb, .gwi, .hdb, .his, .ib, .ibd, .icdb, .idb, .ihx, .ipj, .itdb, .itw, .jet, .jtx, .kdb, .lgc, .lwx, .maf, .maq, .mar, .marshal, .mas, .mav, .maw, .mdb, .mdbhtml, .mdf, .mdn, .mdt, .mfd, .mpd, .mrg, .mud, .mwb, .myd, .ndf, .nnt, .ns2, .ns3, .ns4, .nsf, .nv2, .nwdb, .nyf, .odb, .odl, .oqy, .ora, .orx, .owc, .pan, .pdb, .pdm, .pnz, .pqa, .pvoc, .qry, .qvd, .rbf, .rctd, .realm, .rod, .rsd, .sbf, .scx, .sdb, .sdc, .sdf, .sis, .spq, .sql, .sqlite, .sqlite3, .sqlitedb, .te, .temx, .tmd, .tps, .trc, .trm, .tvdb, .udb, .udl, .vis, .vvv, .wdb, .wmdb, .wrk, .xdb, .xld, .xmlff

Подготовка данных для передачи в систему ГосСОПКА

Вы можете получить данные обнаружений и событий NDR в формате, допустимом для импорта в систему ГосСОПКА, с помощью утилиты kata-alert-export. Утилита входит в комплект поставки Kaspersky Anti Targeted Attack Platform.

В результате работы утилиты для каждого обнаружения и события NDR создаются отдельные файлы формата XML версии 1.0 (кодировка UTF-8) с данными об этом обнаружении или событии за указанный период времени.

Подготовка данных обнаружений для передачи в систему ГосСОПКА

Для подготовки данных обнаружений, которые вы хотите передать в систему ГосСОПКА, достаточно запустить утилиту.

Подготовка данных событий NDR для передачи в систему ГосСОПКА

Процесс подготовки данных событий NDR для передачи в систему ГосСОПКА состоит из следующих этапов:

1. Создание коннектора в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

   Создайте коннектор типа Generic и сохраните файл свертки для него.

   Если вы используете режим распределенного решения или мультитенантности, на шаге 4c инструкции по созданию коннектора вам нужно указать IP-адрес того сервера PCN или SCN, с которого вы хотите получить данные. Если вы хотите получить данные с нескольких серверов Central Node, вам нужно создать коннектор для каждого из этих серверов.

   Если компонент Central Node развернут в виде кластера, при создании коннектора вы можете указать IP-адрес любого сервера кластера.

2. Запуск утилиты.

   Запустите утилиту на сервере Central Node, IP-адрес которого вы указали при создании коннектора на шаге 4c инструкции по созданию коннектора.

Особенности записи данных о событиях NDR и обнаружениях

Для обнаружений, которые создаются на основе событий, зарегистрированных в результате проверки технологией EXT, в качестве технологии проверки указывается **Aggregated Alerts**.

Запуск утилиты для подготовки данных к передаче в систему ГосСОПКА

Чтобы запустить утилиту для подготовки данных к передаче в систему ГосСОПКА:

1. Поместите архив gossopka_alert_exporter.tar.gz на сервер Central Node, с которого вы хотите получить данные.

2. Войдите в консоль управления этого сервера Central Node по протоколу SSH или через терминал.

3. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке компонента.

   Отобразится меню администратора компонента приложения.

4. В меню администратора приложения выберите режим **Technical Support Mode**.

5. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

6. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **ENTER**.

7. Выполните команду:

   ```
   sudo -i
   ```

8. Распакуйте архив с утилитой, выполнив команду:

   ```
   tar -xzvf gossopka_alert_exporter.tar.gz
   ```

9. Если вы хотите получить данные обнаружений, выполните команду:

   ```
   python3 export_main.py -s <yyyy-mm-ddThh:mm:ss> -b <yyyy-mm-ddThh:mm:ss>
   ```

10. Если вы хотите получить данные обнаружений и событий NDR, выполните команду:

    ```
    python3 export_main.py -s <yyyy-mm-ddThh:mm:ss> -b <yyyy-mm-ddThh:mm:ss> -c <путь к файлу свертки>
    ```

    Утилита будет запущена.

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Описание параметров запуска утилиты

Обязательный параметр	Параметр	Описание
Нет	`--help`	Страница помощи.
Нет	`-m <id>`	Идентификатор производителя (module_id). По умолчанию установлено значение `50`. Перед запуском утилиты необходимо уточнить у специалистов центра ГосСОПКА актуальный идентификатор, присвоенный "Лаборатории Касперского".
Да	`-s <yyyy-mm-ddThh:mm:ss>`	Начало временного интервала, за который необходимо получить информацию.

Обязательный параметр	Параметр	Описание
Да	`-b <yyyy-mm-ddThh:mm:ss>`	Конец временного интервала, за который необходимо получить информацию.
Нет	`-o <путь к директории>`	Путь к директории, в которой будут сохраняться файлы. По умолчанию установлено значение `/tmp`.
Да, если вы хотите получить данные событий NDR	`-c <имя файла свертки, включая расширение>`	Имя файла свертки (включая расширение), полученного в процессе создания коннектора.
Да, если вы хотите получить данные событий NDR	`-p <пароль к файлу свертки>`	Пароль к файлу свертки, указанный в процессе создания коннектора.
Нет	`-z <смещение относительно времени UTC в минутах>`	Смещение относительно времени UTC в минутах. По умолчанию установлено значение 180 (+3 часа).

Пример команды для запуска утилиты с параметрами:

```
python3 export_main.py -s 2025-01-01T00:00:00 -b 2025-05-23T00:00:00 -c test.zip -o /home/administrator/export
```

В результате работы утилиты в выбранную директорию помещаются следующие файлы:

- Файл с названием Alert<идентификатор обнаружения>.xml.
- Файл с названием Event<идентификатор события>.xml.

Для каждого обнаружения и события создается отдельный файл. Если в директории уже есть файл с идентичным именем, он перезаписывается.

Отправка уведомлений

Пользователи с ролями **Администратор**, **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** могут настроить отправку уведомлений на один или несколько адресов электронной почты.

Вы можете создать уведомления об обнаружениях и о работоспособности системы.

Уведомления содержат ссылку на веб-интерфейс приложения. Убедитесь, что имя, назначенное серверу Central Node для использования DNS-серверами, указано верно и резолвится DNS-сервером. Если имя указано неверно или оно не резолвится DNS-сервером, ссылка на веб-интерфейс в уведомлении будет некорректной.

Пользователи с ролью **Аудитор** могут просматривать список правил для отправки уведомлений, свойства выбранного правила и параметры соединения с почтовым сервером без возможности редактирования.

Для корректной отправки уведомлений на адрес электронной почты необходимо предварительно настроить параметры соединения с почтовым сервером. Настройку соединения выполняет **Администратор**.

Просмотр таблицы правил для отправки уведомлений

Правила для отправки уведомлений отображаются в разделе **Параметры**, подразделе **Уведомления** окна веб-интерфейса приложения.

Таблица правил для отправки уведомлений содержит следующую информацию:

- **Тип** – тип правила для отправки уведомлений.

  Возможны следующие типы правил:

  - **Обнаружения** – правило для отправки уведомления об обнаружениях.
  - **Здоровье компонентов** – правило для отправки уведомления о работе компонентов приложения.
- **Тема** – тема сообщения с уведомлением.
- **Кому** – адреса электронной почты, на которые отправляются уведомления.
- **Состояние** – состояние правила для отправки уведомления.

Создание правила для отправки уведомлений об обнаружениях

Чтобы создать правило для отправки уведомлений об обнаружениях:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
4. В поле **Кому** введите один или несколько адресов электронной почты, на которые вы хотите настроить отправку уведомлений.

   Вы можете ввести несколько адресов электронной почты через запятую.
5. В поле **Тема** введите тему сообщения с уведомлением.
6. Если вы хотите, чтобы приложение подставляло важность обнаружения в тему сообщения, добавьте в поле **Тема** макрос `%importance%`.
7. В поле **Тип уведомления** выберите **Обнаружения**.
8. В раскрывающемся списке **Важность обнаружения** выберите минимальное значение важности обнаружений, о которых вы хотите настроить отправку уведомлений.

   Например, вы можете настроить отправку уведомлений об обнаружениях только высокой степени важности или только средней и высокой степени важности.
9. В поле **Адрес источника или назначения** введите IP-адрес и маску сети, если вы хотите настроить отправку уведомлений об обнаружениях, связанных с определенным IP-адресом или адресом подсети источника или назначения.
10. В поле **Email** введите адрес электронной почты, если вы хотите настроить отправку уведомлений об обнаружениях, связанных с определенным адресом отправителя или получателя сообщений электронной почты.
11. В блоке параметров **Компоненты** установите флажки рядом с названиями одной или нескольких технологий, если вы хотите настроить отправку уведомлений об обнаружениях, выполненных определенными технологиями.
12. Нажмите на кнопку **Добавить**.

Правило для отправки уведомлений об обнаружениях будет добавлено в список правил. Чтобы уведомления приходили на указанный адрес электронной почты, требуется включить правило отправки уведомлений. Уведомления отправляются однократно по всем указанным в правиле адресам электронной почты.

Для пользователей с ролью **Администратор** и **Аудитор** функция создания правил для отправки уведомлений об обнаружениях недоступна.

В режиме распределенного решения уведомления требуется создать отдельно для каждого подчиненного сервера (*Secondary Central Node*, *SCN*).

Создание правила для отправки уведомлений о работе компонентов приложения

Чтобы создать правило для отправки уведомлений о работе компонентов приложения:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
4. В поле **Кому** введите один или несколько адресов электронной почты, на которые вы хотите настроить отправку уведомлений.

   Вы можете ввести несколько адресов электронной почты через запятую.
5. В поле **Тема** введите тему сообщения с уведомлением.
6. Если вы хотите, чтобы приложение указывало важность обнаружения в теме сообщения, добавьте в поле **Тема** макрос `%importance%`.
7. В поле **Тип уведомления** выберите **Здоровье компонентов**.
8. В блоке параметров **Компоненты** установите флажки рядом с названиями тех функциональных областей приложения, о которых вы хотите получать уведомления.
9. Нажмите на кнопку **Добавить**.

Правило для отправки уведомлений о работе компонентов приложения будет добавлено в список правил. Чтобы уведомления приходили на указанный адрес электронной почты, требуется включить правило отправки уведомлений. Уведомления отправляются однократно по всем указанным в правиле адресам электронной почты.

Для пользователей с ролью **Аудитор** функция создания правил для отправки уведомлений о работе приложения недоступна.

В режиме распределенного решения уведомления настраиваются отдельно для каждого подчиненного сервера (*Secondary Central Node*, *SCN*).

Включение и отключение правила для отправки уведомлений

Чтобы включить или отключить правило для отправки уведомлений об обнаружениях:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. В столбце **Состояние** включите или отключите правило для отправки уведомлений с помощью переключателя рядом с этим правилом.

Состояние правила для отправки уведомлений об обнаружениях будет изменено.

Для пользователей с ролью **Аудитор** функция включения и отключения правил для отправки уведомлений недоступна.

Изменение правила для отправки уведомлений

Чтобы изменить правило для отправки уведомлений:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. В списке правил для отправки уведомлений выберите правило, которое вы хотите изменить.

   Откроется окно **Изменить правило**.
4. Внесите необходимые изменения.
5. Нажмите на кнопку **Сохранить**.

Правило для отправки уведомлений будет изменено.

Для пользователей с ролью **Аудитор** функция изменения правил для отправки уведомлений недоступна.

Удаление правила для отправки уведомлений

Чтобы удалить правило для отправки уведомлений:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. Установите флажок слева от названия каждого правила, которое вы хотите удалить.

   Если вы хотите удалить все правила, установите флажок над списком.
4. Нажмите на кнопку **Удалить** в нижней части окна.
5. В окне подтверждения нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Для пользователей с ролью **Аудитор** функция удаления правил для отправки уведомлений недоступна.

Фильтрация и поиск правил отправки уведомлений по типу правила

Чтобы отфильтровать или найти правила отправки уведомлений по типу правила:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. В таблице правил для отправки уведомлений нажмите на значок ⬚.

   Откроется окно настройки фильтрации.
4. Выберите один из следующих вариантов:

   - **Все**.
   - **Алерты**.
   - **Здоровье компонентов**.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск правил отправки уведомлений по теме уведомлений

Чтобы отфильтровать или найти правила отправки уведомлений по теме уведомлений:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. По ссылке **Тема** откройте окно настройки фильтрации.
4. Введите один или несколько символов темы уведомлений.
5. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

   В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск правил отправки уведомлений по адресу электронной почты

Чтобы отфильтровать или найти правила отправки уведомлений по адресу электронной почты, на который они отправляются:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. По ссылке **Кому** откройте окно настройки фильтрации.
4. Введите один или несколько символов адреса электронной почты.
5. Нажмите на кнопку **Применить**.

   В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск правил отправки уведомлений по их состоянию

Чтобы отфильтровать или найти правила отправки уведомлений по их состоянию:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. По ссылке **Состояние** откройте окно настройки фильтрации.
4. Установите один или несколько флажков рядом со значениями состояний:
   - **Включено**.
   - **Выключено**.
5. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

   В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил отправки уведомлений

Чтобы сбросить фильтр правил отправки уведомлений по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. Нажмите на кнопку справа от того заголовка столбца таблицы правил отправки уведомлений, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

   Выбранные фильтры будут сброшены.

   В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Управление журналами

Этот раздел содержит информацию об управлении журналами Kaspersky Anti Targeted Attack Platform.

В веб-интерфейсе Kaspersky Anti Targeted Attack Platform вы можете управлять следующими журналами:

- Журнал активности пользователей. Управлять журналом могут пользователи с ролью **Администратор**. Пользователи с ролью **Аудитор** могут скачивать журнал.
- Журнал активности пользователей функциональности NDR. Управлять журналом могут пользователи с ролью **Администратор**. Пользователи с ролью **Аудитор** могут просматривать журнал.

Управление журналом активности пользователей приложения

Некоторые действия пользователей в веб-интерфейсе приложения могут привести к ошибкам в работе Kaspersky Anti Targeted Attack Platform. Вы можете включить запись информации о действиях пользователей в веб-интерфейсе приложения в журнал и при необходимости просмотреть эту информацию, скачав файлы журнала.

Информация о действиях пользователей в веб-интерфейсе компонента Sandbox и меню администратора компонента Sensor записывается в журналы Sandbox и Sensor.

Включение и отключение записи информации в журнал активности

Чтобы включить или отключить запись информации о действиях пользователей в веб-интерфейсе Kaspersky Anti Targeted Attack Platform в журнал активности:

1. В окне веб-интерфейса приложения перейдите в раздел **Журналы**, подраздел **Активность пользователей**.
2. Выполните одно из следующих действий:
   - Установите переключатель **Запись в журнал** в положение **Включено**, если хотите включить запись информации о действиях пользователей в веб-интерфейсе приложения в журнал активности.
   - Установите переключатель **Запись в журнал** в положение **Выключено**, если хотите отключить запись информации о действиях пользователей в веб-интерфейсе приложения в журнал активности.

     По умолчанию функция включена.

Информация о действиях пользователей записывается в файл user_actions.log, который хранится на сервере с компонентом Central Node в директории /data/storage/volumes/siem_proxy/log-user-actions/. По умолчанию записи в этом файле хранятся 90 дней, после чего удаляются.

Для просмотра записей в журнале активности вам нужно скачать файл user_actions.log.

Вы можете настроить запись информации о действиях пользователей в веб-интерфейсе приложения в удаленный журнал. Удаленный журнал хранится на сервере, на котором установлена SIEM-система. Для записи в удаленный журнал должны быть настроены параметры интеграции с SIEM-системой.

В режиме распределенного решения информация о действиях пользователей в веб-интерфейсе записывается в журнал того сервера, в веб-интерфейсе которого работают пользователи. Информация о действиях пользователей сервера PCN, влияющих на параметры серверов SCN, записывается в журнал сервера PCN.

Пользователи с ролью **Аудитор** могут только просматривать настройки записи информации в журнал активности.

Скачивание файла журнала активности

Чтобы скачать файл журнала активности:

1. В окне веб-интерфейса приложения перейдите в раздел **Журналы**, подраздел **Активность пользователей**.
2. Нажмите на кнопку **Скачать**.

Файл журнала будет сохранен на ваш локальный компьютер в папку загрузки браузера. Файл загружается в формате ZIP-архива.

В режиме распределенного решения вы можете скачать файл журнала активности только для того сервера, в веб-интерфейсе которого работаете.

Записи в журнале активности пользователей приложения

В заголовке каждого сообщения содержится следующая информация:

- Версия формата.

  Номер текущей версии: `0`. Текущее значение поля: `CEF:0`.

- Производитель.

  Текущее значение поля: `AO Kaspersky Lab`.

- Название приложения.

  Текущее значение поля: `Kaspersky Anti Targeted Attack Platform`.

- Версия приложения.

  Текущее значение поля: 7.1.1.531.

- Тип события.

  См. таблицу ниже.

- Наименование события.

  См. таблицу ниже.

- Важность события.

  Текущее значение поля: `Low`.

  Пример:
  ```
  CEF:0|AO Kaspersky Lab|Kaspersky Anti Targeted Attack Platform|7.1.1.531|tasks|Managing tasks|Low|
  ```

Все поля тела CEF-сообщения представлены в формате `"<ключ>=<значение>"`. Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Тип события	Наименование и описание события	Ключ и описание его значения
`alerts`	`User actions performed on alerts` Операции с алертами.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>. • `cs1label` = <пользователь, на которого назначен алерт>. • `externalId` = <ID алерта>.
`ep`	`Managing hosts with the Endpoint Agent component` Операции с хостами, на которых установлен компонент Endpoint Agent.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>. • `cs1label` = <имя хоста с компонентом Endpoint Agent>.
`storage`	`Managing objects in Storage and Quarantine` Операции с объектами в Хранилище и на карантине.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>. • `cs1label` = <имя файла, помещенного в Хранилище или на карантин>.
`sensors`	`Managing the Sensor component` Подключение компонента Sensor к серверу Central Node, изменение настроек компонента.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`sb`	`Configuring integration with the Sandbox component` Подключение компонента Sandbox к серверу Central Node.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`ex_integration`	`Configuring integration with external systems` Настройки интеграции с внешними системами.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`ksn_kpsn_mdr`	`Participation in KSN, KPSN and MDR` Настройка участия в Kaspersky Security Network, включение / отключение использования Kaspersky Private Security Network и настройка интеграции с Kaspersky Managed Detection and Response.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`yara`	`Managing YARA rules` Операции с правилами YARA.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>. • `cs1label` = <имя загружаемого файла>.

Тип события	Наименование и описание события	Ключ и описание его значения
`ioc`	`Managing indicator of compromise` Операции с правилами IOC.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`ids`	`Managing IDS rules` Операции с правилами IDS.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`taa`	`Managing TAA rules` Операции с правилами TAA (IOA).	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`sb_rules`	`Managing Sandbox rules` Операции с правилами Sandbox.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`prevention`	`Managing prevention rules` Операции с правилами запрета.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`exclusions`	`Managing scan exclusions` Операции с правилами исключений из проверки.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`tasks`	`Managing tasks` Операции с задачами.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`network_isolation`	`Network isolation of Endpoint Agent hosts` Сетевая изоляция хостов Endpoint Agent.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`settings`	`Settings` Изменение параметров сервера Central Node	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`vip`	`Managing rules for assigning the VIP status` Операции с правилами назначения алертам статуса VIP.	• `dvchost` = <имя хоста Central Node>.

Тип события	Наименование и описание события	Ключ и описание его значения
		• `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`report`	`Managing reports` Операции с отчетами.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>. • `cs1label` = <имя отчета или шаблона отчета>.
`mt`	`Managing CN, PCN and SCN servers` Изменение параметров сервера Primary Central Node и Secondary Central Node в режиме распределенного решения и мультитенантности.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`user_account`	`Managing user accounts` Действия с учетными записями пользователей.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>. • `cs1label` = <имя пользователя, чья учетная запись была создана или изменена>. • `cn1` = <число неуспешных попыток авторизации>.
	`Count of unsuccessful authorization attempts exceeded` Превышение количества неуспешных попыток авторизации.	
`notifications`	`Sending notifications` Настройка отправки уведомлений на электронную почту.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`license`	`License` Управление лицензионным ключом.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`system_health`	`System health` Проверка работоспособности компонентов приложения.	• `dvchost` = <имя хоста Central Node>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>. • `cs1label` = <объект компонента>. • `msg` = <результат проверки>

Если одна операция проводится с более чем 30 объектами одновременно, в журнал записывается одно сообщение об этой операции. В сообщении указывается информация об операции и количество объектов, с которыми она была проведена.

Управление журналом активности пользователей NDR

Этот раздел содержит информацию об управлении журналами функциональности NDR.

Управлять журналом могут пользователи с ролью **Администратор**. Пользователи с ролью **Аудитор** могут просматривать журнал.

Журналы доступны при использовании любого типа лицензионного ключа Kaspersky Anti Targeted Attack Platform.

Управление параметрами хранения журналов

Вы можете изменить параметры хранения записей журналов в базе данных Central Node.

Чтобы изменить параметры хранения журналов:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Серверы Sensor**.
3. Выберите карточку сервера Central Node.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для изменения параметров сервера.
5. На вкладке **Общие** настройте следующие параметры в блоках параметров **События, Записи аудита** и **Сообщения программы**:

   a. С помощью параметра **Макс. объем** задайте ограничение занимаемого объема для хранения записей. Вы можете выбрать единицу измерения для указанного значения: **МБ** или **ГБ**.

   При изменении значения параметра обратите внимание на оцениваемое максимальное количество записей для указанного объема. Также вам нужно учитывать, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для узла.

   b. При необходимости с помощью параметра **Время хранения (дней)** включите ограничение на минимальное время хранения записей и укажите нужное количество дней для хранения.
6. Нажмите на кнопку **Сохранить**.

Параметры хранения журналов будут настроены.

Включение и выключение аудита действий пользователей

Вы можете включать и выключать аудит действий пользователей функциональности NDR.

По умолчанию аудит действий пользователей включен.

Чтобы включить или выключить аудит действий пользователей:

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Перейдите в раздел **Журналы**, подраздел **Аудит**.
3. Включите или выключите аудит действий пользователей с помощью переключателя **Аудит действий пользователей** в панели инструментов.
4. Дождитесь применения изменений. До завершения перевода в другое состояние переключатель недоступен.

Аудит действий пользователей будет включен или выключен.

Просмотр записей аудита действий пользователей

Kaspersky Anti Targeted Attack Platform может сохранять информацию о действиях, совершенных пользователями функциональности NDR. Информация сохраняется в журнале аудита, если включен аудит действий пользователей.

Вы можете просматривать записи аудита при подключении к серверу Central Node через веб-интерфейс. При необходимости вы также можете настроить отправку записей аудита в сторонние системы через коннекторы.

Просматривать записи аудита могут только пользователи с ролью Администратор.

Чтобы просмотреть записи аудита:

1. Подключитесь к серверу Central Node через веб-интерфейс.
2. Выберите раздел **Журналы**, подраздел **Аудит**.

В таблице отобразятся записи аудита, которые соответствуют заданным параметрам фильтрации и поиска.

Параметры записей аудита отображаются в следующих столбцах таблицы:

- **Дата и время**.

  Дата и время регистрации данных о действии пользователя.

- **Действие**.

  Зарегистрированное действие, которое совершил пользователь.

- **Результат**.

  Результат выполнения зарегистрированного действия (успешно или неуспешно).

- **Пользователь**.

  Имя пользователя, который совершил зарегистрированное действие.

- **Узел пользователя**.

  IP-адрес узла, на котором совершено зарегистрированное действие.

- **Описание**.

  Дополнительные сведения о зарегистрированном действии.

При просмотре таблицы записей аудита вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Настройка максимального объема хранения журналов трассировки

Данные о работе функциональности NDR записываются в журналы трассировки. Вы можете ограничить объем для хранения этих журналов. В этом случае при достижении ограничения в директории `/var/log/kaspersky` удаляются старые файлы журналов трассировки.

Управлять параметрами хранения журналов могут пользователи с ролью **Администратор**. Пользователи с ролью **Аудитор** могут просматривать эти параметры.

Чтобы ограничить объем хранения журналов трассировки:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor.**
3. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.
4. Откроется окно с информацией о компоненте.
5. Нажмите на кнопку **Изменить**.
6. Перейдите на вкладку **Общие**.
7. В поле **Данные трассировки** с помощью параметра **Макс. объем** задайте ограничение занимаемого объема для хранения журналов. Вы можете выбрать единицу измерения для указанного значения: **МБ** или **ГБ**.

Объем хранения журналов трассировки будет ограничен.

Настройка максимального объема хранения журналов статистики

В журналы статистики записываются данные метрик функциональности NDR, например, количество принятых сетевых пакетов. Вы можете ограничить объем для хранения этих журналов. В этом случае при достижении ограничения в директории `var/log/kaspersky` удаляются старые файлы журналов статистики.

Управлять параметрами хранения журналов могут пользователи с ролью **Администратор**. Пользователи с ролью **Аудитор** могут просматривать эти параметры.

Чтобы ограничить объем хранения журналов статистики:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor.**
3. Наведите курсор мыши на карточку нужного компонента Sensor и нажмите на нее левой кнопкой мыши.
4. Откроется окно с информацией о компоненте.
5. Нажмите на кнопку **Изменить**.
6. Перейдите на вкладку **Общие**.
7. В поле **Данные статистики** с помощью параметра **Макс. объем** задайте ограничение занимаемого объема для хранения журналов. Вы можете выбрать единицу измерения для указанного значения: **МБ** или **ГБ**.

Объем хранения журналов статистики будет ограничен.

Журнал активности пользователей Sensor

Информация о действиях пользователей в меню администратора компонента записывается в журнал активности пользователей Sensor – admin_menu.log.

Вы можете скачать файл журнала активности пользователей Sensor, следуя инструкции в разделе *Скачивание журналов Kaspersky Anti Targeted Attack Platform*. В результате выполнения шагов инструкции в выбранную вами директорию будет помещен архив collect--<дата выгрузки архива>.tar.gz. Журнал активности пользователей Sensor располагается внутри этого архива в директории admin_menu.log в директории /var/log/kaspersky/admin_menu/.

Записи о действиях пользователей в меню администратора компонента Sensor

Записи в журнале пользовательских действий в меню администратора компонента Sensor (admin_menu.log) сгруппированы по уровням.

На уровне INFO записывается информация о действиях пользователей в меню администратора компонента.

Пример записи о событии на уровне INFO:

```
June 18 20:45:46 1 admin-menu - INFO Menu item pressed label=[Example ...]
```

На уровне WARNING записывается информация о событии, которое произошло в результате выполнения действий, описанных на уровне INFO. Информация на этом уровне представлена в формате CEF-сообщения.

В заголовке каждого сообщения содержится следующая информация:

- Версия формата.

  Номер текущей версии: `0`. Текущее значение поля: `CEF:0`.

- Производитель.

  Текущее значение поля: `AO Kaspersky Lab`.

- Название приложения.

  Текущее значение поля: `Kaspersky Anti Targeted Attack Platform`.

- Версия приложения.

  Текущее значение поля: 7.1.1.531.

- Тип события.

  См. таблицу ниже.

- Наименование события.

  См. таблицу ниже.

- Важность события.

  Текущее значение поля: `Low`.

  Пример заголовка сообщения:
  `CEF:0|AO Kaspersky Lab|Kaspersky Anti Targeted Attack Platform|7.1.1.531|user_account|Managing user accounts|Low|`

Все поля тела CEF-сообщения представлены в формате `"<ключ>=<значение>"`. Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Информация о событии в CEF-сообщениях

Тип события	Наименование и описание события	Ключ и описание его значения
`sensors`	`Managing the Sensor component` Управление сервером, изменение параметров компонента.	• `dvchost` = <имя сервера с компонентом Sensor>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`settings`	`Settings` Изменение параметров даты и времени сервера, управление журналами.	• `dvchost` = <имя сервера с компонентом Sensor>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.
`user_account`	`Managing user accounts` Изменение пароля учетной записи администратора, начало и завершение пользовательской сессии, вход в режим Technical Support Mode.	• `dvchost` = <имя сервера с компонентом Sensor>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `suser` = <имя пользователя>. • `cs1` = <тип события>.

Журналы Sandbox

Компонент Sandbox записывает в журналы информацию двух типов:

- В системный журнал записывается подробная информация о событиях в Sandbox.
- В журнал активности пользователей записывается информация о действиях пользователей Sandbox в веб-интерфейсе.

Вы можете скачать как системный журнал, так и журнал активности пользователей.

Скачивание системного журнала Sandbox

Данные в системном журнале Sandbox хранятся в открытом незашифрованном виде. Данные хранятся за последние 7 дней.

Чтобы скачать системный журнал Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Системные журналы** нажмите на кнопку **Скачать**.

   Загрузка файла на ваш компьютер может начаться с задержкой. Дождитесь начала загрузки файла, не обновляйте страницу и не нажимайте на кнопку **Скачать** повторно. Скачивание системного журнала Sandbox может занимать много времени.

   Файл журнала будет сохранен на ваш локальный компьютер в папку загрузки браузера.

Скачивание журнала активности пользователей Sandbox

В журнал активности пользователей записывается информация о действиях пользователей в веб-интерфейсе Sandbox. По умолчанию данные в журнале хранятся в течение 90 дней.

Чтобы скачать журнал активности пользователей Sandbox:

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Журнал активности пользователей** нажмите на кнопку **Скачать**.

   Файл журнала user_actions.log будет сохранен на ваш локальный компьютер в папку загрузки браузера.

Записи в журнале активности пользователей Sandbox

Журнал активности пользователей Sandbox содержит записи в формате CEF (CEF-сообщения). По записи в журнале можно понять, какое событие произошло вследствие действий пользователя.

Пример записи об установке образа виртуальной машины:

```
CEF:0|AO Kaspersky Lab|Kaspersky Anti Targeted Attack Platform (Sandbox)|7.1.0.530|vm|Managing virtual machines|Low| dvs=<IP> deviceExternalId=ubuntu-server eventId=1965096788380487496 rt=Apr 25 2025 04:59:16 src=<IP> suser=admin cs1=installing the default image cs1label=CentOS7_x64-1.0.0.19888
```

Пример выше содержит три группы полей:

- `CEF:0|AO Kaspersky Lab|Kaspersky Anti Targeted Attack Platform (Sandbox)|7.1.0.530|vm|Managing virtual machines|Low|` – поля заголовка.
- `dvs=<IP> deviceExternalId=ubuntu-server eventId=1965096788380487496 rt=Apr 25 2025 04:59:16 src=<IP> suser=admin cs1=installing the default image` – поля тела CEF-сообщения, общие для всех записей.
- `cs1label=CentOS7_x64-1.0.0.19888` – поле, специфичное для действий, имеющих объект. Например, объектом действия "установка образа виртуальной машины" является образ виртуальной машины, и в поле `cs1label` указывается имя этого образа.

Поля заголовка

В заголовке каждого сообщения содержится следующая информация:

- Версия формата.

  Номер текущей версии: `0`. Текущее значение поля: `CEF:0`.

- Производитель.

  Текущее значение поля: `AO Kaspersky Lab`.

- Название приложения.

  Текущее значение поля: `Kaspersky Anti Targeted Attack Platform`.

- Версия приложения.

  Текущее значение поля: 7.1.1.531.

- Тип события.

  Может содержать одно из следующих значений:

  - `user_account`

    События, связанные с учетными записями пользователей Sandbox.

  - `settings`

    События, связанные с настройками Sandbox.

  - `kata`

    События, связанные с соединением между Sandbox и Central Node.

  - `vm`

    События, связанные с виртуальными образами операционных систем, развернутых в Sandbox.

- Наименование события, указанное в заголовке.

Может содержать одно из следующих значений:

- `Managing user accounts`

  Действия с учетными записями пользователей. Относится к типу `user_account`.

- `Count of unsuccessful authorization attempts exceeded`

  Превышение количества неуспешных попыток авторизации. Относится к типу `user_account`.

- `Settings`

  Изменение параметров сервера Sandbox. Относится к типу `settings`.

- `Configuring integration with KATA Central Node`

  Настройка интеграции с Central Node. Относится к типу `kata`.

- `Managing virtual machines`

  Действия с виртуальными машинами. Относится к типу `vm`.

- Важность события.

  Текущее значение поля: `Low`.

Общие поля для всех событий

Поля тела CEF-сообщения представлены в формате `"<ключ>=<значение>"`. В каждом CEF-сообщении имеются следующие поля:

- `dvs`

  IP-адрес сервера Sandbox.

- `device external ID`

  Имя сервера Sandbox.

- `eventId`

  ID события.

- `rt`

  Дата и время события.

- `src`

  IP-адрес пользователя, выполнившего действие.

- `suser`

  Имя пользователя, выполнившего действие.

- `cs1`

  Событие (см. таблицу ниже).

Специфические поля событий

События и специфические поля

Событие, указанное в поле cs1	Специфические поля события
Managing user accounts	
changing the administrator password	cs1label Имя пользователя, чей пароль был изменен.
log on	cs1label Имя пользователя, выполнившего авторизацию.
log off	cs1label Имя пользователя, завершившего сессию.
Count of unsuccessful authorization attempts exceeded	
count of unsuccessful authorization attempts	cs1label Имя пользователя, которому не удалось авторизоваться. cn1 Количество неуспешных попыток авторизации.
Settings	
• assigning the server name to be used by DNS servers • configuring DNS settings • configuring settings of the management interface • configuring settings of the network interface for internet access of processed objects • configuring the route settings • configuring proxy server connection settings • configuring the date and time on the server • configuring the time zone on the server • configuring the synchronization with NTP servers	cs1label Имя сервера, параметры которого были изменены.
• saving the configuration • restoring the configuration	cs1label Имя сервера, параметры которого были сохранены или восстановлены.
• restarting the server • powering off the server	cs1label Имя сервера, который был перезагружен или выключен.
• downloading the logs • downloading the user actions log	cs1label Имя сервера, с которого были скачаны файлы журналов.
• selecting a database update source • updating database manually	cs1label Имя сервера, на котором были обновлены антивирусные базы или изменен источник обновлений.
setting the maximum number of virtual machines	cs1label Количество виртуальных машин, которое было задано.
• enabling counting of unsuccessful authorization attempts • disabling counting of unsuccessful authorization attempts	cs1label Имя сервера, на котором включен или выключен подсчет неуспешных попыток авторизации.
modifying the counting period for unsuccessful authorization attempts	cs1label Имя сервера, на котором изменен период подсчета неуспешных попыток авторизации. cn1 Период подсчета неуспешных попыток авторизации, в минутах.

Событие, указанное в поле cs1	Специфические поля события
changing user session lock time	cs1label Имя сервера, на котором изменена максимальная длительность неактивной пользовательской сессии. cn1 Максимальная длительность неактивной пользовательской сессии, в минутах.
Configuring integration with KATA Central Node	
• accepting connection to KATA Central Node • rejecting connection to KATA Central Node • removing connection to KATA Central Node	cs1label Цифровой отпечаток Central Node, с которого поступил запрос на подключение.
Managing virtual machines	
• importing the default image • deleting the default image • unpacking the default image	cs1label Имя загружаемого или удаляемого файла с образом виртуальной машины.
• installing the default image • deleting the virtual machine deployed from the default image • cancelling the default images installation	cs1label Имя образа виртуальной машины, который был развернут, удален или чья установка отменена.
• uploading ISO • removing ISO	cs1label Название загружаемого или удаляемого iso-образа.
• creating custom template • importing custom template • exporting custom template • enabling custom template • disabling custom template • stopping custom template • deleting custom template	cs1label Имя пользовательского шаблона виртуальной машины, который был создан, импортирован, экспортирован, включен, выключен, остановлен или удален.
• downloading manifest file • uploading debug symbols	Нет специфических полей.
• mounting ISO to custom template • unmounting ISO from custom template	cs1label Имя пользовательского шаблона виртуальной машины, к которому был примонтирован iso-образ или от которого был размонтирован iso-образ. cs2label Название примонтированного или размонтированного iso-образа.
• creating custom virtual machine from custom template • deleting custom virtual machine • changing the custom virtual machine status to "online" • changing the custom virtual machine status to "enabled"	cs1label Имя виртуальной машины, которая была развернута из пользовательского образа, удалена или статус которой был изменен.

Если одна операция проводится с более чем 30 объектами одновременно, в журнал записывается одно сообщение об этой операции. В сообщении указывается информация об операции и количество объектов, с которыми она была проведена.

Скачивание журналов Kaspersky Anti Targeted Attack Platform

При необходимости вы можете скачать файлы системных журналов Kaspersky Anti Targeted Attack Platform. Для этого вам нужно получить данные о работе приложения с помощью скрипта kata-collect.

Чтобы получить данные о работе приложения с помощью скрипта kata-collect:

1. Войдите в консоль управления того сервера, с которого вы хотите получить данные, по протоколу SSH или через терминал.

   Если вы используете Kaspersky Anti Targeted Attack Platform в режиме распределенного решения и мультитенантности, вам нужно выполнить шаги этой инструкции на каждом сервере Central Node. Если в инфраструктуре вашей организации есть отдельно установленные компоненты Sensor, вам также требуется выполнить шаги инструкции на серверах с этим компонентом. При развертывании приложения в виде кластера вам нужно выполнить шаги инструкции на одном любом сервере с ролью manager в Docker swarm. Для просмотра роли сервера используйте команду `$ docker node ls`.

2. В ответ на приглашение системы введите имя и пароль учетной записи администратора, заданный при установке компонента.

   Отобразится меню администратора компонента приложения.

3. В списке разделов меню администратора приложения выберите раздел **Technical Support Mode**.

4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.

6. Запустите скрипт, выполнив команду:

   ```
   sudo kata-run.sh kata-collect --output-dir <path>
   ```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Параметры для утилиты kata-collect

Обязательный параметр	Параметр	Описание
Да	`--output-dir <path>`	Создать директорию по указанному пути, где <path> – это абсолютный или относительный путь к директории, в которую будет записан архив с выгруженными данными. Если путь не был указан, архив с данными по умолчанию будет помещен в директорию /tmp/collect.
Нет	`--no-prometheus`	Пропустить подготовку и выгрузку дампа базы данных prometheus. Использование этого параметра значительно ускоряет работу скрипта.
Нет	`--no-siem-logs`	Пропустить выгрузку данных, записываемых в SIEM-систему.
Нет	`--siem-logs-range-start <YYYY-MM-DD-HH>`	Выгрузить данные, записываемые в SIEM-систему, начиная с этой даты (включительно).
Нет	`--siem-logs-range-end <YYYY-MM-DD-HH>`	Выгрузить данные, записываемые в SIEM-систему, заканчивая этой датой (включительно).

Пример:
Команда для получения данных о работе приложения с данными SIEM-системы, отфильтрованными по дате, и без базы данных prometheus:

```
sudo kata-run.sh kata-collect --output-dir <path> --no-prometheus --siem-logs-range-start <YYYY-MM-DD-HH> --siem-logs-range-end <YYYY-MM-DD-HH>
```

Когда скрипт завершит работу, в указанную директорию будет помещен архив collect--<дата выгрузки архива>.tar.gz. В этом архиве содержатся файлы системных журналов приложения.

Просмотр сообщений приложения

В журнале сообщений приложения сохраняется информация об ошибках в работе функциональности NDR и операциях, выполненных системными процессами Kaspersky Anti Targeted Attack Platform.

Вы можете просматривать сообщения приложения через веб-интерфейс. При необходимости вы также можете настроить отправку сообщений приложения в сторонние системы через коннекторы.

Просматривать сообщения приложения могут пользователи с ролью **Администратор**, **Аудитор**, **Сотрудник службы безопасности** или **Старший сотрудник службы безопасности**.

Чтобы просмотреть сообщения приложения:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. Выберите раздел **Параметры**, подраздел **Сообщения приложения**.

   В таблице отобразятся сообщения приложения, которые соответствуют заданным параметрам фильтрации и поиска.

Параметры сообщений приложения отображаются в следующих столбцах таблицы:

- **Дата и время**.

  Дата и время регистрации сообщения приложения.

- **Статус**.

  Название статуса сообщения. Для сообщений предусмотрены следующие статусы:

  - *Нормальная работа* – для информационных сообщений.
  - *Неизвестно*, *Сбой* – для сообщений о некритических сбоях в работе приложения.
  - *Серьезный сбой*, *Критический сбой*, *Неустранимый сбой* – для сообщений о нарушении работы приложения.

- **Узел**.

  Имя или IP-адрес узла, от которого поступило сообщение.

- **Системный процесс**.

  Процесс приложения, который вызвал регистрацию сообщения.

- **Сообщение**.

  Числовой идентификатор и текст сообщения.

При просмотре таблицы сообщений приложения вы можете использовать функции фильтрации, поиска и сортировки.

Настройка срока хранения системных журналов и обнаружений Kaspersky Anti Targeted Attack Platform

Вы можете настроить срок хранения некоторых журналов и данных обнаружений в базе данных компонента Central Node, а также срок хранения журналов компонентов Sensor и Sandbox. По умолчанию данные обнаружений в базе данных компонента Central Node ротируются, когда количество записей об обнаружениях, созданных в результате проверки одной технологией, достигает 1 000 000. Срок хранения журналов по умолчанию составляет 90 дней.

Настройка параметров хранения журналов компонентов Central Node и Sensor осуществляется в меню администратора компонента Central Node или Sensor. Для настройки хранения журналов компонента Sandbox используются штатные средства операционной системы.

Вы можете настроить срок хранения следующих журналов:

- Central Node или Sensor:
  - Системный журнал Syslog.
  - Журнал пользовательских действий в веб-интерфейсе приложения user_actions.log.
  - Журнал событий ядра операционной системы kern.log.
  - Журнал авторизации пользователей в веб-интерфейсе и меню администратора компонента auth.log.
- Sandbox:
  - Журнал обновлений apt-history.log.
  - Журнал аудита системных событий apt-audit.log.
  - Журнал пользовательских действий в веб-интерфейсе приложения user_actions.log.
  - Журнал авторизации пользователей в веб-интерфейсе и меню администратора компонента auth.log.

Чтобы настроить срок хранения журналов компонентов Central Node или Sensor, а также срок хранения данных обнаружений в базе данных Central Node:

1. Если вы хотите настроить срок хранения журналов и данных обнаружений в базе данных компонента Central Node, войдите в консоль управления сервером Central Node по протоколу SSH или через терминал.
2. Если вы хотите настроить срок хранения журналов компонента Sensor, войдите в консоль управления сервером Sensor по протоколу SSH или через терминал.
3. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке компонента.

   Отобразится меню администратора компонента приложения.
4. Выберите пункт **Program settings**.

5. Нажмите на клавишу **ENTER**.

   Откроется окно **Select action**.

6. Выберите **Configure storage period for detects and logs**.

7. Нажмите на клавишу **ENTER**.

   Откроется окно **Configure storage period**.

8. Выберите **Change storage period**.

   Откроется окно **Storage period**.

9. В поле **Storage period** укажите время хранения журналов в днях. Максимальный срок хранения журналов, который вы можете указать, – 10 000 дней.

   Значение по умолчанию – 90.

10. Выберите **Apply Changes**.

    Откроется окно **Apply storage period**.

11. В открывшемся окне выберите **Ок**.

Срок хранения журналов компонентов Central Node или Sensor и срок хранения данных обнаружений (при изменении параметров для компонента Central Node) будут настроены.

Чтобы изменить срок хранения журналов Sandbox:

1. Если вы хотите изменить срок хранения журналов apt-audit.log, apt-history.log, user-actions.log, откройте файл /etc/logrotate.d/apt-audit для редактирования с root-правами и укажите новое значение параметра rotate для нужного журнала.

2. Если вы хотите изменить срок хранения журнала auth.log, откройте файл /etc/logrotate.d/auth для редактирования с root-правами и укажите новое значение параметра rotate.

   Максимальный срок хранения журналов, который вы можете указать, – 10 000 дней. По умолчанию максимальный срок хранения журналов составляет 90 дней.

Срок хранения журналов компонента Sandbox будет настроен.

Просмотр информации о файлах, поступавших на проверку в Kaspersky Anti Targeted Attack Platform

При необходимости вы можете просмотреть, проходил ли файл проверку в Kaspersky Anti Targeted Attack Platform и с каким результатом завершилась проверка. Для этого вам нужно получить данные о работе приложения с помощью скрипта kata-collect.

Чтобы получить данные о работе приложения с помощью скрипта kata-collect,

выполните шаги инструкции, приведенной в разделе *Скачивание журналов Kaspersky Anti Targeted Attack Platform*.

В результате выполнения шагов инструкции в указанную директорию будет помещен архив collect--<дата выгрузки архива>tar.gz, содержащий файлы журналов Kaspersky Anti Targeted Attack Platform. Информация о файлах, поступавших на проверку, содержится в журнале, который располагается внутри этого архива в директории /logs/kaspersky/siem/log-history/. Если файл был исключен из проверки, информация о нем также будет отражена в журнале.

Вы можете найти любой файл по его имени или MD5-хешу.

Если файл был получен компонентом Sensor, вы можете найти его по следующим полям:

- Информация об источнике файла:
  - IP-адрес источника и IP-адрес назначения, если файл был получен из трафика.
  - Электронный адрес отправителя и получателя, если файл был получен по электронной почте.
  - IP-адрес и идентификатор внешней системы, если файл был получен от нее.
  - IP-адрес и имя хоста, если файл был получен с хоста Endpoint Agent.
  - Имя учетной записи пользователя, если файл был загружен в Kaspersky Anti Targeted Attack Platform вручную.
- Тип источника: span, smtp, icap, pop3, external (внешняя система), endpoint (хост Endpoint Agent), upload (файл загружен вручную).
- Для электронных писем в журнале фиксируется поле Message-ID.

Особенности записи информации о файлах

При поиске информации о файлах в журнале вам нужно учитывать следующие особенности записи информации о файлах:

- Запись информации о файле происходит два раза: при получении файла из трафика и при его проверке. Если в вашей инфраструктуре компонент Sensor установлен отдельно от Central Node, запись о получении файла будет располагаться в журнале компонента Sensor, запись о проверке файла - в журнале компонента Central Node, к которому подключен Sensor. Если компонент Central Node и Sensor установлены на одном сервере, обе записи будут располагаться в журнале Central Node.

- Для составных файлов (например, архив или письмо) в журнале записывается хеш родительского файла и имя и хеш дочернего файла, если дочерний файл был проверен одной из технологий Kaspersky Anti Targeted Attack Platform.

Примеры записей в журнале apt-history для MD5-хеша файла

Вы можете посмотреть примеры записей в журнале apt-history для MD5-хеша файла в таблице ниже.

Примеры записей в журнале apt-history для MD5-хеша файла

Запись в журнале	Значение
2024-06-11 02:37:03.645586 info apt-history: f0429d4845208857cd303df968ef545e enqueued am, priority: normal	Файл поступил на обработку по технологии Anti-Malware Engine.
2024-06-11 02:37:03.647434 info apt-history: external KSMG sensor with ip 10.0.0.0 provide file with name: File_Name 2024/2025, md5: f0429d4845208857cd303df968ef545e, msg_id: <87c13e55e789aa966089b6bf2e8c453b@localhost.localdomain>	Строка для объектов, поступивших на обработку в Kaspersky Anti Targeted Attack Platform от Kaspersky Secure Mail Gateway и Kaspersky Security для Linux Mail Server. Информация, на которую рекомендуется обратить внимание: • external KSMG sensor with ip 10.0.0.0 - IP-адрес сервера Kaspersky Secure Mail Gateway. • File_Name 2024/2025 - имя файла. • md5 - MD5-хеш проверяемого файла. • msg_id - идентификатор сообщения (message id).

2024-06-11 02:37:03.847696 info apt-history: f0429d4845208857cd303df968ef545e engine am result {verdict: CLEAN, bases_version: 202406071010, detect_time: 2024-06-11 02:37:03.841275, rescan_priority: 3, sb_hash: 77f5b6276dd9b1c534b6c9adcff86845, multitask_details: {priority: background, tasks: {pdf: 1}}, scanEngines: [sb]}	Результат обработки объекта по технологии Anti-Malware Engine. Включает статус, присвоенный объекту после проверки (CLEAN) и информацию о технологиях, по которым объект будет дополнительно проверен ("scanEngines: [sb]"). Информация, на которую рекомендуется обратить внимание: • multitask_details -сведения о задаче на проверку. • priority - приоритет проверки. Возможные значения параметра: background, must. • scanEngines - технология проверки. Возможные значения: [yr] - YARA, [sb] - Sandbox.
2024-06-11 02:37:03.886784 info apt-history: f0429d4845208857cd303df968ef545e enqueued sb: {pdf: 1}, priority: low, sb_priority: background	Задание было отправлено на обработку компоненту Sandbox. Информация, на которую рекомендуется обратить внимание: • {pdf: 1} - количество и тип объектов, отправленных на проверку. • low - приоритет обработки. Возможные значения приоритета обработки: low, medium, high. • background - тип очереди на обработку компонентом Sandbox. Возможные значения: background, must.
2024-06-11 02:37:04.179597 info apt-history: f0429d4845208857cd303df968ef545e delivered to sb, sb_hash: 77f5b6276dd9b1c534b6c9adcff86845, node: Server_Name, mtask_id: 900	Задание было отправлено на обработку компоненту Sandbox. Информация, на которую рекомендуется обратить внимание: • node:Server_Name - имя сервера с компонентом Sandbox. • mtask_id: 900 - ID задания.
2024-06-11 02:38:44.515070 info apt-history: f0429d4845208857cd303df968ef545e sb result received, sb_hash: 77f5b6276dd9b1c534b6c9adcff86845, node: Server_Name, mtask_id: 900, priority: low	Получен результат обработки объекта компонентом Sandbox.

2024-06-11 02:38:44.783370 info apt-history: f0429d4845208857cd303df968ef545e engine sb result {bases_version: 202406102122, detect_time: 2024-06-11 02:38:44.776655, verdict: SILENT, hidden: True, details: [{file: //[From WCR <test@mail.com>][Date 11 Jun 2024 03:51:21][Subj Company_Name 2024/2025]/WCR-form.pdf, images: [{verdicts_info: {ScannerVersion: 1.22.3.34, ...}, hidden: True, verdict: SILENT, sb_id: fb15ec106318b0d54babce2379d956f7, image: Win7_x64, task_id: task0, file: //[From WCR <test@mail.com>][Date 11 Jun 2024 03:51:21][Subj Company_Name 2024/2025]/WCR-form.pdf, file_id: 1, filesize: 445856, md5: 0d87eebc9676214f35046a482150e537, tracing_mode: all_events, store_artifacts: False, bases_version: 202406102122, ids_bases_version: 202406101817, version: 1.22.3.34, suspicious_log: [], network_activity: {http: [], dns: []}}], verdict: SILENT, hidden: True, priority: 150}], md5_list: [], file_list: [], sb_hash: 77f5b6276dd9b1c534b6c9adcff86845, sb_names_map: {0: {md5: , name: }, 1: {md5: 0d87eebc9676214f35046a482150e537, name: //[From WCR <test@mail.com>][Date 11 Jun 2024 03:51:21][Subj Company_Name 2024/2025]/WCR-form.pdf}, 2: {md5: 71072dd9a36d7ce560cebc533ecb3cad, name: }}}

Результат обработки объектов на всех виртуальных машинах компонента Sandbox.

Информация, на которую рекомендуется обратить внимание:

- verdict - результаты проверки файла. Формируется по результатам проверки файла на всех виртуальных машинах. Для обнаружений с результатом SILENT не создается запись в базе обнаружений.
- hidden: True - объект с этим результатом не требует дальнейшей проверки модулями Kaspersky Anti Targeted Attack Platform.
- details - информация о проверке объекта в виртуальных машинах. Включает следующие поля:
  - file - имя файла для отображения (WCR-form.pdf). В этой записи поле содержит следующую информацию:
  - From - электронный адрес отправителя.
  - Date - дата и время выполнения события.
  - Subj - тема письма.
  - images - информация о проверке объекта в виртуальных машинах.
  - verdicts_info - результаты проверки файла. Может отличаться для каждой виртуальной машины, в которой был проверен объект.
  - hidden: True - объект с этим результатом не требует дальнейшей проверки модулями Kaspersky Anti Targeted Attack Platform.
  - verdict - результаты проверки файла на виртуальной машине. Для обнаружений с результатом SILENT не создается запись в базе обнаружений.
  - image - образ, в котором был запущен файл.
  - filesize - размер файла.
  - md5 - MD5-хеш файла.

	• tracing mode: all_events - запись операций, которые выполняет файл после запуска. • suspicious log [] - запись о вредоносных действиях, которые выполнил файл. Для этого поля нет значений, так как файл не выполнял вредоносные действия. • network activity - сетевая активность, инициированная файлом. • http [] - файл не выполнял обращений по HTTP. • dns [] - файл не выполнял обращений по DNS. В полях suspicious log и network activity фиксируется только факт вредоносной активности. Если вы хотите посмотреть детали обнаружений, вы можете сделать это в веб-интерфейсе приложения. • priority - приоритет проверки. Возможные значения: 1 - высокий, 100 - стандартный, 150 - фоновая проверка. • md5_list - MD5-хеши файлов, при проверке которых были найдены обнаружения. • file_list - имена файлов, при проверке которых были найдены обнаружения. • sb_names_map - имя файла, которое будет отображаться в информации об обнаружении в веб-интерфейсе приложения.
2024-06-11 02:38:44.841529 info apt-history: New sb_detect for file alert: {id: 2720, victim: default, state: new, md5: f0429d4845208857cd303df968ef545e}	Информация о результатах обработки компонентом Sandbox сохранена в базе приложения. Служебная запись. Не является признаком наличия обнаружения в базе обнаружений приложения.

Управление приложением Kaspersky Endpoint Security для Windows

Kaspersky Endpoint Security – приложение, которое устанавливается на отдельные устройства, входящие в IT-инфраструктуру организации. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Anti Targeted Attack Platform. Приложение Kaspersky Endpoint Security также передает на сервер Kaspersky Anti Targeted Attack Platform данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

При настроенной интеграции Kaspersky Endpoint Security с Kaspersky Anti Targeted Attack Platform приложение выполняет задачи и применяет параметры, поступающие от Kaspersky Anti Targeted Attack Platform, а также отправляет на сервер с компонентом Central Node данные телеметрии с защищаемого устройства. Подробнее о действиях, которые может выполнять Kaspersky Endpoint Security при интеграции с Kaspersky Anti Targeted Attack Platform, см. в разделе *Принцип работы приложения*.

Подробнее об управлении Kaspersky Endpoint Security см. в справке приложения:

- Установка и удаление приложения.
- Лицензирование приложения.

  Для интеграции с Kaspersky Anti Targeted Attack Platform, кроме ключа активации Kaspersky Endpoint Security, вам нужно также нужно добавить ключ Kaspersky Endpoint Detection and Response (KATA) Add-on. Подробнее о лицензировании приложения см. в справке Kaspersky Endpoint Security → Интеграция с EDR (KATA).
- Интеграция с EDR (KATA).
- Настройка отправки телеметрии.
- Работа с карантином.
- Команды управления Detection and Response KATAEDR: Интеграция с EDR (KATA).

Управление приложением Kaspersky Endpoint Security для Linux

Kaspersky Endpoint Security для Linux – приложение, которое устанавливается на отдельные устройства под управлением операционных систем Linux, входящие в IT-инфраструктуру организации. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Anti Targeted Attack Platform. Приложение Kaspersky Endpoint Security для Linux также передает на сервер Kaspersky Anti Targeted Attack Platform данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

При настроенной интеграции Kaspersky Endpoint Security с Kaspersky Anti Targeted Attack Platform приложение выполняет задачи и применяет параметры, поступающие от Kaspersky Anti Targeted Attack Platform, а также отправляет на сервер с компонентом Central Node данные телеметрии с защищаемого устройства. Подробнее о действиях, которые может выполнять Kaspersky Endpoint Security при интеграции с Kaspersky Anti Targeted Attack Platform, см. в разделе *Принцип работы приложения*.

Подробнее об управлении Kaspersky Endpoint Security для Linux см. в справке приложения:

- Установка, удаление и обновление приложения.
- Управление приложением с помощью командной строки:
  - Управление лицензионным ключом: задача Лицензирование (License, ID:9).
  - Интеграция с Kaspersky Anti Targeted Attack Platform: задача Интеграция с Kaspersky Endpoint Detection and Response (KATA) (KATAEDR, ID:24).
- Управление приложением с помощью Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console:
  - Управление лицензионным ключом: см. подробнее разделы *Управление задачами в Web Console → Создание задачи* и *Параметры задач → Добавление ключа*.
  - Интеграция с Kaspersky Anti Targeted Attack Platform: см. подробнее разделы *Управление политиками в Web Console → Создание политики* и *Параметры политики → Интеграция с Kaspersky Endpoint Detection and Response (KATA)*.

Для интеграции с Kaspersky Anti Targeted Attack Platform вам не требуется добавлять дополнительный лицензионный ключ в Kaspersky Endpoint Security для Linux.

Управление приложением Kaspersky Endpoint Security для Mac

Kaspersky Endpoint Security для Mac – приложение, которое устанавливается на отдельные устройства под управлением операционных систем macOS, входящие в IT-инфраструктуру организации. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Anti Targeted Attack Platform. Приложение Kaspersky Endpoint Security для Mac также передает на сервер Kaspersky Anti Targeted Attack Platform данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

При настроенной интеграции Kaspersky Endpoint Security для Mac с Kaspersky Anti Targeted Attack Platform приложение выполняет задачи и применяет параметры, поступающие от Kaspersky Anti Targeted Attack Platform, а также отправляет на сервер с компонентом Central Node данные телеметрии с защищаемого устройства. Подробнее о действиях, которые может выполнять Kaspersky Endpoint Security для Mac при интеграции с Kaspersky Anti Targeted Attack Platform, см. в разделе *Принцип работы приложения*.

Подробнее об управлении Kaspersky Endpoint Security для Mac см. в справке приложения.

- Установка, удаление и обновление приложения.
- Лицензирование приложения.

  Для интеграции с Kaspersky Anti Targeted Attack Platform, кроме ключа активации Kaspersky Endpoint Security, вам нужно также нужно добавить ключ Kaspersky Endpoint Detection and Response (KATA) Add-on. Подробнее о лицензировании приложения см. в справке Kaspersky Endpoint Security → Расширенная настройка приложения → Endpoint Detection and Response (KATA).
- Управление приложением с помощью командной строки.
- Удаленное управление приложением через Kaspersky Security Center Web Console и Cloud Console:
  - Управление лицензионным ключом: см. подробнее разделы Создание задачи → Настройка параметров задачи Добавление ключа.
  - Интеграция с Kaspersky Anti Targeted Attack Platform: см. подробнее разделы Создание политики → Настройка параметров Detection and Response → Настройка Endpoint Detection and Response (KATA).

Резервное копирование и восстановление данных

Вы можете создать резервную копию и восстановить данные из нее в случае проблем с работоспособностью или при необходимости переустановить Kaspersky Anti Targeted Attack Platform. Поддерживается восстановление данных между Kaspersky Anti Targeted Attack Platform на базе разных операционных систем. Например, вы можете восстановить данные Kaspersky Anti Targeted Attack Platform, сохраненные на базе операционной системы Ubuntu, для Kaspersky Anti Targeted Attack Platform, развернутого на базе операционной системы Astra Linux, и наоборот.

Для приложения, развернутого на базе операционной системы Astra Linux, поддерживается восстановление приложения из резервной копии, созданной для версии 7.1.2, на сервере с версией 7.1.1.

Для других версий приложения возможность восстановления с одной версии на другую не предусмотрена: версия приложения, для которой будет выполнено восстановление данных, должна совпадать с версией приложения на сервере, где было выполнено резервное копирование. Если версии приложений не совпадают, при запуске восстановления отобразится сообщение об ошибке и процесс восстановления будет прерван.

Вы можете создать резервную копию сервера Central Node, подключившись к серверу по протоколу SSH или в меню администратора приложения.

Схема процесса представлена на рисунке ниже.



Процесс создания резервной копии и восстановления данных

Следующие возможности не предусмотрены в Kaspersky Anti Targeted Attack Platform:

- Восстановление из резервной копии в зоне аварийного восстановления.
- Автоматизация создания резервных копий по определенным условиям.
- Создание резервных копий по расписанию.
- Дублирование установки с помощью восстановления из резервной копии.

Мы настоятельно не рекомендуем выполнять перечисленные выше действия.

Резервное копирование и восстановление данных сервера Central Node

В этом сценарии описана процедура создания резервной копии и восстановления данных из нее на сервере Central Node.

Резервное копирование и восстановление данных на сервере Central Node содержит следующие этапы:

1. **Подготовка к созданию резервной копии**

   Убедитесь, что на Central Node, для которого вы хотите создать резервную копию, настроено получение зеркалированного трафика со SPAN-портов. Если получение зеркалированного трафика со SPAN-портов не включено, вам нужно включить его и проверить корректность работы. При отсутствии или неправильной работе функции во время создания резервной копии произойдет ошибка и полученный архив будет неполным. Восстановление данных из такого архива завершится неудачно.

   Как настроить получение зеркалированного трафика со SPAN-портов

   Вы можете включить получение зеркалированного трафика при установке компонента. Если вы отказались от получения трафика на этапе установки, выполните шаги инструкции ниже.

   Чтобы включить получение зеркалированного трафика со SPAN-портов:

   1. Если Central Node установлен на сервере, войдите в консоль управления этим сервером по протоколу SSH или через терминал.
   2. Если Central Node развернут в виде кластера, войдите в консоль управления любым из обрабатывающих серверов кластера по протоколу SSH или через терминал.
   3. Выполните команду:

      ```
      kata-enable-span
      ```

   Получение зеркалированного трафика со SPAN-портов будет включено.

   Как проверить, что получение зеркалированного трафика со SPAN-портов настроено и работает корректно

   Чтобы убедиться, что на Central Node, для которого вы хотите создать резервную копию, настроено и корректно работает получение зеркалированного трафика со SPAN-портов:

   1. Если Central Node установлен на сервере, войдите в консоль управления этим сервером по протоколу SSH или через терминал.
   2. Если Central Node развернут в виде кластера, войдите в консоль управления любым сервером кластера по протоколу SSH или через терминал.

3. Выполните последовательность команд:

   a. `sudo -i`

   b. `docker service ls | grep -P '(nta|ID|_span)'`

   В выводе в столбце REPLICAS для сервиса nta_configurator_services должно отображаться значение 0/1, для сервиса nta_core должно отображаться значение 1/1. Другие значения в выводе означают, что сервисы работают некорректно либо выключены.

2 Создание резервной копии

Во время создания резервной копии будут недоступны некоторые функции приложения. Список функций, которые будут недоступны, и инструкция по устранению этого ограничения приведены в статье Ограничения, действующие во время создания резервной копии.

Вы можете создать резервную копию с помощью меню администратора или с помощью режима Technical Support Mode:

Как создать резервную копию в меню администратора

Резервная копия Kaspersky Anti Targeted Attack Platform будет содержать только базы данных (базу обнаружений, сведения о статусе VIP, список данных, исключенных из проверки, уведомления) и параметры Central Node или PCN.

1. Войдите в консоль управления того сервера, резервную копию которого вы хотите создать, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя и пароль учетной записи администратора.

   Отобразится меню администратора компонента приложения.
3. В списке разделов меню администратора приложения выберите раздел **System administration**.
4. Нажмите на клавишу **Enter**.

   Откроется окно выбора действий.
5. В списке действий выберите **Backup/Restore settings**.
6. Нажмите на клавишу **Enter**.

   Откроется окно **Backup/Restore settings**.
7. В списке действий выберите **New**.
8. Нажмите на клавишу **Enter**.

   Откроется окно **Backup settings**.
9. Нажмите на кнопку **Back up**.

Резервная копия будет создана.

Как создать резервную копию в режиме Technical Support Mode

1. Войдите в консоль управления того сервера, резервную копию которого вы хотите создать, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя и пароль учетной записи администратора.

   Отобразится меню администратора компонента приложения.
3. В списке разделов меню администратора приложения выберите раздел **Technical Support Mode**.
4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.
6. Выполните команду:

   ```
   sudo kata-run.sh kata-backup-restore backup
   ```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

Параметры для создания резервной копии

Обязательный параметр	Параметр	Описание
Да	`-b <path>`	Создать резервную копию по указанному пути, где <path> – абсолютный или относительный путь к директории, в которой создается резервная копия.
Нет	`-c`	Очистить директорию перед сохранением резервной копии.
Нет	`-d <number of stored files>`	Указать максимальное количество файлов резервной копии, хранимых в директории, где <number> – количество файлов.
Нет	`-e`	Сохранить файлы в Хранилище.
Нет	`-q`	Сохранить файлы на карантине.
Нет	`-a`	Сохранить файлы, ожидающие повторной проверки (rescan).
Нет	`-s`	Сохранить артефакты Sandbox.
Нет	`-n`	Сохранить параметры Central Node или PCN.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Если дополнительные параметры не указаны, резервная копия будет содержать только базы данных (базу обнаружений, сведения о статусе VIP, список данных, исключенных из проверки, уведомления).

Пример:

Команда для создания резервной копии:

```
sudo kata-run.sh kata-backup-restore backup -b <path> -c -d <number of stored files> -e -q -a -s -n -l <filepath>
```

3 Сохранение резервной копии на жесткий диск

Сохраните резервную копию на жестком диске компьютера, выполнив команду:

```
scp <имя учетной записи для работы в меню администратора и в консоли управления сервером>@<IP-адрес сервера>:<имя файла резервной копии вида data_kata_<дата и время создания резервной копии>.tar>
```

Пример:

Команда для загрузки на жесткий диск компьютера резервной копии, созданной на сервере Central Node с IP-адресом 10.0.0.10 под учетной записью admin 10 апреля 2020 года в 10 часов 00 минут 00 секунд:

```
scp admin@10.0.0.10:data_kata_2020_04_10T10_00_00.tar
```

Резервная копия будет сохранена на жесткий диск вашего компьютера в текущую директорию.

4 Переустановка приложения

Удалите и заново установите Kaspersky Anti Targeted Attack Platform.

При установке приложения вам нужно указать то же значение маски сети для адресации серверов, которое было указано для маски сети в резервной копии приложения. Если значения не совпадают, после восстановления приложения возникает ошибка в работе встроенного Sensor. При необходимости вы можете восстановить работу компонента.

После установки вам нужно добавить в приложение те же типы лицензионных ключей (KATA, KATA + NDR, KEDR), что и в приложении на сервере, где была создана резервная копия. Это необходимо для того, чтобы восстановить все сохраненные в резервной копии параметры Central Node, PCN или SCN.

5 Загрузка резервной копии на сервер

Загрузите резервную копию на сервер Central Node, выполнив команду:

```
scp <имя файла резервной копии вида data_kata_<дата и время создания резервной копии>.tar> <имя учетной записи для работы в меню администратора и в консоли управления сервером>@<IP-адрес сервера>:
```

Пример:

Команда для загрузки резервной копии, созданной 10 апреля 2020 года в 10 часов 00 минут 00 секунд, на сервер Central Node с IP-адресом 10.0.0.10 под учетной записью admin:

```
scp data_kata_2020_04_10T10_00_00.tar admin@10.0.0.10:
```

Резервная копия будет загружена на сервер Central Node в текущую директорию.

6 Восстановление данных из резервной копии

Вы можете восстановить данные из резервной копии на сервере Central Node с помощью меню администратора или с помощью режима Technical Support Mode:

Как восстановить данные в меню администратора

1. Войдите в консоль управления того сервера, данные которого вы хотите восстановить, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя и пароль учетной записи администратора компонента приложения.

   Отобразится меню администратора компонента приложения.
3. В списке разделов меню администратора приложения выберите раздел **System administration**.
4. Нажмите на клавишу **Enter**.

   Откроется окно выбора действий.
5. В списке действий выберите **Backup/Restore settings**.

6. Нажмите на клавишу **Enter**.

   Откроется окно **Backup/Restore settings**.

7. В списке файлов с резервными копиями приложения выберите файл, из которого вы хотите восстановить данные сервера.

   Если нужного файла нет в списке, вам нужно загрузить файл с резервной копией на сервер.

8. Нажмите на клавишу **Enter**.

   Откроется окно выбора действий.

9. В списке действий выберите **Restore <имя файла резервной копии вида data_kata_<дата и время создания резервной копии>.tar>**

10. Нажмите на клавишу **Enter**.

    Откроется окно подтверждения действия.

11. Нажмите на кнопку **Restore**.

    Начнется процесс восстановления данных сервера из резервной копии.

Настройки получения зеркалированного трафика со SPAN-портов будут восстановлены автоматически, если имена сетевых интерфейсов совпадают на сервере, на котором была создана резервная копия, и на сервере, на котором происходит восстановление данных из резервной копии.

Как восстановить данные в режиме Technical Support Mode

1. Войдите в консоль управления того сервера, данные которого вы хотите восстановить, по протоколу SSH или через терминал.

2. В ответ на приглашение системы введите имя и пароль учетной записи администратора приложения.

   Отобразится меню администратора компонента приложения.

3. В списке разделов меню администратора приложения выберите раздел **Technical Support Mode**.

4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.

6. Выполните команду:

   ```
   sudo kata-run.sh kata-backup-restore restore
   ```

   Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

   Подсказка по использованию параметров доступна по команде `-h`.

Параметры для восстановления данных

Обязательный параметр	Параметр	Описание команды
Да	`-r <path>`	Восстановить данные из файла резервной копии, где <path> – полный путь к файлу резервной копии.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Пример:

Команда для восстановления данных из резервной копии:

```
sudo kata-run.sh kata-backup-restore restore -r <path> -l <filepath>
```

Настройки получения зеркалированного трафика со SPAN-портов будут восстановлены автоматически, если имена сетевых интерфейсов совпадают на сервере, на котором была создана резервная копия, и на сервере, на котором происходит восстановление данных из резервной копии.

Резервная копия параметров сервера не содержит PCAP-файлы записанного зеркалированного сетевого трафика. Вы можете сохранить и восстановить PCAP-файлы самостоятельно, выполнив копирование из директории /data/volumes/dumps подключенного хранилища. После восстановления данных вам необходимо подключить внешнее хранилище.

Если аппаратная конфигурация сервера Central Node, на котором была создана резервная копия, отличается от аппаратной конфигурации сервера, на котором вы планируете восстановить параметры сервера, после восстановления вам нужно заново настроить параметры масштабирования приложения.

Резервное копирование и восстановление данных сервера Central Node в виде кластера

В этом сценарии описана процедура создания резервной копии и восстановления данных из нее на сервере Central Node, развернутого в виде кластера.

Резервное копирование и восстановление данных на сервере Central Node, развернутого в виде кластера, содержит следующие этапы:

1. **Подготовка к созданию резервной копии**

   Убедитесь, что на одном из серверов кластера Central Node настроено получение зеркалированного трафика со SPAN-портов. Если получение зеркалированного трафика со SPAN-портов не включено, вам нужно включить его и проверить корректность работы. При отсутствии или неправильной работе функции во время создания резервной копии произойдет ошибка и полученный архив будет неполным. Восстановление данных из такого архива завершится неудачно.

   Как определить сервер кластера, на котором включена обработка зеркалированного трафика со SPAN-портов

Чтобы определить, на каком сервере кластера Central Node включена обработка зеркалированного трафика со SPAN-портов:

1. Войдите в консоль управления любого сервера кластера по протоколу SSH или через терминал.

2. Выполните команду:

   ```
   sudo docker node ls -q | sudo xargs docker node inspect -f '{{ if eq (index
   .Spec.Labels "infrastructure.span") "true" }}{{ .Description.Hostname }}{{ end
   }}'
   ```

   Отобразится адрес обрабатывающего сервера кластера, на котором включена обработка зеркалированного SPAN-трафика.

Как настроить получение зеркалированного трафика со SPAN-портов

Вы можете включить получение зеркалированного трафика при установке компонента. Если вы отказались от получения трафика на этапе установки, выполните шаги инструкции ниже.

Чтобы включить получение зеркалированного трафика со SPAN-портов:

1. Если Central Node установлен на сервере, войдите в консоль управления этим сервером по протоколу SSH или через терминал.

2. Если Central Node развернут в виде кластера, войдите в консоль управления любым из обрабатывающих серверов кластера по протоколу SSH или через терминал.

3. Выполните команду:

   ```
   kata-enable-span
   ```

Получение зеркалированного трафика со SPAN-портов будет включено.

Как проверить, что получение зеркалированного трафика со SPAN-портов настроено и работает корректно

Чтобы убедиться, что на Central Node, для которого вы хотите создать резервную копию, настроено и корректно работает получение зеркалированного трафика со SPAN-портов:

1. Если Central Node установлен на сервере, войдите в консоль управления этим сервером по протоколу SSH или через терминал.

2. Если Central Node развернут в виде кластера, войдите в консоль управления любым сервером кластера по протоколу SSH или через терминал.

3. Выполните последовательность команд:

   a. `sudo -i`

   b. `docker service ls | grep -P '(nta|ID|_span)'`

   В выводе в столбце REPLICAS для сервиса nta_configurator_services должно отображаться значение 0/1, для сервиса nta_core должно отображаться значение 1/1. Другие значения в выводе означают, что сервисы работают некорректно либо выключены.

2. **Создание резервной копии**

Во время создания резервной копии будут недоступны некоторые функции приложения. Список функций, которые будут недоступны, и инструкция по устранению этого ограничения приведены в статье Ограничения, действующие во время создания резервной копии.

Вы можете создать резервную копию с помощью меню администратора или с помощью режима Technical Support Mode:

Как создать резервную копию приложения в меню администратора

Резервная копия Kaspersky Anti Targeted Attack Platform будет содержать только базы данных (базу обнаружений, сведения о статусе VIP, список данных, исключенных из проверки, уведомления) и параметры Central Node или PCN.

1. Войдите в консоль управления любого работоспособного сервера кластера по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя и пароль учетной записи администратора.

   Отобразится меню администратора компонента приложения.
3. В списке разделов меню администратора приложения выберите раздел **System administration**.
4. Нажмите на клавишу **Enter**.

   Откроется окно выбора действий.
5. В списке действий выберите **Backup/Restore settings**.
6. Нажмите на клавишу **Enter**.

   Откроется окно **Backup/Restore settings**.
7. В списке действий выберите **New**.
8. Нажмите на клавишу **Enter**.

   Откроется окно **Backup settings**.
9. Нажмите на кнопку **Back up**.

Резервная копия будет создана.

Как создать резервную копию приложения в режиме Technical Support Mode

1. Войдите в консоль управления любого работоспособного сервера кластера по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя и пароль учетной записи администратора компонента приложения.

   Отобразится меню администратора компонента приложения.
3. В списке разделов меню администратора приложения выберите раздел **Technical Support Mode**.
4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.
6. Определите адрес обрабатывающего сервера, на котором включена обработка зеркалированного SPAN-трафика, в кластере:

```
sudo docker node ls -q | sudo xargs docker node inspect -f '{{ if eq (index
.Spec.Labels "infrastructure.span") "true" }}{{ .Description.Hostname }}{{ end
}}'
```

Отобразится адрес обрабатывающего сервера кластера, на котором включена обработка зеркалированного SPAN-трафика.

7. Войдите в консоль управления этого сервера по протоколу SSH:

```
ssh admin@<адрес сервера, полученный на шаге 6>
```

8. Выполните команду:

```
sudo kata-run.sh kata-backup-restore backup
```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

Параметры для создания резервной копии

Обязательный параметр	Параметр	Описание
Да	`-b <path>`	Создать резервную копию по указанному пути, где <path> – абсолютный или относительный путь к директории, в которой создается резервная копия.
Нет	`-c`	Очистить директорию перед сохранением файла резервной копии.
Нет	`-d <number of stored files>`	Указать максимальное количество файлов, хранимых в директории, где <number> – количество файлов.
Нет	`-n`	Сохранить параметры Central Node или PCN.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Если дополнительные параметры не указаны, резервная копия будет содержать только базы данных (базу обнаружений, сведения о статусе VIP, список данных, исключенных из проверки, уведомления).

Пример:

Команда для создания резервной копии:

```
sudo kata-run.sh kata-backup-restore backup -b <path> -c -d <number of stored files> -e -q -a -s -n -l
<filepath>
```

Для приложения версии 7.1.2 не предусмотрено создание резервной копии с помощью меню администратора приложения.

3 Сохранение резервной копии на жесткий диск

Сохраните резервную копию на жестком диске компьютера, выполнив команду:

```
scp <имя учетной записи для работы в меню администратора и в консоли управления
сервером>@<IP-адрес сервера>:<имя файла резервной копии вида data_kata_<дата и время
создания резервной копии>.tar>
```

Пример:

Команда для загрузки на жесткий диск компьютера резервной копии, созданной на сервере Central Node с IP-адресом 10.0.0.10 под учетной записью admin 10 апреля 2020 года в 10 часов 00 минут 00 секунд:

```
scp admin@10.0.0.10:data_kata_2020_04_10T10_00_00.tar
```

Резервная копия будет сохранена на жесткий диск вашего компьютера в текущую директорию.

4. **Переустановка приложения**

Удалите и заново установите Kaspersky Anti Targeted Attack Platform.

При установке приложения вам нужно указать то же значение маски сети для адресации серверов, которое было указано для маски сети в резервной копии приложения. Если значения не совпадают, после восстановления приложения возникает ошибка в работе встроенного Sensor. При необходимости вы можете восстановить работу компонента.

После установки вам нужно добавить в приложение те же типы лицензионных ключей (KATA, KATA + NDR, KEDR), что и в приложении на сервере, где была создана резервная копия. Это необходимо для того, чтобы восстановить все сохраненные в резервной копии параметры Central Node, PCN или SCN.

5. **Загрузка резервной копии на сервер**

Загрузите резервную копию на сервер Central Node, выполнив команду:

```
scp <имя файла резервной копии вида data_kata_<дата и время создания резервной копии>.tar> <имя учетной записи для работы в меню администратора и в консоли управления сервером>@<IP-адрес сервера>:
```

Пример:

Команда для загрузки резервной копии, созданной 10 апреля 2020 года в 10 часов 00 минут 00 секунд, на сервер Central Node с IP-адресом 10.0.0.10 под учетной записью admin:

```
scp data_kata_2020_04_10T10_00_00.tar admin@10.0.0.10:
```

Резервная копия будет загружена на сервер Central Node в текущую директорию.

6. **Восстановление данных из резервной копии**

Вы можете восстановить данные из резервной копии на сервере Central Node с помощью меню администратора или с помощью режима Technical Support Mode:

Как восстановить данные приложения версии или в меню администратора

1. Войдите в консоль управления любого работоспособного сервера кластера по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя и пароль учетной записи администратора компонента приложения.

   Отобразится меню администратора компонента приложения.
3. В списке разделов меню администратора приложения выберите раздел **System administration**.
4. Нажмите на клавишу **Enter**.

   Откроется окно выбора действий.
5. В списке действий выберите **Backup/Restore settings**.

6. Нажмите на клавишу **Enter**.

   Откроется окно **Backup/Restore settings**.

7. В списке файлов с резервными копиями приложения выберите файл, из которого вы хотите восстановить данные сервера.

   Если нужного файла нет в списке, вам нужно загрузить файл с резервной копией на сервер.

8. Нажмите на клавишу **Enter**.

   Откроется окно выбора действий.

9. В списке действий выберите **Restore <имя файла резервной копии вида data_kata_<дата и время создания резервной копии>.tar>**

10. Нажмите на клавишу **Enter**.

    Откроется окно подтверждения действия.

11. Нажмите на кнопку **Restore**.

    Начнется процесс восстановления данных сервера из резервной копии.

Настройки получения зеркалированного трафика со SPAN-портов будут восстановлены автоматически, если имена сетевых интерфейсов совпадают на сервере, на котором была создана резервная копия, и на сервере, на котором происходит восстановление данных из резервной копии.

Если имена сетевых интерфейсов отличаются, после выполнения шага 11 инструкции, расположенной выше, вам будет предложено выбрать сетевые интерфейсы для получения зеркалированного трафика со SPAN-портов.

Как восстановить данные приложения версии или в режиме Technical Support Mode

1. Войдите в консоль управления любого работоспособного сервера кластера по протоколу SSH или через терминал.

2. В ответ на приглашение системы введите имя и пароль учетной записи администратора приложения.

   Отобразится меню администратора компонента приложения.

3. В списке разделов меню администратора приложения выберите раздел **Technical Support Mode**.

4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.

6. Запустите процесс восстановления данных, выполнив команду:

   ```
   sudo kata-run.sh kata-backup-restore restore
   ```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

Параметры для восстановления данных

Обязательный параметр	Параметр	Описание команды
Да	`-r <path>`	Восстановить данные из файла резервной копии, где <path> – полный путь к файлу резервной копии.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Пример:

Команда для восстановления данных из резервной копии:

```
sudo kata-run.sh kata-backup-restore restore -r <path> -l <filepath>
```

Настройки получения зеркалированного трафика со SPAN-портов будут восстановлены автоматически, если имена сетевых интерфейсов совпадают на сервере, на котором была создана резервная копия, и на сервере, на котором происходит восстановление данных из резервной копии.

Если имена сетевых интерфейсов отличаются, после выполнения шага 6 инструкции, расположенной выше, вам будет предложено выбрать сетевые интерфейсы для получения зеркалированного трафика со SPAN-портов.

Если вы хотите восстановить данные приложения версии 7.1.2 на сервере с приложением 7.1.1 или 7.1.2, вам нужно использовать инструкцию, приведенную ниже.

Как восстановить данные приложения версии 7.1.1 или 7.1.2 в режиме Technical Support Mode

1. Войдите в консоль управления любого работоспособного сервера кластера по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя и пароль учетной записи администратора приложения.

   Отобразится меню администратора компонента приложения.
3. В списке разделов меню администратора приложения выберите раздел **Technical Support Mode**.
4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.
6. Определите адрес обрабатывающего сервера, на котором включена обработка зеркалированного SPAN-трафика, в кластере:

   ```
   sudo docker node ls -q | sudo xargs docker node inspect -f '{{ if eq (index .Spec.Labels "infrastructure.span") "true" }}{{ .Description.Hostname }}{{ end }}'
   ```

   Отобразится адрес обрабатывающего сервера кластера, на котором включена обработка зеркалированного SPAN-трафика.

7. Войдите в консоль управления этого сервера по протоколу SSH:

   ```
   ssh admin@<адрес сервера, полученный на шаге 6>
   ```

8. Запустите процесс восстановления данных, выполнив команду:

   ```
   sudo kata-run.sh kata-backup-restore restore
   ```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

Параметры для восстановления данных

Обязательный параметр	Параметр	Описание команды
Да	`-r <path>`	Восстановить данные из файла резервной копии, где <path> – полный путь к файлу резервной копии.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Пример:

Команда для восстановления данных из резервной копии:

```
sudo kata-run.sh kata-backup-restore restore -r <path> -l <filepath>
```

Настройки получения зеркалированного трафика со SPAN-портов будут восстановлены автоматически, если имена сетевых интерфейсов совпадают на сервере, на котором была создана резервная копия, и на сервере, на котором происходит восстановление данных из резервной копии.

Если имена сетевых интерфейсов отличаются, после выполнения шага 6 инструкции, расположенной выше, вам будет предложено выбрать сетевые интерфейсы для получения зеркалированного трафика со SPAN-портов.

Резервная копия параметров сервера не содержит PCAP-файлы записанного зеркалированного сетевого трафика. Вы можете сохранить и восстановить PCAP-файлы самостоятельно, выполнив копирование из директории /data/volumes/dumps подключенного внешнего хранилища. После восстановления данных вам необходимо подключить внешнее хранилище.

Если аппаратная конфигурация сервера Central Node, на котором была создана резервная копия, отличается от аппаратной конфигурации сервера, на котором вы планируете восстановить параметры сервера, после восстановления вам нужно заново настроить параметры масштабирования приложения.

Резервное копирование и восстановление данных сервера Central Node в режиме распределенного решения и мультитенантности

В этом сценарии описана процедура создания резервной копии и восстановления данных из нее на серверах Central Node, развернутых в режиме распределенного решения или мультитенантности.

Для создания резервной копии и восстановления данных при использовании режима распределенного решения или мультитенантности вам необходимо подключиться к каждому серверу Central Node в иерархии и выполнить этапы инструкции, расположенной ниже.

Резервное копирование и восстановление данных на серверах Central Node, развернутых в режиме распределенного решения или мультитенантности, содержит следующие этапы:

1. **Подготовка к созданию резервной копии**

   Убедитесь, что на Central Node, для которого вы хотите создать резервную копию, настроено получение зеркалированного трафика со SPAN-портов. При развертывании Central Node в виде кластера оно должно быть включено на одном сервере кластера. Если получение зеркалированного трафика со SPAN-портов не включено, вам нужно включить его и проверить корректность работы. При отсутствии или неправильной работе функции во время создания резервной копии произойдет ошибка и полученный архив будет неполным. Восстановление данных из такого архива завершится неудачно.

   Как определить сервер кластера, на котором включена обработка зеркалированного трафика со SPAN-портов

   Чтобы определить, на каком сервере кластера Central Node включена обработка зеркалированного трафика со SPAN-портов:

   1. Войдите в консоль управления любого сервера кластера по протоколу SSH или через терминал.
   2. Выполните команду:

      ```
      sudo docker node ls -q | sudo xargs docker node inspect -f '{{ if eq (index .Spec.Labels "infrastructure.span") "true" }}{{ .Description.Hostname }}{{ end }}'
      ```

      Отобразится адрес обрабатывающего сервера кластера, на котором включена обработка зеркалированного SPAN-трафика.

   Как настроить получение зеркалированного трафика со SPAN-портов

   Вы можете включить получение зеркалированного трафика при установке компонента. Если вы отказались от получения трафика на этапе установки, выполните шаги инструкции ниже.

   Чтобы включить получение зеркалированного трафика со SPAN-портов:

   1. Если Central Node установлен на сервере, войдите в консоль управления этим сервером по протоколу SSH или через терминал.
   2. Если Central Node развернут в виде кластера, войдите в консоль управления любым из обрабатывающих серверов кластера по протоколу SSH или через терминал.

3. Выполните команду:

   ```
   kata-enable-span
   ```

   Получение зеркалированного трафика со SPAN-портов будет включено.

Как проверить, что получение зеркалированного трафика со SPAN-портов настроено и работает корректно

Чтобы убедиться, что на Central Node, для которого вы хотите создать резервную копию, настроено и корректно работает получение зеркалированного трафика со SPAN-портов:

1. Если Central Node установлен на сервере, войдите в консоль управления этим сервером по протоколу SSH или через терминал.

2. Если Central Node развернут в виде кластера, войдите в консоль управления любым сервером кластера по протоколу SSH или через терминал.

3. Выполните последовательность команд:

   a. `sudo -i`

   b. `docker service ls | grep -P '(nta|ID|_span)'`

   В выводе в столбце REPLICAS для сервиса nta_configurator_services должно отображаться значение 0/1, для сервиса nta_core должно отображаться значение 1/1. Другие значения в выводе означают, что сервисы работают некорректно либо выключены.

2 **Создание резервной копии**

Во время создания резервной копии будут недоступны некоторые функции приложения. Список функций, которые будут недоступны, и инструкция по устранению этого ограничения приведены в статье Ограничения, действующие во время создания резервной копии.

Вы можете создать резервную копию с помощью меню администратора или с помощью режима Technical Support Mode:

Как создать резервную копию в меню администратора

> Резервная копия Kaspersky Anti Targeted Attack Platform будет содержать только базы данных (базу обнаружений, сведения о статусе VIP, список данных, исключенных из проверки, уведомления) и параметры Central Node или PCN.

1. Войдите в консоль управления того сервера, резервную копию которого вы хотите создать, по протоколу SSH или через терминал.

2. В ответ на приглашение системы введите имя и пароль учетной записи администратора.

   Отобразится меню администратора компонента приложения.

3. В списке разделов меню администратора приложения выберите раздел **System administration**.

4. Нажмите на клавишу **Enter**.

   Откроется окно выбора действий.

5. В списке действий выберите **Backup/Restore settings**.

6. Нажмите на клавишу **Enter**.

   Откроется окно **Backup/Restore settings**.

7. В списке действий выберите **New**.

8. Нажмите на клавишу **Enter**.

   Откроется окно **Backup settings**.

9. Нажмите на кнопку **Back up**.

Резервная копия будет создана.

Как создать резервную копию в режиме Technical Support Mode

1. Войдите в консоль управления того сервера, резервную копию которого вы хотите создать, по протоколу SSH или через терминал.

2. В ответ на приглашение системы введите имя и пароль учетной записи администратора.

   Отобразится меню администратора компонента приложения.

3. В списке разделов меню администратора приложения выберите раздел **Technical Support Mode**.

4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.

6. Выполните команду:

   ```
   sudo kata-run.sh kata-backup-restore backup
   ```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

Параметры для создания резервной копии

Обязательный параметр	Параметр	Описание
Да	`-b <path>`	Создать резервную копию по указанному пути, где <path> – абсолютный или относительный путь к директории, в которой создается резервная копия.
Нет	`-c`	Очистить директорию перед сохранением резервной копии.
Нет	`-d <number of stored files>`	Указать максимальное количество файлов резервной копии, хранимых в директории, где <number> – количество файлов.
Нет	`-e`	Сохранить файлы в Хранилище.
Нет	`-q`	Сохранить файлы на карантине.
Нет	`-a`	Сохранить файлы, ожидающие повторной проверки (rescan).
Нет	`-s`	Сохранить артефакты Sandbox.

Нет	`-n`	Сохранить параметры Central Node или PCN.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Если дополнительные параметры не указаны, резервная копия будет содержать только базы данных (базу обнаружений, сведения о статусе VIP, список данных, исключенных из проверки, уведомления).

Пример:

Команда для создания резервной копии:

```
sudo kata-run.sh kata-backup-restore backup -b <path> -c -d <number of stored files> -e -q -a -s -n -l <filepath>
```

3 Сохранение резервной копии на жесткий диск

Сохраните резервную копию на жестком диске компьютера, выполнив команду:

```
scp <имя учетной записи для работы в меню администратора и в консоли управления сервером>@<IP-адрес сервера>:<имя файла резервной копии вида data_kata_<дата и время создания резервной копии>.tar>
```

Пример:

Команда для загрузки на жесткий диск компьютера резервной копии, созданной на сервере Central Node с IP-адресом 10.0.0.10 под учетной записью admin 10 апреля 2020 года в 10 часов 00 минут 00 секунд:

```
scp admin@10.0.0.10:data_kata_2020_04_10T10_00_00.tar
```

Резервная копия будет сохранена на жесткий диск вашего компьютера в текущую директорию.

4 Переустановка приложения

Удалите и заново установите Kaspersky Anti Targeted Attack Platform.

Восстановление данных из резервной копии производится только на сервер с ролью Central Node. Если вы предварительно назначите серверу роль PCN или SCN, процесс восстановления завершится ошибкой.

При установке приложения вам нужно указать то же значение маски сети для адресации серверов, которое было указано для маски сети в резервной копии приложения. Если значения не совпадают, после восстановления приложения возникает ошибка в работе встроенного Sensor. При необходимости вы можете восстановить работу компонента.

После установки вам нужно добавить в приложение те же типы лицензионных ключей (KATA, KATA + NDR, KEDR), что и в приложении на сервере, где была создана резервная копия. Это необходимо для того, чтобы восстановить все сохраненные в резервной копии параметры Central Node, PCN или SCN.

5 Загрузка резервной копии на сервер

Загрузите резервную копию на сервер Central Node, выполнив команду:

```
scp <имя файла резервной копии вида data_kata_<дата и время создания резервной копии>.tar> <имя учетной записи для работы в меню администратора и в консоли управления сервером>@<IP-адрес сервера>:
```

Пример:

Команда для загрузки резервной копии, созданной 10 апреля 2020 года в 10 часов 00 минут 00 секунд, на сервер Central Node с IP-адресом 10.0.0.10 под учетной записью admin:

```
scp data_kata_2020_04_10T10_00_00.tar admin@10.0.0.10:
```

Резервная копия будет загружена на сервер Central Node в текущую директорию.

6 Восстановление данных из резервной копии

Вы можете восстановить данные из резервной копии на сервере Central Node с помощью меню администратора или с помощью режима Technical Support Mode:

Как восстановить данные в меню администратора

1. Войдите в консоль управления того сервера, данные которого вы хотите восстановить, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя и пароль учетной записи администратора компонента приложения.

   Отобразится меню администратора компонента приложения.
3. В списке разделов меню администратора приложения выберите раздел **System administration**.
4. Нажмите на клавишу **Enter**.

   Откроется окно выбора действий.
5. В списке действий выберите **Backup/Restore settings**.
6. Нажмите на клавишу **Enter**.

   Откроется окно **Backup/Restore settings**.
7. В списке файлов с резервными копиями приложения выберите файл, из которого вы хотите восстановить данные сервера.

   Если нужного файла нет в списке, вам нужно загрузить файл с резервной копией на сервер.
8. Нажмите на клавишу **Enter**.

   Откроется окно выбора действий.
9. В списке действий выберите **Restore <имя файла резервной копии вида data_kata_<дата и время создания резервной копии>.tar>**
10. Нажмите на клавишу **Enter**.

    Откроется окно подтверждения действия.
11. Нажмите на кнопку **Restore**.

    Начнется процесс восстановления данных сервера из резервной копии.

Настройки получения зеркалированного трафика со SPAN-портов будут восстановлены автоматически, если имена сетевых интерфейсов совпадают на сервере, на котором была создана резервная копия, и на сервере, на котором происходит восстановление данных из резервной копии.

Как восстановить данные в режиме Technical Support Mode

1. Войдите в консоль управления того сервера, данные которого вы хотите восстановить, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя и пароль учетной записи администратора приложения.

   Отобразится меню администратора компонента приложения.

3. В списке разделов меню администратора приложения выберите раздел **Technical Support Mode**.

4. Нажмите на клавишу **Enter**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **Enter**.

6. Выполните команду:

```
sudo kata-run.sh kata-backup-restore restore
```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

Параметры для восстановления данных

Обязательный параметр	Параметр	Описание команды
Да	`-r <path>`	Восстановить данные из файла резервной копии, где <path> – полный путь к файлу резервной копии.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Пример:

Команда для восстановления данных из резервной копии:

```
sudo kata-run.sh kata-backup-restore restore -r <path> -l <filepath>
```

Настройки получения зеркалированного трафика со SPAN-портов будут восстановлены автоматически, если имена сетевых интерфейсов совпадают на сервере, на котором была создана резервная копия, и на сервере, на котором происходит восстановление данных из резервной копии.

Если аппаратная конфигурация сервера Central Node, на котором была создана резервная копия, отличается от аппаратной конфигурации сервера, на котором вы планируете восстановить параметры сервера, после восстановления вам нужно заново настроить параметры масштабирования приложения.

После восстановления данных вам не требуется заново подключать SCN к PCN: параметры подключения к PCN и список подключенных SCN восстанавливаются из резервной копии.

Резервная копия параметров сервера не содержит PCAP-файлы записанного зеркалированного сетевого трафика. Вы можете сохранить и восстановить PCAP-файлы самостоятельно, выполнив копирование из директории /data/volumes/dumps подключенного хранилища. После восстановления данных вам необходимо подключить внешнее хранилище.

Ограничение, действующее при восстановлении данных в режиме распределенного решения и мультитенантности

После восстановления данных в режиме распределенного решения и мультитенантности в таблице алертов могут не отображаться новые алерты, созданные в результате проверки технологией AM. Вы можете проверить наличие ограничения и при необходимости устранить его.

Чтобы проверить отображение новых алертов в таблице алертов:

1. Включите точку мониторинга для используемого Sensor.
2. Если вы используете Sensor, установленный отдельно, войдите в консоль управления этого сервера Sensor по протоколу SSH или через терминал.
3. Если вы используете встроенный Sensor, войдите в консоль управления того сервера Central Node, на котором располагается встроенный Sensor, по протоколу SSH или через терминал.

   Если Central Node развернут в виде кластера, вам требуется войти в консоль управления обрабатывающего сервера, на котором включена обработка зеркалированного SPAN-трафика.

   Как определить адрес этого сервера

   1. Войдите в консоль управления любого работоспособного сервера кластера по протоколу SSH или через терминал.
   2. В ответ на приглашение системы введите имя и пароль учетной записи администратора компонента приложения.

      Отобразится меню администратора компонента приложения.
   3. В списке разделов меню администратора приложения выберите раздел Technical Support Mode.
   4. Нажмите на клавишу Enter.

      Отобразится окно подтверждения входа в режим Technical Support Mode.
   5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите Yes и нажмите на клавишу Enter.
   6. Определите адрес обрабатывающего сервера, на котором включена обработка зеркалированного SPAN-трафика, в кластере:

      ```
      sudo docker node ls -q | sudo xargs docker node inspect -f '{{ if eq (index
      .Spec.Labels "infrastructure.span") "true" }}{{ .Description.Hostname }}{{ end }}'
      ```

      Отобразится адрес обрабатывающего сервера кластера, на котором включена обработка зеркалированного SPAN-трафика.
   7. Войдите в консоль управления этого сервера по протоколу SSH:

      ```
      ssh admin@<адрес сервера, полученный на шаге 6>
      ```
4. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке компонента.

   Отобразится меню администратора компонента приложения.
5. В меню администратора приложения выберите режим Technical Support Mode.

6. Нажмите на клавишу ENTER.

7. Отобразится окно подтверждения входа в режим Technical Support Mode.

8. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите Yes и нажмите на клавишу ENTER.

9. Выполните команду:

```
watch "curl http://127.0.0.1:9191/metrics | grep
preprocessor_files_extracted_fromhttp"
```

Если для поля *preprocessor_files_extracted_fromhttp* отображается значение 0, выполните приведенные ниже шаги инструкции по устранению ограничения.

Чтобы устранить ограничение при использовании встроенного Sensor:

1. Войдите в консоль управления того сервера Central Node, на котором располагается встроенный Sensor, по протоколу SSH или через терминал.

   Если Central Node развернут в виде кластера, вам требуется войти в консоль управления обрабатывающего сервера, на котором включена обработка зеркалированного SPAN-трафика.

   Как определить адрес этого сервера

   1. Войдите в консоль управления любого работоспособного сервера кластера по протоколу SSH или через терминал.

   2. В ответ на приглашение системы введите имя и пароль учетной записи администратора компонента приложения.

      Отобразится меню администратора компонента приложения.

   3. В списке разделов меню администратора приложения выберите раздел Technical Support Mode.

   4. Нажмите на клавишу Enter.

      Отобразится окно подтверждения входа в режим Technical Support Mode.

   5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите Yes и нажмите на клавишу Enter.

   6. Определите адрес обрабатывающего сервера, на котором включена обработка зеркалированного SPAN-трафика, в кластере:

      ```
      sudo docker node ls -q | sudo xargs docker node inspect -f '{{ if eq (index
      .Spec.Labels "infrastructure.span") "true" }}{{ .Description.Hostname }}{{ end }}'
      ```

      Отобразится адрес обрабатывающего сервера кластера, на котором включена обработка зеркалированного SPAN-трафика.

   7. Войдите в консоль управления этого сервера по протоколу SSH:

      ```
      ssh admin@<адрес сервера, полученный на шаге 6>
      ```

2. Повысьте привилегии пользователя, выполнив команду:

   ```
   sudo -i
   ```

3. Выполните команды:

   ```
   kata-sensor-tool reset
   ```

```
kata-sensor-tool reset-core
kata-sensor-tool init-embedded-sensor
```

4. Убедитесь, что новый алерт отображается в таблице алертов, выполнив шаги инструкции по проверке отображения новых алертов.

Ограничение будет устранено.

Чтобы устранить ограничение при использовании Sensor, установленного на отдельном от Central Node сервере:

1. Удалите подключенный Sensor в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.
2. Войдите в консоль управления этого сервера Sensor, по протоколу SSH или через терминал.
3. Повысьте привилегии пользователя, выполнив команду:

   ```
   sudo -i
   ```

4. Выполните команду:

   ```
   kata-sensor-tool reset
   ```

5. Подключите Sensor к Central Node заново.
6. Убедитесь, что новый алерт отображается в таблице алертов, выполнив шаги инструкции по проверке отображения новых алертов.

Ограничение будет устранено.

Состав экспортируемых данных

В Kaspersky Anti Targeted Attack Platform могут содержаться данные пользователей и другая конфиденциальная информация. Администратору Kaspersky Anti Targeted Attack Platform нужно обеспечить безопасность этих данных самостоятельно при создании резервной копии, замене оборудования, на которое установлено приложение, и в прочих случаях, когда может потребоваться удаление данных без возможности восстановления. Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за доступ к данным, хранящимся на серверах приложения.

Из резервной копии **не** восстанавливаются следующие данные:

- Параметры интеграции с компонентом Sandbox.

  После восстановления Kaspersky Anti Targeted Attack Platform из резервной копии Sandbox не подключается к Central Node автоматически.

- Параметры интеграции с внешними системами (в том числе с почтовыми сенсорами).

  При создании резервной копии Kaspersky Anti Targeted Attack Platform вам нужно учитывать, что внешние системы могут не возобновить отправку трафика на Central Node даже после того, как он снова начнет его принимать.

- Параметры интеграции с SIEM-системами.

- Параметры часового пояса.
- Параметры записи данных в журналы приложения.
- Телеметрия от компонентов Endpoint Agents при интеграции с функциональными блоками NDR и KEDR.
- Дампы сетевого трафика.
- Изменения в конфигурационных файлах, которые производились в режиме Technical Support Mode.

Перед восстановлением данных из резервной копии на сервере Central Node, на котором выполняется восстановление приложения, происходит очистка следующих данных:

- Базы данных приложения.
- Объектов в Хранилище.
- Файлов из алертов, созданных при повторной проверке (rescan).
- Артефактов Sandbox.
- Конфигурационных файлов.
- Параметров Central Node.

Состав данных, экспортируемых для создания резервной копии

Тип данных	Экспортируемые данные	Режим работы с приложением	Способ развертывания
Параметры Central Node, включая TLS-сертификат сервера. Базы данных приложения на Central Node: • события в трафике сети; • алерты и наличие у алертов статуса VIP; • риски и аномалии; • задачи и результаты их выполнения; • предустановки и правила запрета; • пользовательские правила TAA (IOA) и исключения; • пользовательские правила обнаружения вторжений и исключения из них; • пользовательские правила YARA; • IOC-файлы; • правила исключений из проверки; • правила, по которым определяются разрешенные сетевые взаимодействия; • информация о файлах в Хранилище; • информация об объектах на карантине; • список компьютеров с Endpoint Agent; • настройки подключения компьютеров с Endpoint Agent; • данные об устройствах: • инвентарный список устройств; • список учетных записей пользователей, зарегистрированных в операционных системах устройств; • список исполняемых файлов на устройствах; • адресные пространства устройств; • метки, присвоенные устройствам; • данные о расположении устройств на карте сетевых взаимодействий; • общие отчеты и шаблоны отчетов; • отчеты и шаблоны отчетов NDR; • данные учетных записей пользователей; • журнал активности пользователей; • данные сетевых сессий; • топологическая карта; • уведомления; • параметры встроенного Sensor.	Параметры Central Node – по выбору. Базы данных приложения – по умолчанию.	Отдельный сервер Central Node.	Все способы развертывания.
Параметры подключения к PCN. Список подключенных SCN.	Да	Режим распределенного решения и мультитенантности.	Все способы развертывания.
Параметры PCN, включая TLS-сертификат сервера.	По выбору.	Режим распределенного решения и мультитенантности.	Все способы развертывания.
Параметры SCN, включая TLS-сертификат сервера.	По выбору. Как для отдельного сервера Central Node.	Режим распределенного решения и мультитенантности.	Все способы развертывания.

Тип данных	Экспортируемые данные	Режим работы с приложением	Способ развертывания
Базы данных приложения на PCN: • события в трафике сети; • алерты и наличие у алертов статуса VIP; • риски и аномалии; • задачи и результаты их выполнения; • предустановки и правила запрета; • пользовательские правила TAA (IOA) и исключения; • пользовательские правила обнаружения вторжений и исключения из них; • пользовательские правила YARA; • IOC-файлы; • правила исключений из проверки; • правила, по которым определяются разрешенные сетевые взаимодействия; • информация о файлах в Хранилище; • информация об объектах на карантине; • список компьютеров с Endpoint Agent; • настройки подключения компьютеров с Endpoint Agent; • данные об устройствах: • инвентарный список устройств; • список учетных записей пользователей, зарегистрированных в операционных системах устройств; • список исполняемых файлов на устройствах; • адресные пространства устройств; • метки, присвоенные устройствам; • данные о расположении устройств на карте сетевых взаимодействий; • общие отчеты и шаблоны отчетов; • отчеты и шаблоны отчетов NDR; • данные учетных записей пользователей; • журнал активности пользователей; • данные сетевых сессий; • топологическая карта; • уведомления; • параметры встроенного Sensor.	По умолчанию.	Режим распределенного решения и мультитенантности.	Все способы развертывания.
Конфигурационные файлы, кроме конфигурационного файла для интеграции с MDR.	Да	Все режимы.	Все способы развертывания.
Хранилище.	По выбору.	Все режимы.	Неотказоустойчивая версия.
Артефакты Sandbox.	По выбору.	Все режимы.	Неотказоустойчивая версия.
Файлы из алертов, созданных при повторной проверке (rescan).	По выбору.	Все режимы.	Неотказоустойчивая версия.
Файлы, которые в момент создания резервной копии приложения находились в очереди на проверку.	Нет.	Все режимы.	Все способы развертывания.
Лицензионные ключи.	Нет.	Все режимы.	Все способы развертывания.
База событий.	Нет.	Все режимы.	Все способы развертывания.
Параметры Sensor, установленных отдельно от Central Node.			
Параметры точек мониторинга, связанных с сетевыми интерфейсами встроенного Sensor.			
Параметры сетевых интерфейсов.	Нет.	Все режимы.	Все способы развертывания.
Дампы SPAN-трафика.	Нет.	Все режимы.	Все способы развертывания.

Ограничения, действующие во время создания резервной копии

Во время создания резервной копии недоступны следующие функции приложения:

- Разделы **Серверы Sensor**, **События в трафике сети**, **Карта сети**, **Риски и аномалии**, **Коннекторы**, **Серверы интеграции**.

  При переходе в эти разделы отобразится предупреждение *Процессы NDR запускаются. Пожалуйста, подождите*.

- Соединение с Kaspersky Anti Targeted Attack Platform с помощью коннекторов.
- Передача телеметрии от компонентов Endpoint Agent, подключенных к функциональному блоку NDR.
- Прием ERSPAN- и SPAN-трафика.

  Внешние системы могут не возобновить отправку трафика в Kaspersky Anti Targeted Attack Platform даже после того, как приложение снова начнет его принимать.

- Соединение с Kaspersky Anti Targeted Attack Platform по API NDR.

Если Central Node установлен на сервере, вы можете устранить эти ограничения, запустив сервисы, отвечающие за эти функции приложения.

Чтобы запустить сервисы приложения:

1. Войдите в консоль управления сервером Central Node по протоколу SSH или через терминал.
2. Выполните последовательность команд:

   a. `sudo -i`

   b. `docker service scale kata_product_main_1_nta_database=1`

   c. `docker service scale kata_product_main_1_nta_core=1`

   d. `docker service scale kata_product_main_1_nta_syncer=1`

Сервисы будут запущены. Функционал приложения будет доступен в полном объеме.

Восстановление работы встроенного Sensor после восстановления приложения из резервной копии

Если значение маски сети в резервной копии приложения не совпадает со значением маски сети в приложении, на базе которого производилось восстановление, после восстановления в работе встроенного Sensor возникает ошибка. Рекомендуется проверить текущее значение маски сети, чтобы убедиться, что ошибка в работе компонента возникает из-за несовпадения значений.

Чтобы проверить текущее значение маски сети,

в окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

Текущее значение маски сети отображается на карточке компонента под его названием. Если значения не совпадают, выполните шаги инструкции по восстановлению работы встроенного Sensor.

После восстановления работы компонента параметры интеграции с прокси-сервером по протоколу ICAP и с почтовым сервером по протоколам SMTP и POP3 сбрасываются. Параметры перенаправления трафика от компонента Endpoint Agent на сервер Sensor, если они были настроены, также сбрасываются.

Чтобы восстановить работу встроенного Sensor:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.
2. Наведите курсор мыши на карточку нужного компонента и нажмите на нее левой кнопкой мыши.

   Откроется окно с информацией о компоненте.
3. Нажмите на кнопку **Удалить**.
4. Карточка компонента будет удалена.
5. Войдите в консоль управления сервера Central Node, на котором располагался нужный вам встроенный Sensor, по протоколу SSH или через терминал.
6. Повысьте привилегии пользователя, выполнив команду:

   ```
   sudo -i
   ```
7. Выполните команды:

   ```
   kata-sensor-tool reset
   kata-sensor-tool init-embedded-sensor
   ```

   Работа встроенного Sensor будет восстановлена. Информация о компоненте отобразится в разделе **Серверы Sensor**.

Если работа компонента не восстанавливается, обратитесь в Службу технической поддержки.

Обновление Kaspersky Anti Targeted Attack Platform

Перед установкой пакета обновления приложения рекомендуется предварительно создать резервную копию текущего состояния каждого обновляемого сервера Central Node и загрузить ее на жесткий диск из меню администратора приложения. В случае сбоя при установке пакета обновления приложения или при необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией приложения.
Рекомендуется также ознакомиться с ограничениями для той версии, до которой вы обновляете приложение.

Миграция с неотказоустойчивой версии приложения на отказоустойчивую с помощью обновления не предусмотрена: если вы используете неотказоустойчивую версию приложения, при обновлении вы можете установить только неотказоустойчивую версию, и наоборот.

Обновление приложения включает в себя следующие этапы:

1. Обновление компонента Sandbox.

   В приложении не предусмотрена процедура обновления компонента. Вам требуется установить компонент версии 7.1.

   После установки компонента вам нужно указать максимальное количество одновременно запускаемых виртуальных машин. По умолчанию используется значение 48.

   При установке компонента на виртуальную машину VMware ESXi вам требуется задать для нее конфигурацию, описанную в разделе *Расчеты для компонента Sandbox*.

2. Обновление компонента Central Node.

   - Если компонент развернут на базе операционной системы Ubuntu, доступны следующие способы обновления:

     - С версии 7.0.3 до версии 7.1.1.

       В этом случае вам нужно выполнить одну из следующих инструкций: *Обновление Central Node, установленного на сервере* или *Обновление Central Node, установленного в виде кластера*.

     - С версии 7.1 до версии 7.1.1.

       В этом случае вам нужно выполнить инструкцию *Обновление Kaspersky Anti Targeted Attack Platform с версии 7.1 до версии 7.1.1 или 7.1.2*.

     - С версии 7.1.1 до версии 7.1.3

       В этом случае вам нужно выполнить инструкцию *Обновление Kaspersky Anti Targeted Attack Platform с версии 7.1.1 или 7.1.2 до версии 7.1.3*.

- С версии 7.1.3 до версии 7.1.7.

  В этом случае вам нужно выполнить инструкцию *Обновление Kaspersky Anti Targeted Attack Platform с версии 7.1.3 до версии 7.1.7*.

- Если компонент развернут на базе операционной системы Astra Linux и вам требуется использовать сертифицированную версию приложения, вы можете обновить компонент одним из следующих способов:

  - С версии 7.0.3 до версии 7.1.1.

    В этом случае вам нужно выполнить одну из следующих инструкций: *Обновление Central Node, установленного на сервере* или *Обновление Central Node, установленного в виде кластера*.

  - С версии 7.1 до версии 7.1.1.

    В этом случае вам нужно выполнить инструкцию *Обновление Kaspersky Anti Targeted Attack Platform с версии 7.1 до версии 7.1.1 или 7.1.2*.

- Если компонент развернут на базе операционной системы Astra Linux и сертификация не требуется, вы можете обновить компонент одним из следующих способов:

  - С версии 7.0.3 до версии 7.1.2.

    В этом случае вам нужно выполнить одну из следующих инструкций: *Обновление Central Node, установленного на сервере* или *Обновление Central Node, установленного в виде кластера*.

  - С версии 7.1 до версии 7.1.2.

    В этом случае вам нужно выполнить инструкцию *Обновление Kaspersky Anti Targeted Attack Platform с версии 7.1 до версии 7.1.1 или 7.1.2*.

  - С версии 7.1.2 до версии 7.1.3.

    В этом случае вам нужно выполнить инструкцию *Обновление Kaspersky Anti Targeted Attack Platform с версии 7.1.1 или 7.1.2 до версии 7.1.3*.

  - С версии 7.1.3 до версии 7.1.7.

    В этом случае вам нужно выполнить инструкцию *Обновление Kaspersky Anti Targeted Attack Platform с версии 7.1.3 до версии 7.1.7*.

  Если вы используете приложение версии 7.1.2 и хотите перейти на версию 7.1.1, вы можете развернуть приложение этой версии и перенести в него данные, полученные во время работы с версией 7.1.2. Для этого вам нужно создать резервную копию приложения версии 7.1.2 и восстановить из нее данные на сервере с версией 7.1.1. См. подробнее раздел Резервное копирование и восстановление данных.

  Для приложения других версий восстановление возможно только из резервной копии, созданной в этой же версии.

Если вы использовали компонент Central Node версии 7.0.3 на одном сервере или в виде кластера более полугода, мы настоятельно рекомендуем перед обновлением применить скрипт fix_old_slots.sh для очистки диска сервера или серверов кластера. Вы можете получить файл скрипта и инструкцию по его применению, обратившись в Службу технической поддержки.

Обновление до версий 7.1.1 и 7.1.2 с более ранних версий приложения, чем 7.0.3, невозможно. Если вы используете более раннюю версию приложения, вам требуется последовательно обновить Central Node до версии 7.0.3: 3.7 → 3.7.1, 3.7.1 → 3.7.2, 3.7.2 → 4.0, 4.0 → 4.1, 4.1 → 5.0, 5.0 → 5.1, 5.1 → 6.0, 6.0 → 6.0.2, 6.0.2 → 6.1, 6.1 → 7.0.3.

Если вы подключили и настроили внешнее хранилище для встроенного Sensor (Embedded Sensor), после обновления вам нужно выполнить шаги инструкции *Восстановление данных на внешнем хранилище для компонента Sensor*.

3. Обновление компонента Sensor, установленного на отдельном сервере.

   В приложении не предусмотрена процедура обновления компонента. Вам требуется установить компонент версии 7.1.7 с учетом рекомендаций.

4. Обновление компонента Endpoint Agent:

   - Kaspersky Endpoint Security для Windows.
   - Kaspersky Endpoint Security для Linux.
   - Kaspersky Endpoint Security для Mac.

Обновление Central Node, установленного на сервере

Перед установкой пакета обновления приложения рекомендуется предварительно создать резервную копию текущего состояния каждого обновляемого сервера Central Node и загрузить ее на жесткий диск из меню администратора приложения. В случае сбоя при установке пакета обновления приложения или при необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией приложения.
Рекомендуется также ознакомиться с ограничениями для той версии, до которой вы обновляете приложение.

Если вы используете режим распределенного решения и мультитенантности, вам нужно обновить каждый Central Node в соответствии с описанной ниже процедурой, не отключая при этом SCN от PCN.

Отключение SCN от PCN необратимо, повторное подключение SCN к какому-либо серверу PCN не предусмотрено.

Обновление поставляется в виде пакета обновлений. Пакет входит в комплект поставки приложения.

Чтобы обновить Central Node, установленный на сервере:

1. Удалите коннекторы, серверы интеграции, внешние системы из списка разрешенных к интеграции, компоненты Sandbox и компоненты Sensor, установленные отдельно от обновляемого Central Node.

   Все описанные ниже действия выполняются на серверах в режиме Technical Support Mode после повышения привилегий пользователя с помощью команды `sudo -i`.

2. Если вы обновили Central Node до версии 7.0.3 с версии 6.1 или более ранней, выполните следующие команды:

   ```
   rm -rf /data/upgrade/
   rm -rf /opt/upgrade_venv
   ```

Если обновление до версии 7.0.3 не выполнялось, пропустите этот шаг.

3. Поместите пакет с обновлением приложения на сервер Central Node в директорию `/data`.
4. Войдите в консоль управления сервера Central Node, на котором вы хотите выполнить обновление, по протоколу SSH или через терминал.
5. Убедитесь, что на разделе /dev/sda2 свободно более 100 ГБ.
6. Распакуйте архив с обновлением, выполнив команду:
   - Для обновления до 7.1.1:

     ```
     tar xvf /data/kata-upgrade-7.1.1.531-x86_64_en-ru-zh.tar.gz -C /data/
     ```

   - Для обновления до 7.1.2:

     ```
     tar xvf /data/kata-upgrade-7.1.2.532-x86_64_en-ru-zh.tar.gz -C /data/
     ```

7. Установите пакет с обновлением, выполнив следующие команды:

   ```
   cd /data/upgrade/
   ./run_kata_upgrade.py
   ```

   Отобразится окно ввода имени пользователя.
8. В отобразившемся окне в поле **Username** введите имя пользователя с правами администратора, выберите кнопку **OK** и нажмите на клавишу **Enter**.

   Значение по умолчанию: **admin**.
9. В отобразившемся окне в поле **Password** введите пароль от учетной записи с правами администратора, выберите кнопку **OK** и нажмите на клавишу **Enter**.

   Отобразится окно ввода пути к архиву с обновлением.
10. В отобразившемся окне в поле **Data directory** введите путь до архива с обновлением, выберите кнопку **OK** и нажмите на клавишу **Enter**.

    Значение по умолчанию: **/data/upgrade**
11. В отобразившемся окне выберите язык локализации функционала NDR.

    Области приложения, связанные с функциональностью NDR, будут отображаться на выбранном языке.

    Через некоторое время в консоли отобразится сообщение о необходимости выключения сервера.
12. После отображения сообщения о необходимости выключения сервера выполните команду:

    ```
    poweroff
    ```

13. Смонтируйте iso-образ на базе операционной системы Ubuntu с Kaspersky Anti Targeted Attack Platform версии 7.1.1 (kata-cn-7.1.1.531-inst.x86_64_en-ru-zh.iso). Если вы используете Kaspersky Anti Targeted Attack Platform на базе операционной системы Astra Linux, воспользуйтесь инструкцией для создания iso-образа.
14. Загрузитесь с устройства, на котором находится смонтированный iso-образ.
15. В меню загрузчика GRUB выберите пункт **Upgrade KATA 7.0.3**.

16. Следуйте дальнейшим шагам мастера до завершения обновления на сервере.

17. Когда обновление завершится, войдите в консоль управления сервером Central Node, на котором вы выполнили обновление, по протоколу SSH или через терминал.

18. Удалите временные файлы инсталлятора, выполнив команду:

    ```
    rm -rf /data/upgrade /data/install_data
    ```

19. Выполните команду:

    ```
    docker exec -it $(docker ps | grep nta_database | awk '{print $1}') psql -p 5433 -U
    postgres -d kics -c 'GRANT SELECT ON TABLE kics_webserver.wl_rule_attributes TO
    kics_webserver;'
    ```

Компонент Central Node будет обновлен.

После обновления требуется заново выполнить вход в консоль управления сервера Central Node по протоколу SSH или через терминал.

Особенности обновления Central Node версии 7.0.3, установленного на сервере с операционной системой Astra Linux

При обновлении Central Node версии 7.0.3, установленного на сервере с операционной системой Astra Linux, может потребоваться больший объем дискового пространства. Если дискового пространства оказывается недостаточно, процесс обновления прерывается, отображается сообщение о недостаточности дискового пространства.

Чтобы возобновить обновление при нехватке дискового пространства:

1. Создайте резервную копию Central Node и загрузите ее на жесткий диск из меню администратора приложения.

2. Выполните очистку диска с помощью утилиты.

После очистки диска вы можете возобновить обновление.

Восстановление работы встроенного Sensor в режиме распределенного решения и мультитенантности после обновления

После обновления компонента Central Node, который использовался в режиме распределенного решения или мультитенантности, до версии 7.1.1, 7.1.2 или 7.1.3 может отсутствовать встроенный Sensor (Embedded Sensor).

Чтобы устранить ограничение:

1. Если после обновления компонента Central Node встроенный Sensor присутствует, но находится в выключенном состоянии, удалите Sensor в веб-интерфейсе.
2. Войдите в консоль управления того сервера Central Node, на котором требуется восстановить встроенный Sensor, по протоколу SSH или через терминал.
3. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке компонента.

   Отобразится меню администратора компонента приложения.
4. В меню администратора приложения выберите режим Technical Support Mode.
5. Нажмите на клавишу ENTER.
6. Отобразится окно подтверждения входа в режим Technical Support Mode.
7. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите Yes и нажмите на клавишу ENTER.
8. Выполните команду:

   ```
   docker service update --cap-add=CAP_DAC_OVERRIDE --cap-add=CAP_IPC_LOCK --cap-add=CAP_SYS_PTRACE kata_product_main_1_preprocessor_span
   ```
9. Если встроенный Sensor не восстановился, очистите базы, выполнив команду:

   ```
   kata-sensor-tool reset-core
   ```

Встроенный Sensor будет восстановлен приблизительно через одну минуту.

Очистка диска сервера Central Node

При обновлении Central Node на сервере с операционной системой Astra Linux может потребоваться больший объем дискового пространства. Если дискового пространства оказывается недостаточно, процесс обновления перерывается, отображается сообщение о недостаточности дискового пространства. Вы можете возобновить процесс обновления, очистив диск сервера Central Node с помощью утилиты kata-antiaptdb-cleaner. Утилита становится доступной при обновлении Kaspersky Anti Targeted Attack Platform до версии 7.1.

В результате работы утилиты могут быть удалены следующие данные:

- Данные алертов, включая алерты, созданных в результате проверки объектов технологией YARA (если во время запуска утилиты был указан этот параметр).
- Данные обнаружений.
- Данные событий NDR.
- Данные журналов NDR.
- Данные рисков.
- Данные устройств.

Чтобы выполнить очистку диска с помощью утилиты:

1. Войдите в консоль управления сервера Central Node, на котором вы хотите очистить диск, по протоколу SSH или через терминал.

2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке компонента.

   Отобразится меню администратора компонента приложения.

3. В меню администратора приложения выберите режим **Technical Support Mode**.

4. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **ENTER**.

6. Установите утилиту для очистки диска, выполнив команду:

   ```
   pip install /data/upgrade/whl/kata_antiaptdb_cleaner/kata_antiaptdb_cleaner-1.0-py2.py3-none-any.whl
   ```

7. Выполните команду:

   ```
   kata-antiaptdb-cleaner
   ```

   Система предложит указать количество дней, за которые требуется сохранить данные. По умолчанию сохраняются данные за последние 30 дней.

   Если вы хотите сохранить данные за 1 день, вам нужно иметь в виду, что данные сохраняются за последние 24 часа от момента запуска утилиты.

8. Выполните одно из следующих действий:

   - Если вы хотите указать количество дней, за которые требуется сохранить данные, введите нужное число и нажмите на клавишу **ENTER**.
   - Если вы хотите пропустить этот шаг и использовать значение по умолчанию, нажмите на клавишу **ENTER**.

Утилита будет запущена. Данные будут удалены в соответствии с выбранными параметрами. Процесс удаления данных может занять продолжительное время.

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Описание параметров запуска утилиты

Обязательный параметр	Параметр	Описание
Нет	`--help`	Страница помощи.
Нет	`--days <количество дней>`	Количество дней, за которые требуется сохранить данные. Более старые данные удаляются.
Нет	`--clean-yara`	Удаление алертов, созданных в результате проверки объектов технологией YARA.
Пример команды для запуска утилиты с параметрами: `kata-antiaptdb-cleaner --days 40 --clean-yara`		

Обновление Central Node, установленного в виде кластера

Перед установкой пакета обновления приложения рекомендуется предварительно создать резервную копию текущего состояния каждого обновляемого сервера Central Node и загрузить ее на жесткий диск из меню администратора приложения. В случае сбоя при установке пакета обновления приложения или при необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией приложения.
Рекомендуется также ознакомиться с ограничениями для той версии, до которой вы обновляете приложение.

Обновление поставляется в виде пакета обновлений. Пакет входит в комплект поставки приложения.

Если вы используете режим распределенного решения и мультитенантности, вам нужно обновить каждый Central Node в соответствии с описанной ниже процедурой, не отключая при этом SCN от PCN.

Отключение SCN от PCN необратимо, повторное подключение SCN к какому-либо серверу PCN не предусмотрено.

Чтобы обновить Central Node, установленный в виде кластера:

1. Удалите коннекторы, серверы интеграции, внешние системы из списка разрешенных к интеграции, компоненты Sandbox и компоненты Sensor, установленные отдельно от обновляемого Central Node.

   Все описанные ниже действия выполняются на серверах в режиме Technical Support Mode после повышения привилегий пользователя с помощью команды `sudo -i`.

2. Если вы обновили Central Node до версии 7.0.3 с версии 6.1 или более ранней, зайдите на сервер кластера, куда был помещен пакет обновления до версии 7.0.3, и выполните следующие команды:

   ```
   rm -rf /data/upgrade/
   rm -rf /opt/upgrade_venv
   ```

   Если обновление до версии 7.0.3 не выполнялось, пропустите этот шаг.

3. Зайдите на любой из серверов хранения кластера Central Node и убедитесь в работоспособности Ceph-хранилища. Для этого выполните команду:

   ```
   ceph -s | grep health:
   ```

   Ceph-хранилище работоспособно, если возвращено следующее значение:

   ```
   health: HEALTH_OK
   ```

   Если значение отличается от `health: HEALTH_OK`, обратитесь в Службу технической поддержки.

4. Зайдите на каждый из серверов хранения и перезагрузите службу kata-osd-starter:

   ```
   systemctl restart kata-osd-starter
   ```

5. Убедитесь в работоспособности сервиса Kafka:

   a. Определите, каким из серверов кластера присвоена роль manager в Docker swarm. Для этого на любом из серверов кластера выполните команду:

      ```
      docker node ls
      ```

      Отобразится список серверов кластера. В списке серверов роль manager присвоена тем из них, у которых в столбце `MANAGER STATUS` указано `Leader` или `Reachable`.

   b. Выполните команду:

      ```
      docker service ps kata_product_main_1_schema_registry
      ```

      По значению в столбце `NODE` определите, на каком сервере находится Schema Registry.

   c. Зайдите на сервер с Schema Registry и выполните команду:

      ```
      docker exec -it $(docker ps | grep schema_registry | awk '{ print $1 }')
      curl http://127.0.0.1:8081/subjects
      ```

      Сервис Kafka работоспособен, если был возвращен JSON со списком subject.

6. Поместите пакет с обновлением приложения на сервер кластера Central Node с ролью manager в Docker swarm в директорию `/data`. Для просмотра роли используйте команду `$ docker node ls`.

7. Войдите в консоль управления этим сервером по протоколу SSH или через терминал.

8. Убедитесь, что на разделе /dev/sda2 на каждом сервере кластера свободно более 100 ГБ.

9. Распакуйте архив с обновлением, выполнив команду:

   - Для обновления до версии 7.1.1:

     ```
     tar xvf /data/kata-upgrade-7.1.1.531-x86_64_en-ru-zh.tar.gz -C /data/
     ```

   - Для обновления до версии 7.1.2:

     ```
     tar xvf /data/kata-upgrade-7.1.2.532-x86_64_en-ru-zh.tar.gz -C /data/
     ```

10. Установите пакет с обновлением, выполнив следующие команды:

    ```
    cd /data/upgrade/
    ./run_kata_upgrade.py
    ```

    Отобразится окно ввода имени пользователя.

11. В поле **Username** введите имя пользователя с правами администратора, выберите кнопку **OK** и нажмите на клавишу **Enter**.

    Значение по умолчанию: **admin**.

12. В поле **Password** введите пароль от учетной записи с правами администратора, выберите кнопку **OK** и нажмите на клавишу **Enter**.

    Откроется окно ввода пути к архиву с обновлением.

13. В поле **Data directory** введите путь к архиву с пакетом обновлений, выберите кнопку **OK** и нажмите на клавишу **Enter**.

    Значение по умолчанию: **/data/upgrade**.

14. В отобразившемся окне выберите язык локализации функционала NDR.

Области приложения, связанные с функциональностью NDR, будут отображаться на выбранном языке.

Через некоторое время в консоли отобразится сообщение о необходимости выключения сервера.

15. Подключитесь к серверу, который необходимо выключить, по протоколу SSH или через терминал.
16. Выполните команду `poweroff.`
17. Смонтируйте iso-образ на базе операционной системы Ubuntu с Kaspersky Anti Targeted Attack Platform версии 7.1.1 (kata-cn-7.1.1.531-inst.x86_64_en-ru-zh.iso). Если вы используете Kaspersky Anti Targeted Attack Platform на базе операционной системы Astra Linux, воспользуйтесь инструкцией для создания iso-образа.
18. Загрузитесь с устройства, на котором находится смонтированный iso-образ.
19. В меню загрузчика GRUB выберите пункт **Upgrade KATA 7.0.3**.
20. Следуйте дальнейшим шагам мастера до завершения обновления на сервере.
21. После завершения обновления перейдите в консоль сервера, к которому вы подключились на шаге 6, введите `next` и нажмите на клавишу **`Enter`**.

    Запустится скрипт, завершающий процесс обновления. После того, как обновление завершится, в консоли отобразится сообщение о необходимости выключить следующий сервер кластера.
22. Повторите шаги 14-20 для каждого сервера кластера.

    > Последним обновляется сервер, к которому вы подключились на шаге 6. Для этого сервера шаг 20 отсутствует.
23. Войдите в консоль управления сервера кластера, для которого настроено получение зеркалированного трафика со SPAN-портов, по протоколу SSH или через терминал.
24. Выполните команду:

    ```
    docker exec -it $(docker ps | grep nta_database | awk '{print $1}') psql -p 5433 -U postgres -d kics -c 'GRANT SELECT ON TABLE kics_webserver.wl_rule_attributes TO kics_webserver;
    ```
25. Удалите временные файлы инсталлятора, выполнив команду:

    ```
    rm -rf /data/upgrade /data/install_data
    ```

    Повторите этот шаг для каждого сервера кластера.

Компонент Central Node будет обновлен.

> После обновления компонента требуется заново выполнить вход в консоль управления сервера Central Node по протоколу SSH или через терминал.

Обновление Central Node с версии 7.1 до версии 7.1.1 или 7.1.2

Перед установкой пакета обновления приложения рекомендуется предварительно создать резервную копию текущего состояния каждого обновляемого сервера Central Node и загрузить ее на жесткий диск из меню администратора приложения. В случае сбоя при установке пакета обновления приложения или при необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией приложения.
Рекомендуется также ознакомиться с ограничениями для той версии, до которой вы обновляете приложение.

Если вы используете режим распределенного решения и мультитенантности, вам нужно обновить каждый Central Node в соответствии с описанной ниже процедурой, не отключая при этом SCN от PCN.

Отключение SCN от PCN необратимо, повторное подключение SCN к какому-либо серверу PCN не предусмотрено.

Обновление поставляется в виде пакета обновлений. Пакет входит в комплект поставки приложения.

Чтобы обновить Central Node:

1. Удалите коннекторы, серверы интеграции, внешние системы из списка разрешенных к интеграции, компоненты Sandbox и компоненты Sensor, установленные отдельно от обновляемого Central Node.

   Все описанные ниже действия выполняются на серверах в режиме Technical Support Mode после повышения привилегий пользователя с помощью команды `sudo -i`.

2. Если Central Node установлен на сервере:

   a. Поместите пакет с обновлением приложения на сервер Central Node в директорию `/data`.

   b. Войдите в консоль управления сервера Central Node, на котором вы хотите выполнить обновление, по протоколу SSH или через терминал.

3. Если Central Node установлен в виде кластера:

   a. Поместите пакет с обновлением приложения на сервер кластера Central Node с ролью manager в Docker swarm в директорию `/data`. Для просмотра роли используйте команду `$ docker node ls`.

   b. Войдите в консоль управления этим сервером по протоколу SSH или через терминал.

4. Удалите директорию `upgrade` перед распаковкой архива, выполнив команду:

   ```
   rm -rf /data/upgrade
   ```

5. Убедитесь, что размер свободного дискового пространства в файловой системе /dev/sda2 составляет более 140 ГБ.

6. Распакуйте архив с обновлением, выполнив команду:

   - Для обновления до 7.1.1:

     ```
     tar xvf /data/kata-upgrade-7.1.1.531-x86_64_en-ru.tar.gz -C /data/
     ```

   - Для обновления до 7.1.2:

     ```
     tar xvf /data/kata-upgrade-7.1.2.532-x86_64_en-ru.tar.gz -C /data/
     ```

7. Установите пакет с обновлением, выполнив следующие команды:

   - Для обновления до 7.1.1:

     ```
     cd /data/upgrade/
     ./run_kata_upgrade.py --patch-version 711
     ```

   - Для обновления до 7.1.2:

     ```
     cd /data/upgrade/
     ./run_kata_upgrade.py --patch-version 712
     ```

   Отобразится окно ввода имени пользователя.

8. В отобразившемся окне в поле **Username** введите имя пользователя с правами администратора, выберите кнопку **OK** и нажмите на клавишу **Enter**.

   Значение по умолчанию: **admin**.

9. В отобразившемся окне в поле **Password** введите пароль от учетной записи с правами администратора, выберите кнопку **OK** и нажмите на клавишу **Enter**.

   Отобразится окно ввода пути к архиву с обновлением.

10. В отобразившемся окне в поле **Data directory** введите путь до архива с обновлением, выберите кнопку **OK** и нажмите на клавишу **Enter**.

    Значение по умолчанию: **/data/upgrade**

11. В отобразившемся окне выберите язык локализации функционала NDR.

    Области приложения, связанные с функциональностью NDR, будут отображаться на выбранном языке.

12. Удалите временные файлы инсталлятора, выполнив команду:

    ```
    rm -rf /data/upgrade /data/install_data
    ```

    Если вы обновляете Central Node, развернутый в виде кластера, команду требуется выполнить на каждом сервере кластера.

Компонент Central Node будет обновлен.

После завершения обновления рекомендуется перезагрузить все обновленные Central Node. В случае установки Central Node в виде кластера, рекомендуется поочередно перезагрузить все серверы кластера.

Обновление Central Node с версии 7.1.1 или 7.1.2 до версии 7.1.3

Перед установкой пакета обновления приложения рекомендуется предварительно создать резервную копию текущего состояния каждого обновляемого сервера Central Node и загрузить ее на жесткий диск из меню администратора приложения. В случае сбоя при установке пакета обновления приложения или при необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией приложения.
Рекомендуется также ознакомиться с ограничениями для той версии, до которой вы обновляете приложение.

Если вы используете режим распределенного решения и мультитенантности, вам нужно обновить каждый Central Node в соответствии с описанной ниже процедурой, не отключая при этом SCN от PCN.

Отключение SCN от PCN необратимо, повторное подключение SCN к какому-либо серверу PCN не предусмотрено.

Обновление поставляется в виде пакета обновлений. Пакет входит в комплект поставки приложения.

После обновления Kaspersky Anti Targeted Attack Platform до версии 7.1.3 возвращение к сертифицированному состоянию (версия 7.1.1) невозможно.

Чтобы обновить Central Node:

1. Удалите коннекторы, серверы интеграции, внешние системы из списка разрешенных к интеграции, компоненты Sandbox и компоненты Sensor, установленные отдельно от обновляемого Central Node.

   Все описанные ниже действия выполняются на серверах в режиме Technical Support Mode после повышения привилегий пользователя с помощью команды `sudo -i`.

2. Если Central Node установлен на сервере:

   a. Поместите пакет с обновлением приложения на сервер Central Node в директорию `/data`.

   b. Войдите в консоль управления сервера Central Node, на котором вы хотите выполнить обновление, по протоколу SSH или через терминал.

3. Если Central Node установлен в виде кластера:

   a. Поместите пакет с обновлением приложения на сервер кластера Central Node с ролью manager в Docker swarm в директорию `/data`. Для просмотра роли используйте команду `$ docker node ls`.

   b. Войдите в консоль управления этим сервером по протоколу SSH или через терминал.

4. Удалите директорию `upgrade` перед распаковкой архива, выполнив команду:

   ```
   rm -rf /data/upgrade
   ```

5. Убедитесь, что размер свободного дискового пространства в файловой системе /dev/sda2 составляет более 140 ГБ.

6. Распакуйте архив с обновлением, выполнив команду:

   ```
   tar xvf /data/kata-upgrade-7.1.3.533-x86_64_en-ru.tar.gz -C /data/
   ```

7. Установите пакет с обновлением, выполнив следующие команды:

   ```
   cd /data/upgrade/
   ./run_kata_upgrade.py --patch-version 713
   ```

   Отобразится окно ввода имени пользователя.

8. В отобразившемся окне в поле **Username** введите имя пользователя с правами администратора, выберите кнопку **OK** и нажмите на клавишу **Enter**.

   Значение по умолчанию: **admin**.

9. В отобразившемся окне в поле **Password** введите пароль от учетной записи с правами администратора, выберите кнопку **OK** и нажмите на клавишу **Enter**.

   Отобразится окно ввода пути к архиву с обновлением.

10. В отобразившемся окне в поле **Data directory** введите путь до архива с обновлением, выберите кнопку **OK** и нажмите на клавишу **Enter**.

    Значение по умолчанию: **/data/upgrade**

11. В отобразившемся окне выберите язык локализации функционала NDR.

    Области приложения, связанные с функциональностью NDR, будут отображаться на выбранном языке.

12. Удалите временные файлы инсталлятора, выполнив команду:

    ```
    rm -rf /data/upgrade /data/install_data
    ```

    Если вы обновляете Central Node, развернутый в виде кластера, команду требуется выполнить на каждом сервере кластера.

Компонент Central Node будет обновлен.

После завершения обновления рекомендуется перезагрузить все обновленные Central Node. В случае установки Central Node в виде кластера, рекомендуется поочередно перезагрузить все серверы кластера.

Обновление Central Node с версии 7.1.3 до версии 7.1.7

Перед установкой пакета обновления приложения рекомендуется предварительно создать резервную копию текущего состояния каждого обновляемого сервера Central Node и загрузить ее на жесткий диск из меню администратора приложения. В случае сбоя при установке пакета обновления приложения или при необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией приложения.
Рекомендуется также ознакомиться с ограничениями для той версии, до которой вы обновляете приложение.

Если вы используете режим распределенного решения и мультитенантности, вам нужно обновить каждый Central Node в соответствии с описанной ниже процедурой, не отключая при этом SCN от PCN.

Отключение SCN от PCN необратимо, повторное подключение SCN к какому-либо серверу PCN не предусмотрено.

Обновление поставляется в виде пакета обновлений. Пакет входит в комплект поставки приложения.

Чтобы обновить Central Node:

1. Если Central Node установлен на сервере:
   a. Поместите пакет с обновлением приложения на сервер Central Node в директорию `/data`.
   b. Войдите в консоль управления сервера Central Node, на котором вы хотите выполнить обновление, по протоколу SSH или через терминал.
2. Если Central Node установлен в виде кластера:
   a. Поместите пакет с обновлением приложения на сервер кластера Central Node с ролью manager в Docker swarm в директорию `/data`. Для просмотра роли используйте команду `$ docker node ls`.
   b. Войдите в консоль управления этим сервером по протоколу SSH или через терминал.
3. Удалите директорию `upgrade` перед распаковкой архива, выполнив команду:
   ```
   rm -rf /data/upgrade
   ```
4. Убедитесь, что размер свободного дискового пространства в файловой системе /dev/sda2 составляет более 140 ГБ.
5. Распакуйте архив с обновлением, выполнив команду:
   ```
   tar xvf /data/kata-upgrade-7.1.7.537.1-x86_64_en-ru-zh.tar.gz -C /data/
   ```
6. Установите пакет с обновлением, выполнив следующие команды:
   ```
   cd /data/upgrade/
   ./run_kata_upgrade.py --patch-version 717
   ```
   Отобразится окно ввода имени пользователя.

7. В отобразившемся окне в поле **Username** введите имя пользователя с правами администратора, выберите кнопку **OK** и нажмите на клавишу **Enter**.

   Значение по умолчанию: **admin**.

8. В отобразившемся окне в поле **Password** введите пароль от учетной записи с правами администратора, выберите кнопку **OK** и нажмите на клавишу **Enter**.

   Отобразится окно ввода пути к архиву с обновлением.

9. В отобразившемся окне в поле **Data directory** введите путь до архива с обновлением, выберите кнопку **OK** и нажмите на клавишу **Enter**.

   Значение по умолчанию: **/data/upgrade**

10. В отобразившемся окне выберите язык локализации функционала NDR.

    Области приложения, связанные с функциональностью NDR, будут отображаться на выбранном языке.

11. Удалите временные файлы инсталлятора, выполнив команду:

    ```
    rm -rf /data/upgrade /data/install_data
    ```

    Если вы обновляете Central Node, развернутый в виде кластера, команду требуется выполнить на каждом сервере кластера.

Компонент Central Node будет обновлен.

После завершения обновления рекомендуется перезагрузить все обновленные Central Node. В случае установки Central Node в виде кластера, рекомендуется поочередно перезагрузить все серверы кластера.

Обновление Sensor, установленного на отдельном сервере

В приложении не предусмотрена стандартная процедура обновления. Вам требуется установить компонент версии 7.1.7.

При установке компонента вы можете использовать следующие рекомендации:

1. Сохраните настройки компонента Sensor в удобном для вас формате, например, с помощью скриншотов. Если вы используете фильтрацию трафика по технологиям BPF и Regexp, рекомендуется сохранить правила фильтрации в файл.

2. Выполните установку компонента Sensor.

3. Подключите установленный компонент Sensor к компоненту Central Node.

4. Восстановите сохраненные настройки компонента Sensor вручную.

5. Подключите внешнее хранилище.

6. Выполните шаги инструкции *Восстановление данных на внешнем хранилище для компонента Sensor*, чтобы восстановить данные, сохраненные в хранилище во время работы с предыдущей версией приложения.

Восстановление данных на внешнем хранилище, подключенном к компоненту Sensor

Чтобы восстановить данные на внешнем хранилище, подключенном к компоненту Sensor:

1. Если вы хотите восстановить данные на внешнем хранилище, подключенном к встроенному компоненту Sensor (Embedded Sensor), войдите в консоль управления сервера Central Node, на котором расположен встроенный Sensor, по протоколу SSH или через терминал.

2. Если вы хотите восстановить данные на внешнем хранилище, подключенном к компоненту Sensor, который установлен отдельно от Central Node, войдите в консоль управления сервера Sensor по протоколу SSH или через терминал.

3. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке компонента.

   Отобразится меню администратора компонента приложения.

4. В меню администратора приложения выберите режим **Technical Support Mode**.

5. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

6. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **ENTER**.

7. Выполните команду:

   find /data/volumes/dumps/traffic -depth -maxdepth 2 -mindepth 2 -type f -exec mv {} /data/volumes/dumps/traffic \;

Данные на внешнем хранилище будут восстановлены.

Состав и объем данных, сохраняемых при обновлении приложения Kaspersky Anti Targeted Attack Platform

Состав и объем данных, сохраняемых при обновлении приложения Kaspersky Anti Targeted Attack Platform с версии 7.1 до версии 7.1.1 представлен в таблице ниже.

Состав и объем данных, сохраняемых при обновлении приложения с версии 7.1 до версии 7.1.1

Тип данных	Данные, сохраняемые при обновлении
Параметры Central Node или PCN.	Все данные, кроме: • лицензионных ключей; • параметров интеграции с компонентом Sensor; • параметров интеграции с компонентом Sandbox; • параметров получения зеркалированного трафика со SPAN-портов в отказоустойчивой версии Central Node; • Записанных дампов зеркалированного сетевого трафика со SPAN-портов.

Тип данных	Данные, сохраняемые при обновлении
Базы данных приложения на Central Node или PCN (база алертов, данные мониторинга работы приложения, база пользовательских правил, задачи, политики, правила, добавленные в исключения).	Все данные, кроме: • файлов, которые в момент обновления Kaspersky Anti Targeted Attack Platform до версии 7.1 находились в очереди на проверку; • файлов, которые в момент обновления Kaspersky Anti Targeted Attack Platform до версии 7.1 находились в очереди на повторную проверку (rescan); • данных отчетов; • разрешающих правил; • параметров коннекторов; • параметров серверов интеграции; • данных алертов старше 360 дней на момент установки обновления. Данные алертов младше 360 дней сохраняются.
База событий.	Все данные.
Хранилище и карантин.	Все данные.
Артефакты Sandbox.	Все данные.

Управление компонентами приложения через меню администратора

Перед входом в меню администратора убедитесь в следующем:

- Доступ к меню администратора и консоли управления серверами Kaspersky Anti Targeted Attack Platform есть только с тех компьютеров, которым вы разрешили этот доступ.
- Компьютеры, которым вы разрешаете доступ, находятся в защищенном периметре вашей сети.

  Вы можете настроить доступ к меню администратора и консоли управления серверами Kaspersky Anti Targeted Attack Platform с определенных компьютеров, с помощью утилиты командной строки iptables. Подробнее о работе с iptables см. документацию к iptables.

Чтобы начать работу в меню администратора компонента:

1. Войдите в консоль управления сервером Central Node, Sensor или Sandbox по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке приложения.

   Отобразится меню администратора компонента.

Как пользоваться меню администратора

Для перемещения между элементами меню используйте клавиши со стрелками **Вверх** и **Вниз**.

Для перехода в выбранный раздел меню нажмите на клавишу **ENTER**.

Для возврата на предыдущий уровень меню выберите пункт **Go back** и нажмите на клавишу **ENTER**.

Для применения заданных настроек выберите пункт **Apply changes** и нажмите на клавишу **ENTER**.

Для выбора горизонтально расположенных кнопок подтверждения используйте клавиши со стрелками **Вправо** и **Влево**.

Для нажатия на выбранную кнопку нажмите на клавишу **ENTER**.

Для завершения работы выберите пункт **Logout**.

Меню администратора Central Node

В меню администратора Central Node доступны следующие возможности:

- Просмотреть текст Лицензионного соглашения, Положения о KSN, Политики конфиденциальности или сведения о стороннем коде:

Legal information → Show EULA

Legal information → Show KSN statement

Legal information → Show privacy policy

Legal information → Third-party code

- Выбрать сетевые протоколы для получения зеркалированного трафика со SPAN-портов:

  Program settings → Configure traffic capture → Setup capture protocols

  По умолчанию получение зеркалированного трафика со SPAN-портов включено по всем сетевым протоколам, кроме **HTTP2**.

- Изменить размер временного хранилища входящего трафика:

  Program settings → Configure storage → Changing the size of the traffic hot ring

- Изменить размер файлового хранилища:

  Program settings → Configure storage → Changing the size of the file storage

  Разделы **Changing the size of the traffic hot ring** и **Changing the size of the file storage** используются для информирования о текущем размере хранилища для входящего трафика и максимальном размере файла, который можно поместить в хранилище. Значения рассчитываются автоматически при настройке параметров масштабирования приложения. Мы настоятельно **не** рекомендуем менять эти значения.

- Настроить срок хранения системных журналов и обнаружений:

  Program settings → Configure storage period for detects and logs → Change storage period

- Настроить параметры сетевого интерфейса:

  Network settings → Interface configuration → <сетевой интерфейс>→ Configuration type

- Изменить дату и время сервера:

  Date and time settings → Now: <дата и время> → Change date

  Date and time settings → Now: <дата и время> → Change time

- Изменить часовой пояс сервера:

  Date and time settings → Configure timezone

- Включить или выключить синхронизацию с NTP-серверами:

  Date and time settings → Enable NTP synchronization

- Добавить или удалить NTP-сервер:

  Date and time settings → NTP: <N> item(s) → New (добавление нового NTP-сервера)

  Date and time settings → NTP: <N> item(s) → <NTP-сервер> (удаление ранее добавленного NTP-сервера)

- Посмотреть SSH-ключи сервера:

  System administration → Show SSH host keys

- Создать резервную копию данных сервера:

  System administration → Backup/Restore settings → New

- Восстановить данные из резервной копии:

  System administration → Backup/Restore settings → <имя файла резервной копии>

- Изменить пароль администратора:

  System administration → Change admin password

- Перейти в режим Technical Support Mode:

  Technical Support Mode

- Загрузить системные журналы или удалить ранее загруженные:

  Download system logs → New (загрузка нового системного журнала)

  Download system logs → <системный журнал> (удаление ранее загруженного системного журнала)

- Перезагрузить сервер:

  Reboot the machine

- Выключить сервер:

  Power-off the machine

- Завершить работу с меню администратора и выйти:

  Logout

Меню администратора Sensor

Если вы выбрали сетевые протоколы для получения зеркалированного трафика со SPAN-портов, настроили размер файлового хранилища или пропускную способность при захвате трафика на отдельном Sensor **до** подключения его к Central Node и хотите изменить эти параметры **после** подключения, вам нужно выполнить шаги по подготовке к изменению параметров. После того, как подготовка будет выполнена, вы можете изменить параметры.

В меню администратора Sensor доступны следующие возможности:

- Просмотреть текст Лицензионного соглашения, Положения о KSN, Политики конфиденциальности или сведения о стороннем коде:

  Legal information → Show EULA

  Legal information → Show KSN statement

  Legal information → Show privacy policy

  Legal information → Third-party code

- Посмотреть TLS-сертификат, используемый сервером:

  Program settings → Manage server certificate → View certificate info

- Применить ранее загруженный TLS-сертификат:

  Program settings → Manage server certificate → Install from file

- Сгенерировать новый TLS-сертификат для сервера:

  Program settings → Manage server certificate → Generate new

- Скачать TLS-сертификат, используемый сервером:

  Program settings → Manage server certificate → Get current certificate

- Выбрать сетевые протоколы для получения зеркалированного трафика со SPAN-портов:

  Program settings → Configure traffic capture → Setup capture protocols

  По умолчанию получение зеркалированного трафика со SPAN-портов включено по всем сетевым протоколам, кроме **HTTP2**.

- Задать пропускную способность при захвате трафика:

  Program settings → Configure traffic capture → Traffic capture bandwidth (Mbps)

- Изменить размер файлового хранилища:

  Program settings → Configure storage → Changing the size of the file storage

- Изменить размер временного хранилища входящего трафика:

  Program settings → Configure storage → Changing the size of the traffic hot ring

  > Этот раздел используется для информирования о текущем размере хранилища для входящего трафика. Размер хранилища рассчитывается автоматически при настройке параметров масштабирования приложения. Мы настоятельно **не** рекомендуем менять это значение.

- Задать ограничение на размер файла, отправляемого на проверку в Central Node:

  Program settings → Configure object processing → File size limit

- Настроить срок хранения системных журналов и обнаружений:

  Program settings → Configure storage period for detects and logs → Change storage period

- Включить или выключить использование прокси-сервера:

  Program settings → Configure Proxy → Enabled

- Задать IP-адрес прокси-сервера:

  Program settings → Configure Proxy →Host

- Задать порт прокси-сервера:

  Program settings → Configure Proxy →Port

- Задать имя пользвателя для аутентификации на прокси-сервере:

  Program settings → Configure Proxy →Username

- Изменить параметры интеграции с прокси-сервером:

  Program settings → Configure Proxy →Edit

- Включить или выключить использование прокси-сервера при подключении к локальным адресам сети:

  Program settings → Configure Proxy → Local addresses

- Настроить параметры сетевого интерфейса:

  Network settings → Interface configuration → <сетевой интерфейс>→ Configuration type

- Настроить параметры DNS:

  Network settings → DNS resolver configuration

- Изменить дату и время сервера:

Date and time settings → Now: <дата и время> → Change date

Date and time settings → Now: <дата и время> → Change time

- Изменить часовой пояс сервера:
  Date and time settings → Configure timezone
- Включить или выключить синхронизацию с NTP-серверами:
  Date and time settings → Enable NTP synchronization
- Добавить или удалить NTP-сервер:
  Date and time settings → NTP: <N> item(s) → New (добавление нового NTP-сервера)
  Date and time settings → NTP: <N> item(s) → <NTP-сервер> (удаление ранее добавленного NTP-сервера)
- Изменить пароль администратора:
  Passwords → Change the system administrative account password
- Посмотреть SSH-ключи сервера:
  System administration → Show SSH host keys
- Настроить соединение по протоколу SNMP:
  System administration → SNMPd monitoring settings
- Перейти в режим Technical Support Mode:
  Technical Support Mode
- Загрузить системные журналы или удалить ранее загруженные:
  Download system logs → New (загрузка нового системного журнала)
  Download system logs → <системный журнал> (удаление ранее загруженного системного журнала)
- Перезагрузить сервер:
  Reboot the machine
- Выключить сервер:
  Power-off the machine
- Завершить работу с меню администратора и выйти:
  Logout

Меню администратора Sandbox

В меню администратора Sandbox доступны следующие возможности:

- Перейти в режим Technical Support Mode:
  Technical Support Mode
- Настроить параметры сетевых интерфейсов:
  Network settings → Management interface

- Настроить доступ в интернет с виртуальных машин в Sandbox:
  Network settings → Malware interface
- Настроить сетевые маршруты:
  Network settings → IPv4 Routes
- Настроить параметры DNS:
  Network settings → DNS Settings
- Изменить пароль администратора:
  Change the system administrative account password
- Перезагрузить сервер:
  Reboot the machine
- Выключить сервер:
  Power-off the machine
- Завершить работу с меню администратора и выйти:
  Logout

Использование KATA и KEDR API

Вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с внешними системами, чтобы управлять действиями по реагированию на угрозы, проверять хранящиеся в этих системах файлы и предоставлять внешним системам доступ к информации обо всех обнаружениях и событиях приложения.

Вызовы методов API доступны только для авторизованных внешних систем. Для авторизации администратору приложения необходимо создать запрос на интеграцию внешней системы с приложением. После этого администратор должен обработать запрос в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

Если вы развернули компоненты Central Node и Sensor в виде кластера, вы можете настроить отказоустойчивую интеграцию с внешней системой одним из следующих способов:

- Использовать функцию Round Robin.
- Настроить параметры внешней системы таким образом, чтобы при возникновении таймаута внешняя система переключалась между IP-адресами серверов кластера.

Чтобы настроить отказоустойчивую интеграцию с внешней системой с помощью функции Round Robin:

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.
2. В параметрах почтового сервера укажите это доменное имя.

Интеграция с внешней системой будет настроена по доменному имени. Внешняя система обратится к случайному серверу кластера. При отказе этого сервера внешняя система будет обращаться к другому работоспособному серверу кластера.

Интеграция внешней системы с Kaspersky Anti Targeted Attack Platform

Для начала работы с API необходимо выполнить интеграцию внешней системы с Kaspersky Anti Targeted Attack Platform. Внешняя система должна пройти авторизацию на сервере Kaspersky Anti Targeted Attack Platform.

Чтобы выполнить интеграцию внешней системы с Kaspersky Anti Targeted Attack Platform:

1. Сгенерируйте уникальный идентификатор внешней системы для авторизации в Kaspersky Anti Targeted Attack Platform – `sensorId`.

2. Сгенерируйте сертификат сервера внешней системы.

3. Создайте любой запрос от внешней системы в Kaspersky Anti Targeted Attack Platform, содержащий идентификатор `sensorId`. Например, вы можете создать запрос на проверку объекта из внешней системы в Kaspersky Anti Targeted Attack Platform.

В веб-интерфейсе Kaspersky Anti Targeted Attack Platform отобразится запрос на авторизацию от внешней системы. Обратитесь к администратору приложения для обработки запроса.

Если вам нужно сменить сертификат сервера внешней системы, выполните действия по интеграции внешней системы в Kaspersky Anti Targeted Attack Platform повторно.

API для проверки объектов внешних систем

Kaspersky Anti Targeted Attack Platform предоставляет HTTPS REST интерфейс проверки объектов, хранящихся во внешних системах.

Для проверки объектов, хранящихся во внешних системах, рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

1. **Создание запроса на проверку объектов HTTP-методом `POST`**

2. **Создание запроса на получение результатов проверки HTTP-методом `GET`**

   Интерфейс API является асинхронным, то есть Kaspersky Anti Targeted Attack Platform выполняет проверку объектов не в момент обращения внешней системы, а в фоновом режиме. Поэтому для получения результатов проверки требуется периодически отправлять запрос от внешней системы HTTP-методом `GET`. Рекомендуемая периодичность отправки запроса 1 раз в минуту.

   Вы также можете настроить отправку уведомлений об обнаруженных объектах в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

3. **Создание запроса на удаление результатов проверки HTTP-методом `DELETE`**

   Вы можете удалить результаты проверки указанного объекта или всех объектов.

Работа с кластером

Если внешняя система представляет собой несколько серверов, объединенных в кластер, рекомендуется использовать один идентификатор (`sensorId`) для всех серверов. В этом случае в веб-интерфейсе Kaspersky Anti Targeted Attack Platform будет отображаться один запрос на интеграцию для всей системы. При необходимости разграничить получение результатов проверки по отдельным серверам вы можете назначить каждому серверу уникальный идентификатор экземпляра (`sensorInstanceId`).

Ограничения

В конфигурационном файле Kaspersky Anti Targeted Attack Platform установлены максимально допустимое количество запросов на проверку объектов от внешних систем и максимально допустимый размер проверяемого объекта.

Если превышено максимально допустимое количество одновременных запросов на проверку объектов, Kaspersky Anti Targeted Attack Platform перестает обрабатывать дальнейшие запросы до тех пор, пока количество запросов на проверку объектов не станет меньше максимально допустимого. До этого времени выдается код возврата 429. Необходимо повторить запрос на проверку позже.

Если превышен максимально допустимый размер объекта, Kaspersky Anti Targeted Attack Platform не проверяет этот объект. При создании запроса HTTP-методом `POST` выдается код возврата 413. Вы можете узнать максимально допустимый размер объекта, просмотрев список ограничений приложения на проверку объектов с помощью метода `GET`.

Запрос на проверку объектов

Для создания запроса на проверку объектов используется HTTP-метод `POST`. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Вы можете задавать параметры выполнения команды cURL с помощью дополнительных ключей (см. таблицу ниже).

Подробную информацию о ключах команд cURL см. в документации cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/scanner/v1/sensors/<идентификатор sensorId>/scans?sensorInstanceId=
<идентификатор sensorInstanceId>" -F "content=<путь к файлу, который вы хотите
проверить>" -F scanId=<идентификатор запроса на проверку> -F "objectType=file"
```

При успешной обработке запроса отобразится статус `"OK"`.

Параметры

Параметр	Тип	Описание
`sensorId`	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`content`	file	Содержимое проверяемого объекта.

Параметр	Тип	Описание
`scanId`	string	Уникальный идентификатор запроса на проверку. Должен быть сформирован на стороне внешней системы. Не может содержать пробелы и специальные символы. Не используйте имена файлов в качестве идентификатора запроса на проверку. Если этот параметр не указан, просмотр результатов проверки недоступен.
`objectType`	string	Тип проверяемого объекта. Возможное значения параметра: `file`.
`sensorInstanceId`	string	Уникальный идентификатор экземпляра внешней системы. Экземплярами внешней системы считаются также серверы, объединенные в кластер. Параметр не является обязательным.

Возвращаемое значение

Код возврата	Описание
`200`	Запрос на проверку объектов успешно создан.
`401`	Требуется авторизация.
`429`	Превышено количество запросов. Повторите запрос позднее.
`500`	Внутренняя ошибка сервера. Повторите запрос позднее.

Пример ввода команды с параметрами

```
curl --cert /root/cert.pem --key /root/server.key -
X POST "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans?
sensorInstanceId=instance1" -F "content=@/tmp/test" -F scanId=1 -F "objectType=file"
```

Запрос на получение результатов проверки

Для создания запроса на получение результатов проверки используется HTTP-метод `GET`. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Вы можете задавать параметры выполнения команды cURL с помощью дополнительных ключей (см. таблицу ниже).

Подробную информацию о ключах команд cURL см. в документации cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X
GET<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/scanner/v1/sensors/<идентификатор sensorId>/scans/state?sensorInstanceId=
<идентификатор sensorInstanceId>&state=<один или несколько статусов проверки, которые вы
хотите отобразить в результатах проверки>"
```

При успешной отправке запроса отобразится список запросов на проверку объектов и результаты проверки этих объектов. Результаты проверки будут отфильтрованы по статусам, которые вы указали в параметре `state`. Например, если в запросе на получение результатов проверки вы указали статусы `state=processing,detect`, отобразятся только запросы на проверку объектов, которые находятся в обработке или в которых приложение обнаружило угрозу.

Параметры

Параметр	Тип	Описание
`sensorId`	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`state`	array (тип элементов string)	Статус проверки объекта. При указании этого параметра результаты проверки будут отфильтрованы по статусу. Указывайте один или несколько статусов через запятую. Возможны следующие значения параметра: • `detect`; • `not detected`; • `processing`; • `timeout`; • `error`.
`sensorInstanceId`	string	Уникальный идентификатор экземпляра внешней системы. Экземплярами внешней системы считаются также серверы, объединенные в кластер. Параметр не является обязательным.

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Scans

type Scans struct {
   ScanID  integer `json:"scanId"`
   State   array   `json:"state"`
}
```

Возвращаемое значение

Код возврата	Описание
`204`	Нет содержимого.
`404`	Не найдены результаты проверки по указанному идентификатору.
`500`	Внутренняя ошибка сервера. Повторите запрос позднее.

Пример ввода команды с параметрами, если вы хотите отобразить все статусы проверки объектов в результатах проверки

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/state?
sensorInstanceId=instance1&state=detect,not%20detected,processing,error,timeout"
```

Запрос на удаление результатов проверки

Для создания запроса на удаление результатов проверки одного или нескольких объектов используется метод `DELETE`. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X DELETE "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/scanner/v1/sensors/<идентификатор sensorId>/scans/<идентификатор scanId>"
```

При успешной обработке запроса результаты проверки объекта будут удалены. Отобразится статус `"OK"`.

Параметры

Параметр	Тип	Описание
`sensorId`	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`scanId`	string	Уникальный идентификатор запроса на проверку объекта. Если этот параметр не задан, будут удалены результаты проверки всех объектов.

Возвращаемое значение

Код возврата	Описание
`200`	Запрос на удаление результатов проверки успешно создан.
`401`	Требуется авторизация.
`404`	Не найдены результаты проверки по указанному идентификатору.
`500`	Внутренняя ошибка сервера. Повторите запрос позднее.

Пример ввода команды

```
curl --cert /root/cert.pem --key /root/server.key -
X DELETE "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/1"
```

Запрос на вывод ограничений приложения на проверку объектов

Для создания запроса на вывод ограничений приложения на проверку объектов (например, по размеру) используется HTTP-метод `GET`. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/scanner/v1/sensors/<идентификатор sensorId>/scans/filters"
```

При успешной обработке запроса отобразятся ограничения приложения на проверку объектов. Например, ограничение `maxObjectSize` – максимально допустимый размер объекта, который вы можете отправить на проверку.

Параметры

Параметр	Тип	Описание
`sensorId`	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
   MaxObjectSize integer `json:"maxObjectSize"`
   Version       string  `json:"version"`
}
```

Возвращаемое значение

Код возврата	Описание
401	Требуется авторизация.
500	Внутренняя ошибка сервера. Повторите запрос позднее.

Пример ввода команды

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/filters"
```

API для получения внешними системами информации об алертах

Kaspersky Anti Targeted Attack Platform предоставляет интерфейс API для доступа внешних систем к информации обо всех алертах, а не только о результатах проверки объектов, хранящихся в этих внешних системах.

Вы можете указать в параметрах запроса фильтры, чтобы получить информацию только о тех алертах, которые удовлетворяют требуемым условиям.

> При появлении новых алертов приложение не отправляет информацию о них автоматически на основе предыдущих запросов. Для получения актуальной информации требуется отправить повторный запрос.

Особенности работы в распределенном решении

Если приложение работает в режиме распределенного решения, то вам нужно настроить интеграцию с внешней системой для каждого сервера PCN и SCN, с которого вы хотите получать информацию об алертах, отдельно. Ограничение связано с тем, что в веб-интерфейсе сервера PCN отображается информация обо всех алертах, однако в базе алертов хранятся только те алерты, которые были зарегистрированы на этом сервере.

Запрос на вывод информации об алертах

Вы можете создать запрос на получение информации об алертах, созданных в результате проверки следующими технологиями:

- Anti-Malware Engine.
- Sandbox.
- YARA.
- URL Reputation.
- Intrusion Detection System.
- Intrusion Detection System (NDR).
- Aggregated Alerts (NDR).

Информация об алертах, созданных в результате проверки технологиями Targeted Attack Analyzer и IOC, недоступна для запроса через API.

Для создания запроса на вывод информации об алертах Kaspersky Anti Targeted Attack Platform используется HTTP-метод `GET`. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/scanner/v1/sensors/<идентификатор sensorId>/detects?detect_type=<одна или
несколько технологий, при проверке которыми создан алерт>&limit=<количество алертов в
ответе на запрос>&token=<идентификатор запроса>"
```

При успешной обработке запроса отобразится список алертов, созданных приложением Kaspersky Anti Targeted Attack Platform на сервере внешней системы.

Параметры

Параметр	Тип	Описание
`sensorId`	String	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`detect_type`	Array	Технология, при проверке которой создан алерт. Возможно указать несколько технологий через запятую. Возможные значения: • `am` – Anti-Malware Engine; • `sb` – Sandbox; • `yara` – YARA; • `url_reputation` – URL Reputation; • `ids` – `Intrusion Detection System`. • `NDR_Ids` – Intrusion Detection System (NDR). • `NDR_External` – Aggregated Alerts (NDR). Если параметр не указан, предоставляется информация обо всех перечисленных выше алертах.
`limit`	Integer	Количество объектов, информация о которых будет предоставлена в ответ на запрос. Допустимые значения: целые числа от 1 до 10000. По умолчанию установлено значение `1000`.
`token`	String	Идентификатор запроса. При указании этого параметра в повторном запросе не отображается информация об обнаружениях, полученная в предыдущих запросах. Это позволяет избежать дублирования информации об одних и тех же алертах при повторных запросах. Если этот параметр не указан, предоставляется информация обо всех алертах.

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
   Detects array  `json:"detects"`
   Token   string `json:"token"`
}
```

Возвращаемое значение

Код возврата	Описание
`400`	Ошибка ввода параметров.
`429`	Превышено количество запросов.
`401`	Требуется авторизация.
`500`	Внутренняя ошибка сервера. Повторите запрос позднее.

Пример ввода команды с параметрами

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/detects?detect_type=am,sb&limit=100&token=7b226f6666736574223a20307d"
```

Состав передаваемых данных

Информация, передаваемая о каждом обнаружении, представлена в таблице ниже.

Состав передаваемых данных об алерте

Параметр	Значение	Описание
`alertID`	Целочисленное значение.	Идентификатор алерта.
`eventTimeStamp`	Дата и время.	Время события.
`detectTimestamp`	Дата и время.	Время занесения информации об алерте в базу Kaspersky Anti Targeted Attack Platform.
`importance`	Одно из следующих значений: • `high`; • `medium`; • `low`.	Важность алерта.
`objectSource`	Одно из следующих значений: • `web`; • `mail`; • `endpoint`; • `external`; • `dns`.	Источник обнаруженного объекта.
`technology`	Одно из следующих значений: • `am` – Anti-Malware Engine; • `sb` – Sandbox; • `yara` – YARA; • `url_reputation` – URL Reputation; • `ids` – Intrusion Detection System.	Технология, с помощью которой обнаружен объект.
`objectType`	Одно из следующих значений: • `file`; • `email`; • `host` (для удаленных доменов или хостов).	Тип обнаруженного объекта. Если обнаружение выполнено при проверке сообщения электронной почты (тип объекта `email`), в информации об обнаружении также могут передаваться следующие данные: • `mailFrom` – адрес источника сообщения; • `rcptTo` – адрес назначения сообщения.
`object`	Зависит от типа обнаруженного объекта.	Данные об обнаруженном объекте.
`detection`	Зависит от технологии, с помощью которой обнаружен объект.	Данные о найденных угрозах.
`details`	Зависит от источника обнаруженного объекта.	Данные об окружении обнаруженных объектов.

Данные об обнаруженных объектах

Состав передаваемых данных об обнаруженных объектах в зависимости от типа объекта приведен в таблице ниже.

	Параметр	Тип данных	Описание	Пример
file	processedObject.MD5	MD5	MD5-хеш файла или составного объекта, переданного на проверку.	1839a1e9621c58dadf782e131df3821f
	processedObject.SHA256	SHA256	SHA256-хеш файла или составного объекта, переданного на проверку.	7bbfc1d690079b0c591e146c4294305da1cee857e12db40f431
	processedObject.fileName	String	Имя файла или составного объекта, переданного на проверку.	EICAR-CURE.com
	processedObject.fileType	String	Тип файла или составного объекта, переданного на проверку.	GeneralTxt
	processedObject.fileSize	Integer	Размер файла или составного объекта, переданного на проверку, в байтах.	184
	detectedObject.MD5	MD5	MD5-хеш файла (простого объекта или файла внутри составного объекта), в котором обнаружена угроза.	1839a1e9621c58dadf782e131df3821f
	detectedObject.fileName	String	Имя файла (простого объекта или файла внутри составного объекта), в котором обнаружена угроза.	EICAR-CURE.com
	detectedObject.fileSize	Integer	Размер файла (простого объекта или файла внутри составного объекта), в котором обнаружена угроза, в байтах.	184
URL	detectedObject	String	URL-адрес обнаруженного объекта.	http://example.com/link
host	detectedObject	Array	Список доменов, к которым относятся обнаруженные объекты. Для технологии URL, а также для объектов с параметром objectSource=dns список может содержать несколько доменов.	example.org, example.net

Данные о найденных угрозах

Состав передаваемых данных о найденных угрозах в зависимости от технологии, с помощью которой выполнено обнаружение, приведен в таблице ниже.

Данные о найденных угрозах

Технология	Параметр	Описание	Тип данных	Пример
Одна из следующих технологий: • Anti-Malware Engine. • YARA. • Intrusion Detection System.	`detect`	Список найденных угроз.	Array	`HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic`
	`dataBaseVersion`	Версия баз, с помощью которых проверен файл.	Integer	`201811190706`
Sandbox	`detect`	Список найденных угроз.	Array	`HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic`
	`image`	Имя образа виртуальной машины, на которой был проверен файл.	String	`Win7`
	`dataBaseVersion`	Версия баз в следующем формате: `<версия баз приложения, с помощью которых проверен файл> / <версия баз модуля IDS>`.	Integer	`201902031107/ 201811190706`
URL Reputation	`detect`	Список категорий URL Reputation для обнаруженного объекта (для объектов типа `URL` или `host`).	Array	`Phishing host, Malicious host, Botnet C&C(Backdoor.Win32.Mokes)`

Данные об окружении обнаруженных объектов

Состав передаваемых данных об окружении обнаруженных объектов в зависимости от источника объекта приведен в таблице ниже.

Данные об окружении обнаруженных объектов

Источник объекта	Параметр	Описание	Тип данных	Пример
web	sourceIP	IP-адрес компьютера, установившего соединение.	IP address	192.0.2.0
	sourceHostname	Имя компьютера, установившего соединение.	String	example.com
	destinationIp	IP-адрес компьютера, с которым установлено соединение.	IP address	198.51.100.0
	destinationPort	Порт компьютера, с которым установлено соединение.	Integer	3128
	URL	URL-адрес интернет-ресурса, к которому выполнено обращение. Для обнаружений, выполненных технологией IDS, этот параметр отсутствует. Для обнаружений, выполненных технологией URL, этот параметр совпадает с параметром detectedObject.	String	https://example.com:443/
	method	Метод HTTP-запроса.	String	Connect
	referrer	URL-адрес, на который была выполнена переадресация.	String	https://example.com:443/
	agentString	Заголовок User agent из HTTP-запроса, содержащий название и версию клиентского приложения.	String	Mozilla/4.0
mail	mailFrom	Адрес электронной почты отправителя.	String	sender@example.com
	mailTo	Список адресов электронной почты получателей через запятую.	Array	recipient1@example.com, recipient2@example.com
	subject	Тема сообщения.	String	'You are the winner'

Источник объекта	Параметр	Описание	Тип данных	Пример
	`messageId`	ID сообщения электронной почты.	String	`1745028736.156014.1542897410859.JavaMail.svc_jira_poc`
• `endpoint` • `external`	`hostName`	Имя компьютера, на котором выполнено обнаружение.	String	`computername.example.com`
	`IP`	IP-адрес компьютера, на котором выполнено обнаружение.	IP address	`198.51.100.0`
`dns`	`sourceIp`	IP-адрес компьютера, инициировавшего соединение по протоколу DNS.	IP address	`192.0.2.0`
	`destinationIp`	IP-адрес компьютера, с которым установлено соединение по протоколу DNS (как правило, DNS-сервера).	IP address	`198.51.100.0`
	`destinationPort`	Порт компьютера, с которым установлено соединение по протоколу DNS (как правило, DNS-сервера).	Integer	`3128`
	`dnsMessageType`	Тип DNS-сообщения: • `Request`. • `Response`.	String	`Request`
	`dnsRequestType`	Один из следующих типов записи DNS-запроса: • `A`. • `AAA`. • `CNAME`. • `MX`.	String	`MX`
	`domainToBeResolved`	Имя домена из DNS-запроса.	String	`example.com`

API для получения внешними системами информации о событиях приложения

Kaspersky Anti Targeted Attack Platform предоставляет интерфейс API для доступа внешних систем к информации о зарегистрированных приложением событиях.

Вы можете указать в параметрах запроса фильтры, чтобы получить информацию только о тех событиях, которые удовлетворяют требуемым условиям.

При появлении новых событий приложение не отправляет информацию о них автоматически на основе предыдущих запросов. Для получения актуальной информации требуется отправить повторный запрос.

Информация о новых событиях доступна для получения не более двух часов после их появления в базе Kaspersky Anti Targeted Attack Platform.

Особенности работы в распределенном решении

Если приложение работает в режиме распределенного решения, то вам нужно настроить интеграцию с внешней системой для каждого сервера PCN и SCN, с которого вы хотите получать события, отдельно. Ограничение связано с тем, что в веб-интерфейсе сервера PCN отображается информация обо всех событиях, однако в базе событий хранятся только те события, которые были зарегистрированы на этом сервере.

Запрос на вывод информации о событиях

Для создания запроса на вывод информации о событиях используется HTTP-метод GET.

Вы можете задавать параметры выполнения команды cURL с помощью дополнительных ключей (см. таблицу ниже).

Подробную информацию о ключах команд cURL см. в документации cURL.

При первом запросе Kaspersky Anti Targeted Attack Platform создает *ContinuationToken* (далее также "токен"). Приложение передает события, доступные в системе на момент создания токена. При создании нового токена Kaspersky Anti Targeted Attack Platform отправляет события, доступные в системе на момент создания этого токена.

Токен содержит информацию о том, какие данные были переданы последними. Если вы хотите получать события, записанные с момента последнего запроса, вам нужно сохранить созданный токен и использовать его в следующих запросах.

Синтаксис команды

Для первого запроса:

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/events_api/v1/<идентификатор external_system_id>/events"
```

При успешной обработке запроса отобразится информация о запрошенных событиях и значение токена.

Для следующих запросов:

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/events_api/v1/<идентификатор external_system_id>/events&continuation_token=
<значение токена, полученное при первом запросе>"
```

При успешной обработке запроса отобразится информация о событиях, полученных с момента последнего запроса.

Вы можете создать запрос на вывод информации о событиях, указав максимальные время сбора и количество событий, а также параметры фильтрации событий:

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/events_api/v1/<идентификатор external_system_id>/events?filter=<фильтр для
событий>&max_timeout=<максимальное время сбора событий>&max_events=<максимальное
количество событий>&continuation_token=<значение токена, полученное при первом запросе>"
```

Если при первом запросе вы указали значение параметра `filter`, при повторном запросе вы можете его не указывать: параметры фильтрации сохраняются от предыдущего запроса и используются в случае, если не указаны новые. Если вы не хотите использовать фильтрацию, не указывайте значение для параметра.

Параметры

Параметр	Тип	Описание
`external_system_id`	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`filter`	string	Параметры фильтрации событий. Задаются с помощью языка запросов для работы с событиями.
`max_timeout`	int	Максимальное время сбора событий. Указывается в формате PT<значение, выраженное целым числом>S. Например, PT300S. Сервер отправляет информацию о событиях, собранную за указанное время. Значение по умолчанию – 5 минут. Это значение используется, если в запросе не указано другое. Максимальное время сбора событий не должно превышать 5 минут. Если вы укажете значение, превышающее 5 минут, сервер Central Node вернет ошибку. Фактическое полное время ожидания событий может быть увеличено.
`max_events`	int	Максимальное количество событий. Если в запросе не указано значение, Kaspersky Anti Targeted Attack Platform вычисляет его, исходя из количества хостов, на которые установлен компонент Endpoint Agent. Примеры значений для типовых конфигураций: • Для 1000 хостов – 64000. • Для 5000 хостов – 128000. • Для 10000 хостов – 208000. • Для 15000 хостов – 288000. • Для 30000 хостов – 528000. Указанное в запросе значение не должно их превышать.
`continuation_token`	string	Значение токена.

Пример ввода команд с параметрами

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET
"https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-3d23b20dd609/events"
```

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET
"https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-3d23b20dd609/events?
filter=EventType=='threatdetect' OR
EventType=='threatprocessingresult'&max_timeout=PT300S&max_events=64000&continuation_token=
CiQyZDcyNjNiOS0zZmNlLTQxNzktYTdhOC03N2E0ZmUwNjNjMTkSBAgAEAoSBAgBEAMSBAgCEAsSBAgDEAcSBAgEEAgSBAgFEAkSBAgGEAQSBAg
HEAUSBAgIEAcSBAgJEAMYiYyCmvIw"
```

Если значения параметров содержат специальные символы, вам необходимо в запросах использовать кодирование URL или команду `--data-urlencode`.

Пример ввода команд с параметрами с использованием кодирования URL

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET
"https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-3d23b20dd609/events?
filter=EventType=='threatdetect' OR
EventType=='threatprocessingresult'&max_timeout=PT300S&max_events=64000&continuation_token=
CiQ%3Dcy%7ENiOS0zZmNlLTQxNzktYTdhOC03N2E0Z40%wNjNjMTkSBAgAEAoSBAgB%5EMSB%3CEAsSBAgDEAcSBAgEEAgSBAgFEAkSBAgGEAQSBAg
HEAUSBAgIEAcSBAgJEAMYiYyCmvIw"
```

Пример ввода команд с параметрами с использованием команды `--data-urlencode`

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> --GET -d "max_events=64000" -d
"max_timeout=PT300S" -d "filter=EventType=='threatdetect'" --data-urlencode "continuation_token=
CiQ?Dcy~NiOS0zZmNlLTQxNzktYTdhOC03N2E0Z@wNjNjMTkSBAgAEAoSBAgB^MSB?CEAsSBAgDEAcSBAgEEAgSBAgFEAkSBAgGEAQSBAg
HEAUSBAgIEAcSBAgJEAMYiYyCmvIw" https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-
3d23b20dd609/events
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
   Events            array  `json:"events"`
   ContinuationToken  string `json:"continuationToken"`
}
```

Возвращаемое значение

Код возврата	Описание
`400`	Ошибка ввода параметров.
`401`	Требуется авторизация.
`500, 502, 503, 504`	Внутренняя ошибка сервера. Повторите запрос позднее.

Язык запросов для фильтрации событий

Язык запросов для фильтрации событий поддерживает следующие функции и операторы:

- Функции: `in`.
- Операторы сравнения для значений типа String или Boolean:
  - `==`.
  - `!=`.
- Операторы сравнения для чисел и переменных:
  - `AND`.
  - `OR`.
  - `NOT`.
  - `==`.
  - `!=`.
  - `>`.
  - `>=`.
  - `<`.
  - `<=`.

Вы можете посмотреть список полей, по которым можно отфильтровать события, в разделе Поля для фильтрации событий.

Если вы хотите получить информацию о событиях разного типа, вам нужно создать отдельный запрос для каждого типа событий.

```
EventType=='threatdetect' OR EventType=='threatprocessingresult'
```

Поддерживаются константы числового и строкового типа. Строковые константы заключаются в апострофы: `'example'`. Для строковых констант поддерживаются метасимволы * и ?. Если вы не хотите использовать метасимволы, вам нужно экранировать их: `\*`, `\?`. Также в строковых константах вам нужно экранировать специальные символы.

Поля для фильтрации событий

Список полей для фильтрации событий приведен в таблице ниже.

Если значения полей содержат специальные символы, вам необходимо в запросах использовать кодирование URL или команду `--data-urlencode`.

Список полей для фильтрации событий

Название поля	Тип	Описание
HostName	string	Имя хоста.
HostIp	string	IP-адрес хоста.
EventType	string	Тип события. Может иметь следующие значения: • process – запущен процесс. • process_terminate – завершен процесс. • module – загружен модуль. • connection – удаленное соединение. • applock – правило запрета. • blockdocument – заблокирован документ. • filechange – изменен файл. • windowsevent – журнал событий ОС. • registry – изменение в реестре. • portlisten – прослушан порт. • driver – загружен драйвер. • threatdetect – алерт. • threatprocessingresult – результат обработки алерта. • amsiscan – AMSI-проверка. • process_interpretated_file_run – интерпретированный запуск файла. • process_console_interactive_input – интерактивный ввод команд в консоли.
UserName	string	Имя пользователя.
OsFamily	string	Семейство операционной системы.
OsVersion	string	Версия операционной системы, используемой на хосте.
Ioa.Rules.Id	string	Идентификатор правила TAA (IOA).
Ioa.Rules.Name	string	Информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.
Ioa.Rules.Techniques	string	Техника MITRE.
Ioa.Rules.Tactics	string	Тактика MITRE.
Ioa.Severity	string	Степень важности, присвоенная событию, выполненному по этому правилу TAA (IOA). Может иметь следующие значения: • Low. • Medium. • High.

Название поля	Тип	Описание
loa.Confidence	string	Уровень надежности в зависимости от вероятности ложных срабатываний правила. Может иметь следующие значения: • Low. • Medium. • High.
FileCreationTime	integer	Время создания файла.
DllCreationTime	integer	Время создания библиотеки DLL.
DroppedCreationTime	integer	Время создания измененного файла.
InterpretedFileCreationTime	integer	Время создания интерпретируемого файла.
FileName	string	Имя файла.
DllName	string	Имя библиотеки DLL.
DroppedName	string	Имя измененного файла.
BlockedName	string	Имя заблокированного файла.
InterpretedFileName	string	Имя интерпретируемого файла.
FilePath	string	Путь к директории, в которой располагается файл.
DllPath	string	Путь к директории, в которой располагается библиотека DLL.
DroppedPath	string	Путь к директории, в которой располагается измененный файл.
BlockedPath	string	Путь к директории, в которой располагается заблокированный файл.
InterpretedFilePath	string	Путь к директории, в которой располагается интерпретируемый файл.
FileFullName	string	Полный путь к файлу. Включает путь к директории и имя файла.
DllFullName	string	Полный путь к библиотеке DLL. Включает путь к директории и имя файла.
DroppedFullName	string	Полный путь к измененному файлу. Включает путь к директории и имя файла.
BlockedFullName	string	Полный путь к заблокированному файлу. Включает путь к директории и имя файла.
DetectedName	string	Полный путь к обнаруженному файлу. Включает путь к директории и имя файла.
OriginalFileName	string	Полный путь к исходному файлу. Включает путь к директории и имя файла.
InterpretedFileFullName	string	Полный путь к интерпретируемому файлу. Включает путь к директории и имя файла.
FileModificationTime	integer	Время изменения файла.
DllModificationTime	integer	Время изменения библиотеки DLL.
DroppedModificationTime	integer	Время изменения измененного файла.
InterpretedFileModificationTime	integer	Время изменения интерпретируемого файла.
FileSize	integer	Размер файла.
DllSize	integer	Размер библиотеки DLL.
DroppedSize	integer	Размер измененного файла.
InterpretedFileSize	integer	Размер интерпретируемого файла.
Md5	string	MD5-хеш файла.
DllMd5	string	MD5-хеш библиотеки DLL
DroppedMd5	string	MD5-хеш измененного файла.
InterpretedMd5	string	MD5-хеш интерпретируемого файла.

Название поля	Тип	Описание
DetectedMd5	string	MD5-хеш обнаруженного файла.
Sha256	string	SHA256-хеш файла.
DllSha256	string	SHA256-хеш библиотеки DLL.
DroppedSha256	string	SHA256-хеш измененного файла.
BlockedSha256	string	SHA256-хеш заблокированного файла.
InterpretedSha256	string	SHA256-хеш интерпретируемого файла.
DetectedSha256	string	SHA256-хеш обнаруженного файла.
HijackingPath	string	Вредоносная DLL, помещенная в директорию по стандартному пути обхода, чтобы система загрузила ее раньше, чем исходную DLL.
LogonRemoteHost	string	IP-адрес хоста, с которого был выполнен удаленный вход.
RealUserName	string	Имя пользователя, назначенное ему при регистрации в системе.
EffectiveUserName	string	Имя пользователя, которое было использовано для входа в систему.
Environment	string	Переменные окружения.
ProcessType	integer	Тип процесса. Может иметь следующие значения: • 1 – exec. • 2 – fork. • 3 – vfork. • 4 – clone.
LinuxOperationResult	string	Результат операции. Может иметь следующие значения: • success. • failed.
SystemPid	integer	Идентификатор процесса.
ParentFileFullName	string	Путь к файлу родительского процесса.
ParentMd5	string	MD5-хеш файла родительского процесса.
ParentSha256	string	SHA256-хеш файла родительского процесса.
StartupParameters	string	Параметры запуска процесса.
ParentSystemPid	integer	Идентификатор родительского процесса.
ParentStartupParameters	string	Параметры запуска родительского процесса.
Method	string	Метод HTTP-запроса.
Direction	string	Направление соединения. Может иметь следующие значения: • inbound. • outbound.
LocalIp	string	IP-адрес локального компьютера, с которого была произведена попытка удаленного соединения.
LocalPort	integer	Порт локального компьютера, с которого была произведена попытка удаленного соединения.
RemoteHostName	string	Имя компьютера, на который была произведена попытка удаленного соединения.
RemoteIp	string	IP-адрес компьютера, на который была произведена попытка удаленного соединения.
RemotePort	integer	Порт компьютера, на который была произведена попытка удаленного соединения.
URI	string	Адрес ресурса, к которому произведен запрос HTTP.
KeyName	string	Путь к ключу реестра.
ValueName	string	Имя параметра реестра.
ValueData	string	Значение параметра реестра.

Название поля	Тип	Описание
RegistryOperationType	integer	Тип операции с реестром. Может иметь следующие значения: • 0 – создан ключ реестра. • 1 – удален ключ реестра. • 2 – изменен реестр. • 3 – переименован ключ реестра.
PreviousKeyName	string	Предыдущий путь к ключу реестра.
PreviousValueData	string	Предыдущее имя параметра реестра.
System.EventID.value	string	Идентификатор типа события безопасности в журнале Windows.
LinuxEventType (поле используется для получения типа события, зафиксированного в журнале событий операционных систем Linux и macOS)	string	Тип события. Может иметь следующие значения: • NewUserCreated – создана учетная запись. • UserAccountDeleted – учетная запись пользователя удалена. • GroupCreated – создана группа. • GroupDeleted – изменена группа. • MemberAddedToGroup – учетная запись добавлена в группу. • UserPasswordChanged – изменен пароль учетной записи. • LinuxAuth – выполнена аутентификация в ОС Linux и macOS. • LinuxSessionStart – запущена сессия в ОС Linux и macOS. • LinuxSessionEnd – завершена сессия ОС Linux и macOS. • ServiceStart – запущена служба. • ChangeAccountExpirationDate – изменен срок действия учетной записи. • OperatingSystemShuttingDown – выключена операционная система. • OperatingSystemStarted – запущена операционная система. • ModifyPromiscuousMode – изменена работа неразборчивого режима. • AuditdConfigurationChanged – изменены настройки аудита.
System.Channel.value	string	Имя журнала.
System.EventRecordID.value	string	Идентификатор записи в журнале
System.Provider.Name.value	string	Идентификатор системы, записавшей событие в журнал.
EventData.Data.TargetDomainName.value	string	Доменное имя удаленного компьютера.
EventData.Data.ObjectName.value	string	Имя объекта, инициировавшего событие.
EventData.Data.PackageName.value	string	Имя пакета, инициировавшего событие.
EventData.Data.ProcessName.value	string	Имя процесса, инициировавшего событие.
VerdictName	string	Имя обнаруженного объекта.
RecordId	integer	Идентификатор сработавшего правила.
ProcessingMode	string	Режим проверки. Может иметь следующие значения: • Default – по умолчанию. • OnDemand – при запросе. • OnAccess – при доступе. • OnExecute – при выполнении. • OnDownload – при загрузке. • OnStartup – при запуске приложений. • OnMail – при отправке сообщения. • OnPostpone – при отложенной проверке. • OnDisinfect – при лечении. • OnVulnerability – при поиске уязвимостей. • OnFirstLaunch – при первом запуске. • OnEngineLoad – при запуске системы. • OnQuarantineRescan – при повторной проверке объектов в Хранилище. • OnWebRequest – при веб-запросе. • OnAmsiScan – при проверке AMSI. • OnSystemWatcherScan – при анализе поведения приложений.
DetectedName	string	Имя объекта.

Название поля	Тип	Описание
DetectedObjectType	string	Тип объекта. Может иметь следующие значения: • Unknown – неизвестно. • File – файл. • LogicalDrive – логический диск. • PhysicalDisk – физический диск. • SystemMemory – системная память. • MemoryProcess – память процесса. • MemoryModule – модуль памяти. • MailMsgRef – заголовок References сообщения электронной почты. • MailMsgMime – MIME-вложения. • MailMsgBody – текст сообщения электронной почты. • MailMsgAttach – вложение сообщения электронной почты. • StartUp – объекты автозапуска. • Folder – директория. • Script – скрипт. • Url – URL-адрес. • AmsiStream – поток проверки AMSI.
ThreatStatus	string	Режим обнаружения. Может иметь следующие значения: • Untreated – объект не обработан. • Untreatable – объект не поддается обработке. • NotFound – объект не найден. • Disinfected – объект вылечен. • Deleted – объект удален. • Quarantined – объект помещен на карантин. • AddedByUser – объект добавлен пользователем. • Unknown – неизвестно. • AddedToExclude – объект добавлен в исключения. • Terminated – обработка прервана. • Clear – объект не заражен. • FalseAlarm – ложное срабатывание. • RolledBack – выполнен откат к предыдущему состоянию. • IpNotBlocked – IP-адрес не заблокирован. • IpBlocked – IP-адрес заблокирован. • IpCannotBeBlocked – IP-адрес не может быть заблокирован. • IpBlockIsNotRequired – не требуется блокировка IP-адреса.
UntreatedReason	string	Статус обработки объекта. Может иметь следующие значения: • None – нет данных. • NonCurable – объект невозможно вылечить. • Locked – объект заблокирован. • ReportOnly – приложение работает в режиме *Только отчет*. • NoRights – нет прав на выполнение действия. • Cancelled – обработка отменена. • WriteProtect – объект защищен от записи. • TaskStopped – задача на обработку прервана. • Postponed – действие отложено. • NonOverwritable – объект невозможно перезаписать. • CopyFailed – не удалось создать копию объекта. • WriteError – ошибка записи данных. • OutOfSpace – нет места на диске. • ReadError – ошибка чтения данных. • DeviceNotReady – устройство не готово. • ObjectNotFound – объект не найден. • WriteNotSupported – запись данных не поддерживается. • CannotBackup – не удалось создать резервную копию объекта. • SystemCriticalObject – объект является критическим для системы. • AlreadyProcessed – объект уже был обработан.
InteractiveInputText	string	Команда интерпретатора.
ObjectContent	string	Содержание скрипта, переданного на проверку.
ObjectContentType	integer	Тип содержимого скрипта. Может иметь следующие значения: • 1 – текст. • 2 – двоичный код.

Название поля	Тип	Описание
FileOperationType	integer	Тип операции с файлом. Может иметь следующие значения: • 1 – создан файл. • 2 – изменен файл. • 3 – переименован файл. • 4 – изменены атрибуты файла. • 5 – удален файл. • 6 – прочитан файл.
PreviousFileName	string	Путь к директории, в которой файл располагался ранее.
PreviousFileFullName	string	Полное имя файла, включающее предыдущий путь к директории, в которой файл располагался ранее, и / или предыдущее имя файла.
DroppedFileType	integer	Тип измененного файла. Может иметь следующие значения: • 0 – неизвестно. • 1 – другие файлы. • 2 – образ PE. • 3 – PE DLL. • 4 – ресурсы PE. • 5 – файл ресурсов .NET. • 6 – файл ELF.

API для управления действиями по реагированию на угрозы

Kaspersky Anti Targeted Attack Platform предоставляет интерфейс API для осуществления действий по реагированию на угрозы. Команды на выполнение операций поступают на сервер Central Node, после чего приложение передает их компоненту Endpoint Agent.

С помощью внешних систем вы можете выполнить следующие операции на хостах с компонентом Endpoint Agent:

- Управлять сетевой изоляцией хостов.
- Управлять правилами запрета.
- Запускать приложения.

Все перечисленные операции доступны на хостах, на которых в роли компонента Endpoint Agent используется приложение Kaspersky Endpoint Security для Windows.

Если в роли компонента Endpoint Agent используется Kaspersky Endpoint Security для Linux, вы можете управлять сетевой изоляцией и запускать приложения.

Запрос на получение списка хостов с компонентом Endpoint Agent

Для создания запроса на вывод информации о хостах с компонентом Endpoint Agent используется HTTP-метод GET.

Синтаксис команды

GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/response_api/v1/<идентификатор external_system_id>/sensors"

При успешной обработке запроса отобразится список хостов с компонентом Endpoint Agent.

Вы можете создать запрос на вывод информации о хостах с фильтрами по IP-адресу, имени или идентификатору хоста. Вы можете указать один, несколько или все перечисленные фильтры.

> При указании имени хоста вам нужно учитывать, что фильтр чувствителен к регистру символов.

GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/response_api/v1/<идентификатор external_system_id>/sensors?ip=<IP-адрес хоста>&host=<имя хоста>&sensor_id=<идентификатор sensor_id>"

При успешной обработке запроса отобразится информация о выбранном хосте с компонентом Endpoint Agent.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
ip	string	IP-адрес хоста с компонентом Endpoint Agent.
host	string	Имя хоста с компонентом Endpoint Agent.

Пример ввода команд с параметрами

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/sensors"
```

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/sensors?ip=10.16.40.243&host=host4&sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0"
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response Sensors

type Server struct {
   Version             string  `json:"version"`
},

type Sensors struct {
   SensorID            UUID    `json:"sensorId"`
   HostIP              string  `json:"hostIp"`
   LastAccessTimestamp         `json:"lastAccessTimestamp"`
   Version             string  `json:"version"`
   SelfDefenseState    boolean `json:"selfDefenseState"`
   LicenseStatus       string  `json:"licenseStatus"`
   OSFamily            string  `json:"osFamily"`
   OSName              string  `json:"osName"`
   Capabilities        array   `json:"capabilities"`

}
```

Возвращаемое значение

Код возврата	Описание
400	Требуется авторизация.
401	Ошибка ввода параметров.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Запрос на получение информации о сетевой изоляции и наличии правил запрета для хостов с компонентом Endpoint Agent

Для создания запроса на вывод информации о сетевой изоляции и наличии правил запрета для хостов с компонентом Endpoint Agent используется HTTP-метод GET.

Синтаксис команды

```
GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=
<идентификатор sensor_id>&settings_type=<network_isolation или prevention>"
```

При успешной обработке запроса отобразится список хостов с компонентом Endpoint Agent, для которых на момент выполнения запроса применены правила запрета или сетевой изоляции.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
settings_type	enum	Тип правила - network_isolation или prevention.

Пример ввода команды с параметрами

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation"
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Settings

type Settings struct {
   ExcludedRules             array  `json:"excludedRules"`
   AutoTurnoffTimeoutInSec   int    `json:"autoTurnoffTimeoutInSec"`
}
```

Возвращаемое значение

Код возврата	Описание
400	Требуется авторизация.
401	Ошибка ввода параметров.
404	Не найден указанный хост с компонентом Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка. Повторите запрос позднее.

Управление сетевой изоляцией хостов

Для изоляции хоста с компонентом Endpoint Agent с помощью интерфейса API рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

1. **Создание запроса на получение списка хостов с компонентом Endpoint Agent**
2. **Создание запроса на получение информации о хостах, для которых уже включена сетевая изоляция**
3. **Создание запроса на одну из следующих операций с хостами с компонентом Endpoint Agent:**
   - включение сетевой изоляции;
   - отключение сетевой изоляции;
   - добавление исключения в уже существующее правило сетевой изоляции.

Вы можете управлять созданными правилами сетевой изоляции в веб-интерфейсе приложения.

Запрос на включение сетевой изоляции

Чтобы включить сетевую изоляцию для выбранного хоста, вам требуется добавить правило сетевой изоляции. Для создания запроса используется HTTP-метод POST.

Параметры команды передаются в теле запроса в формате JSON.

Синтаксис команды

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X
POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=
<идентификатор sensor_id>&settings_type=network_isolation" -H 'Content-Type:
application/json' -d '

{

"settings": {

"autoTurnoffTimeoutInSec": <время действия сетевой изоляции>}

}

'
```

При успешной обработке запроса правило сетевой изоляции будет добавлено. Сетевая изоляция для выбранного хоста действует с момента добавления правила.

По истечении времени, указанного при создании запроса, сетевая изоляция перестанет действовать. Правило сетевой изоляции при этом не удаляется. При необходимости вы можете удалить выбранное правило.

Для отключения сетевой изоляции вам требуется создать запрос на отключение выбранного правила.

Параметры

Параметр	Тип	Описание
`external_system_id`	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`sensor_id`	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
`autoTurnoffTimeoutInSec`	integer	Время, в течение которого будет действовать сетевая изоляция хоста. Допустимый диапазон – от 1 до 9999 часов. Время сетевой изоляции указывается в секундах. Например, если вы хотите включить сетевую изоляцию хоста на два часа, вам требуется указать 7200 секунд.

Пример ввода команды с параметрами

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation" -H 'Content-Type: application/json' -d '
{
"settings": {
"autoTurnoffTimeoutInSec": 7200}
}
'
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Settings

type Settings struct {
   ExcludedRules             array   `json:"excludedRules"`
   AutoTurnoffTimeoutInSec   integer `json:"autoTurnoffTimeoutInSec"`
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост с компонентом Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Если вы хотите изменить параметры созданного правила сетевой изоляции, вам требуется создать новый запрос на добавление правила с нужными параметрами.

Запрос на отключение сетевой изоляции

Чтобы отключить сетевую изоляцию для выбранного хоста, вам требуется создать запрос на отключение правила сетевой изоляции. Для создания запроса используется HTTP-метод DELETE.

Синтаксис команды

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X
DELETE "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=
<идентификатор sensor_id>&settings_type=network_isolation"
```

При успешной обработке запроса правило сетевой изоляции будет отключено.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.

Пример ввода команды с параметром DELETE

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X DELETE
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation"
```

Для того чтобы проверить отключение сетевой изоляции, выполните запрос на получение информации о задаче, используя HTTP-метод GET.

Пример ввода команды с параметром GET

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation"| python -m json.tool
```

Если сетевая изоляция отключена, то Kaspersky Anti Targeted Attack Platform возвращает ответ внешней системе в следующем формате:

```
{
  "error": "Not Found"
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост с компонентом Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Запрос на добавление исключения в правило сетевой изоляции

Чтобы добавить исключение для ранее созданного правила сетевой изоляции, вам требуется создать запрос на добавление исключения. Для создания запроса используется HTTP-метод POST.

Параметры команды передаются в теле запроса в формате JSON.

Синтаксис команды

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X
POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=
<идентификатор sensor_id>&settings_type=network_isolation" -H 'Content-Type:
application/json' -d '
```

```
{
"settings":
{"excludedRules": [
{
"direction": "<outbound, inbound или both>",
"protocol": <номер IP-протокола>,
"remoteIpv4Address": "<IP-адрес хоста с компонентом Endpoint Agent, сетевой трафик
которого не должен быть заблокирован>",
"localPortRange":
{
"fromPort": <номер порта>,
"toPort": <номер порта>
}
}
,
{
"direction": "<outbound, inbound или both>",
"protocol": <номер IP-протокола>,
"remoteIpv4Address": "<IP-адрес хоста с компонентом Endpoint Agent, сетевой трафик
которого не должен быть заблокирован>",
"remotePortRange":
{
"fromPort": <номер порта>,
"toPort": <номер порта>
}
}
,
{
"direction": "<outbound, inbound или both>",
"protocol": <номер IP-протокола>,
"remoteIpv4Address": "<IP-адрес хоста с компонентом Endpoint Agent, сетевой трафик
которого не должен быть заблокирован>"
}
]
,
"autoTurnoffTimeoutInSec": <время действия сетевой изоляции>
}
}
'
```

При успешной обработке запроса исключение из правила сетевой изоляции будет добавлено.

Параметры

Параметр	Тип	Описание
`external_system_id`	`UUID`	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`sensor_id`	`UUID`	Уникальный идентификатор хоста с компонентом Endpoint Agent.

`direction`	`array`	Направление сетевого трафика, которое не должно быть заблокировано. Может иметь следующие значения: • inbound; • outbound; • both. Если вы не указали значение параметра, по умолчанию будет применено значение both и приложение будет передавать трафик в обоих направлениях.
`protocol`	`integer`	Номер IP-протокола, назначенный Internet Assigned Numbers Authority (IANA). Если вы не указали значение параметра, по умолчанию сетевая изоляция будет распространена на все протоколы.
`remoteIpv4Address`	`string`	IP-адрес хоста с компонентом Endpoint Agent, сетевой трафик которого не должен быть заблокирован.
`remotePortRange`	`string`	Порт назначения. Вы можете указать порт, только если вы выбрали исходящее (outbound) направление сетевого трафика. Для двунаправленного трафика нельзя задавать диапазон портов.
`localPortRange`	`string`	Порт, с которого устанавливается соединение. Вы можете указать порт, только если вы выбрали входящее (inbound) направление сетевого трафика. Для двунаправленного трафика нельзя задавать диапазон портов.
`autoTurnoffTimeoutInSec`	`integer`	Время, в течение которого будет действовать сетевая изоляция хоста. Допустимый диапазон – от 1 до 9999 часов. Время сетевой изоляции указывается в секундах. Например, если вы хотите включить сетевую изоляцию хоста на два часа, вам требуется указать 7200 секунд.

Пример ввода команды с параметрами

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation" -H 'Content-Type: application/json' -d '
{
"settings":
{"excludedRules": [
{
"direction": "inbound",
"protocol": 6,
"remoteIpv4Address": "10.16.41.0",
"localPortRange":
{
"fromPort": 3389,
"toPort": 3389
}
}
,
{
"direction": "outbound",
"remoteIpv4Address": "10.16.41.1",
"remotePortRange":
{
"fromPort": 13957,
"toPort": 55409
}
}
,
{
"direction": "both",
"protocol": 6,
"remoteIpv4Address": "10.16.41.2"
}
]
,
"autoTurnoffTimeoutInSec": 7200
}
}
'
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Settings
type Settings struct {
   ExcludedRules             array   `json:"excludedRules"`
   AutoTurnoffTimeoutInSec   integer `json:"autoTurnoffTimeoutInSec"`
}
type ExcludedRules struct {
   Direction                 array   `json:"direction"`
   Protocol                  integer `json:"autoTurnoffTimeoutInSec"`
   RemotePortRange           string  `json:"remotePortRange"`
   LocalPortRange            string  `json:"localPortRange"`
}
```

Возвращаемое значение

Код возврата	Описание
`400`	Ошибка ввода параметров.
`401`	Требуется авторизация.
`404`	Не найден указанный хост с компонентом Endpoint Agent.
`500, 502, 503, 504`	Внутренняя ошибка сервера. Повторите запрос позднее.

Если вы хотите изменить параметры созданного исключения, вам требуется создать новый запрос на добавление исключения с нужными параметрами.

Управление правилами запрета

С помощью правил запрета вы можете заблокировать запуск файлов или процессов на выбранном хосте или всех хостах с компонентом Endpoint Agent. Например, вы можете запретить запуск приложений, использование которых считаете небезопасным. Приложение идентифицирует файлы по их хешу с помощью алгоритмов хеширования MD5 и SHA256. Правило запрета, созданное через внешние системы, может содержать несколько хешей файлов.

Через внешние системы вы можете управлять всеми правилами запрета, созданными для одного хоста или всех хостов, одновременно. При создании правила запрета для выбранного хоста через внешние системы Kaspersky Anti Targeted Attack Platform заменяет все правила запрета, назначенные на этот хост, правилом с новыми параметрами. Например, если ранее вы добавили несколько правил запрета для выбранного хоста через веб-интерфейс приложения, а потом добавили правило запрета через внешние системы, все правила запрета, добавленные в веб-интерфейсе, будут заменены добавленным через внешние системы правилом.

При изменении параметров правила запрета, созданного через внешние системы, приложение сохраняет только новые параметры. Например, если вы создали правило запрета, которое содержит хеши для нескольких файлов, и хотите добавить в это правило еще один хеш, вам требуется создать запрос на добавление правила запрета и указать в нем все хеши, для которых вы создавали запрет ранее, и новый хеш.

Описанный сценарий также актуален для правил запрета, назначенных на все хосты.

Для создания правила запрета с помощью интерфейса API рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

1. **Создание запроса на получение списка хостов с компонентом Endpoint Agent**
2. **Создание запроса на получение информации о хостах, для которых существуют правила запрета**
3. **Создание запроса на одну из следующих операций с правилами запрета:**
   - создание правила;
   - удаление правила.

Добавленные правила запрета отображаются в веб-интерфейсе приложения в разделе **Политики**, подразделе **Правила запрета**.

Если вы создаете через внешнюю систему правило запрета для всех хостов, вам требуется предварительно убедиться, что на сервере отсутствует и не применяется к одному или нескольким хостам правило запрета для этого же файла. Это условие также справедливо, если вы хотите создать через внешнюю систему правило запрета для выбранного хоста: вам требуется убедиться, что на сервере отсутствует и не применяется ко всем хостам правило запрета для этого же файла. В противном случае сервер вернет внешней системе ошибку со списком хостов, к которым уже применяется правило запрета.

Если правило запрета, создаваемое через внешнюю систему, содержит несколько хешей файлов, в информации об ошибке указывается только первый файл, вызвавший ошибку. Сведения о других дублирующихся правилах запрета не отображаются.

Для изменения уже созданного через веб-интерфейс или внешние системы правила запрета вам нужно создать запрос на добавление правила запрета с обновленными параметрами.

Запрос на создание правила запрета

Для создания запроса используется HTTP-метод POST. Параметры команды передаются в теле запроса в формате JSON.

Синтаксис команды

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X
POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=
<идентификатор sensor_id или all, если вы хотите создать правило запрета для всех
хостов>&settings_type=prevention" -H 'Content-Type: application/json' -d '

{

"settings": {

"objects": [

{

"file": {

"<sha256 или md5>": "<SHA256- или MD5-хеш файла, запуск которого вы хотите запретить>"

}

},

{
```

```
"file": {

"<sha256 или md5>": "<SHA256- или MD5-хеш файла, запуск которого вы хотите запретить>"

}

}

]

}

}

'
```

При успешной обработке запроса правило запрета будет добавлено. Правило запрета действует с момента добавления.

При необходимости вы можете удалить правило запрета.

Параметры

Параметр	Тип	Описание
`external_system_id`	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`sensor_id`	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
`objects`	string	Тип объекта, запуск которого вы хотите запретить. Возможное значения параметра: file.
`sha256 или md5`	string	SHA256- или MD5-хеш объекта, запуск которого вы хотите запретить.

Пример ввода команды с параметрами

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention" -H 'Content-Type: application/json' -d '
{
"settings": {
"objects": [
{
"file": {
"sha256": "830195824b742ee59390bc5b9302688c778fc95a64e7d597e28a74c03a04dd63"
}
},
{
"file": {
"md5": "d8e577bf078c45954f4531885478d5a9"
}
}
]
}
}
'
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Objects

type Objects struct {
type file struct {
   SHA256 string  `json:"sha256"`
},
type file struct {
   MD5    string  `json:"md5"`
}
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост с компонентом Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Запрос на удаление правила запрета

Вы можете удалить правило запрета с помощью нового запроса с пустыми значениями или запроса с параметром DELETE. Для создания запросов используются HTTP-методы POST и DELETE.

Синтаксис команды для нового запроса

Параметры команды передаются в теле запроса в формате JSON.

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X
POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=
<идентификатор sensor_id или all, если вы хотите удалить правило запрета для всех
хостов>&settings_type=prevention" -H 'Content-Type: application/json' -d '

{

"settings": {

"objects": []

}

}

'
```

Синтаксис команды с параметром DELETE

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X
DELETE "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=
<идентификатор sensor_id или all, если вы хотите удалить правило запрета для всех
хостов>&settings_type=prevention"
```

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.

Пример ввода команды для нового запроса

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention" -H 'Content-Type: application/json' -d '
{

"settings": {

"objects": []

}

}

'
```

Пример ввода команды с параметром DELETE

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X DELETE
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention"
```

При успешной обработке запроса правило запрета будет удалено.

Для того чтобы проверить удаление правила запрета, выполните запрос на получение информации о правиле запрета, используя HTTP-метод GET.

Пример ввода команды с параметром GET

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention"| python -m json.tool
```

Если правило запрета было удалено, то Kaspersky Anti Targeted Attack Platform возвращает ответ внешней системе в следующем формате:

```
{
  "error": "Not Found"
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост с компонентом Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Управление задачей запуска приложения

Для управления задачей запуска приложения с помощью интерфейса API рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

1. **Создание запроса на получение информации о параметрах, времени создания и статусе выполнения задачи**
2. **Создание запроса на одну из следующих операций с задачей:**
   - создание задачи;
   - удаление задачи.

Добавленные задачи отображаются в веб-интерфейсе приложения в разделе **Задачи**.

Запрос на получение информации о задаче

Для создания запроса на получение информации о задаче используется HTTP-метод GET.

Синтаксис команды

```
GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/tasks/<идентификатор
task_id>?settings=<true или false>"
```

При успешной обработке запроса отобразится информация о параметрах, времени создания и статусе выполнения задачи.

Параметры

Параметры	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
task_id	UUID	Уникальный идентификатор задачи.
settings	boolean	Может иметь следующие значения: • true. При указании этого значения отображается информация о параметрах, времени создания и статусе выполнения задачи. • false. При указании этого значения отображается информация о времени создания и статусе выполнения задачи.

Пример ввода команды с параметрами

```
GET https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?settings=<true или false>
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
   State                    `json:"state"`
   LatestStartDateTime      `json:"latestStartDateTime"`
 type Task struct {
 type Schedule struct {
   StartNow          boolean `json:"startNow"`
   ExecCommand       string  `json:"execCommand"`
}
}
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.

Код возврата	Описание
409	Задача с указанным идентификатором уже существует.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Запрос на создание задачи

Для создания запроса на запуск приложения Kaspersky Anti Targeted Attack Platform используется HTTP-метод POST. Параметры команды передаются в теле запроса в формате JSON.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/tasks/<идентификатор
task_id>?sensor_id=<идентификатор sensor_id>&task_type=run_process" -H 'Content-Type:
application/json' -d '

{

"task": {

"shedule": {"startNow": <true или false>},

"execCommand": "<название приложения, которую вы хотите запустить>",

"cmdLineParameters": "<дополнительные параметры запуска файла или выполнения команды>",

"workingDirectory": "<рабочая директория>"

}

}

'
```

При успешной обработке запроса задача на запуск приложения будет создана.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
task_id	UUID	Уникальный идентификатор задачи.

Пример ввода команды с параметрами

```
curl -k --example.cert --example.key -X POST "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&task_type=run_process" -H 'Content-Type: application/json' -d '
{

"task": {

"schedule": {"startNow": true},

"execCommand": "Example.exe",

"cmdLineParameters": "C:\Windows\System32\",

"workingDirectory": "/all"

}

}

'
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
   State                    `json:"state"`
   LatestStartDateTime      `json:"latestStartDateTime"`
 type Task struct {
 type Schedule struct {
   StartNow          boolean `json:"startNow"`
   ExecCommand       string  `json:"execCommand"`
}
}
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.

Код возврата	Описание
404	Задача с указанным идентификатором не найдена.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Если вы хотите изменить параметры созданной задачи, вам требуется создать новый запрос на добавление задачи с нужными параметрами.

Запрос на удаление задачи

Для создания запроса на удаление задачи Kaspersky Anti Targeted Attack Platform используется HTTP-метод DELETE.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X DELETE "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/tasks/<идентификатор
task_id>"
```

При успешной обработке запроса задача на запуск приложения будет удалена.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
task_id	UUID	Уникальный идентификатор задачи.

Пример ввода команды с параметром DELETE

```
curl -k --example.cert --example.key -X DELETE "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-
81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8"
```

При успешной обработке запроса правило запрета будет удалено.

Для того чтобы проверить удаление задачи, выполните запрос на получение информации о задаче, используя HTTP-метод GET.

Пример ввода команды с параметром GET

```
curl -k --example.cert --example.key -X GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?settings=false"| python -m json.tool
```

Если задача была удалена, то Kaspersky Anti Targeted Attack Platform возвращает ответ внешней системе в следующем формате:

```
{
  "error": "Not Found"
}
```

Возвращаемое значение

Код возврата	Описание
`400`	Ошибка ввода параметров.
`401`	Требуется авторизация.
`404`	Задача с указанным идентификатором не найдена.
`500, 502, 503, 504`	Внутренняя ошибка сервера. Повторите запрос позднее.

Использование NDR API

Сервер REST API, который обеспечивает доступ внешних систем к функциональности NDR, функционирует на сервере с компонентом Central Node и обрабатывает запросы с использованием архитектурного стиля взаимодействия REST (Representational State Transfer). Обращения к серверу REST API выполняются по протоколу HTTPS. Вы можете настроить параметры сервера REST API в разделе **Параметры** → **Серверы подключений** (в том числе заменить используемый по умолчанию самоподписанный сертификат на доверенный).

Для представления данных в запросах и ответах используется формат JSON.

Документация с описанием запросов на основе архитектурного стиля REST публикуется в виде онлайн-справки на странице Kaspersky Online Help. Документация представляет собой руководство разработчика на английском языке. В руководстве разработчика также представлены примеры кода и подробные описания вызываемых элементов, которые доступны в запросах к серверу REST API.

Открыть документ с описанием запросов к серверу REST API, версия 4

С помощью Kaspersky Anti Targeted Attack Platform API внешние системы могут выполнять следующие действия:

- получать данные об известных приложению устройствах;
- добавлять, изменять и удалять устройства;
- получать данные о зарегистрированных событиях в трафике сети (событиях NDR);
- отправлять события NDR в Kaspersky Anti Targeted Attack Platform (для регистрации используется системный тип события с кодом 4000005400);
- получать данные об обнаруженных уязвимостях;
- получать сообщения приложения и записи аудита;
- получать данные о разрешающих правилах;
- включать, выключать и удалять разрешающие правила;
- получать данные о рисках, связанных с устройствами;
- получать данные об адресных пространствах;
- отправлять отчет о топологической карте сети в Kaspersky Anti Targeted Attack Platform;
- отправлять, получать и удалять сведения о пользователях на устройствах;
- отправлять и получать сведения о приложениях и патчах на устройствах;
- отправлять и удалять сведения об исполняемых файлах на устройствах;
- отправлять содержимое журналов устройств;

- получать следующие данные о приложении:
  - список серверов с компонентами приложения;
  - список точек мониторинга и их параметры;
  - список поддерживаемых стеков протоколов и их параметры;
  - список типов событий NDR и их параметры;
  - текущее состояние и режимы работы технологий;
  - версия приложения и даты выпуска установленных обновлений;
  - информация о добавленном лицензионном ключе;
  - язык локализации приложения.

Внешние системы, использующие Kaspersky Anti Targeted Attack Platform API, подключаются к компоненту Central Node через коннекторы. Коннекторы обеспечивают безопасное соединение с использованием сертификатов. Для каждой внешней системы, из которой вы хотите отправлять запросы на сервер REST API, вам нужно создать отдельный коннектор в Kaspersky Anti Targeted Attack Platform.

Для соединения с Kaspersky Anti Targeted Attack Platform внешняя система должна использовать токен аутентификации. Kaspersky Anti Targeted Attack Platform выдает токен аутентификации по запросу внешней системы и использует для токена сертификаты коннектора, который был создан для этой системы. Время действия токена аутентификации составляет 10 часов. Внешняя система может обновить токен аутентификации по специальному запросу.

Документация с описанием запросов для выполнения действий с токеном аутентификации публикуется в виде онлайн-справки на странице Kaspersky Online Help. Документация представляет собой руководство разработчика на английском языке.

Открыть документацию с описанием запросов для действий с токеном аутентификации, версия 4

В Kaspersky Anti Targeted Attack Platform API предусмотрены следующие способы работы со внешними системами:

- взаимодействие на основе архитектурного стиля REST;
- взаимодействие по протоколу WebSocket.

Внешние системы могут использовать способ взаимодействия по протоколу WebSocket в Kaspersky Anti Targeted Attack Platform API для создания подписок на изменяемые значения, которые получает приложение.

Обеспечение безопасного взаимодействия при использовании Kaspersky Anti Targeted Attack Platform API

Внешние системы получают доступ к функциям приложения с использованием Kaspersky Anti Targeted Attack Platform API, устанавливая зашифрованные соединения по протоколу HTTPS. Для обеспечения безопасности соединений используются сертификаты, выданные компонентом Central Node Kaspersky Anti Targeted Attack Platform. Компонент выдает сертификаты для коннекторов, через которые подключаются внешние системы.

Для каждой внешней системы в Kaspersky Anti Targeted Attack Platform должен быть создан отдельный коннектор. Подключение через коннектор возможно с использованием только того сертификата, который был выдан компонентом Central Node и сохранен в файле свертки для этого коннектора. Подключение невозможно установить, если внешняя система предъявляет сертификат от другого коннектора, другого компонента Central Node Kaspersky Anti Targeted Attack Platform, или сертификат, используемый для других подключений (например, сертификат компонента Sensor).

После установки зашифрованного соединения внешняя система должна запросить *токен аутентификации* для коннектора, который будет указываться внешней системой в запросах к Central Node REST API.

Токен аутентификации действителен в течение 10 часов после выдачи. При необходимости дальнейшего использования токена внешняя система должна запросить продление времени его действия до наступления момента прекращения действия.

> Сведения о предусмотренных запросах и методах в Kaspersky Anti Targeted Attack Platform API см. в документации для Kaspersky Anti Targeted Attack Platform API.

При обработке запросов от внешних систем Kaspersky Anti Targeted Attack Platform сохраняет в журнале аудита сведения о попытках выполнения следующих операций:

- получение токена аутентификации;
- продление времени действия для токена аутентификации;
- добавление устройства в таблицу устройств;
- изменение сведений об устройстве;
- удаление устройства;
- запрос журнала аудита (при первом чтении записей аудита через коннектор после загрузки веб-сервера).

Создание и использование коннекторов для Kaspersky Anti Targeted Attack Platform API

Для взаимодействия внешней системы с Kaspersky Anti Targeted Attack Platform API вам нужно добавить коннектор для этой системы. При создании коннектора для него требуется указать системный тип **Generic**.

При добавлении коннектора, а также при создании нового файла свертки для этого коннектора Central Node формирует файл свертки, который вам нужно использовать для работы коннектора.

Файл свертки представляет собой архив, содержащий следующие файлы:

- certificates.pfx – содержит в зашифрованном виде открытый ключ сертификата Central Node, а также сертификат, выданный Central Node для коннектора (с закрытым ключом). Содержимое файла зашифровано с использованием пароля, который был указан при добавлении коннектора или при создании нового файла свертки для этого коннектора.

- metadata.json – содержит конфигурационные данные для коннектора. Данные представлены в формате JSON.

Перечисленные файлы вам нужно использовать для подключения внешней системы через коннектор. Для расшифровки файла certificates.pfx и применения содержащегося в нем сертификата с ключами вы можете использовать стандартные методы обработки файлов этого формата (например, команды `openssl`). Адреса, указанные в файле metadata.json, требуются для работы коннектора и отправки запросов к серверу REST API.

Сертификат и конфигурационные данные в файле свертки действительны до тех пор, пока не создан новый файл свертки или пока не удален коннектор в приложении.

Источники информации о приложении

Этот раздел содержит описание источников информации о приложении.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

Страница Kaspersky Anti Targeted Attack Platform на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Anti Targeted Attack Platform вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

Страница Kaspersky Anti Targeted Attack Platform содержит ссылку на интернет-магазин. В нем вы можете приобрести приложение или продлить право пользования приложением.

Страница Kaspersky Anti Targeted Attack Platform в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Anti Targeted Attack Platform в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Anti Targeted Attack Platform, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение приложений "Лаборатории Касперского" на Форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме.

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Anti Targeted Attack Platform, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Anti Targeted Attack Platform.

Kaspersky предоставляет поддержку Kaspersky Anti Targeted Attack Platform в течение жизненного цикла (см. страницу жизненного цикла приложений). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;

- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Глоссарий

Advanced persistent threat (APT)

Сложная целевая атака на IT-инфраструктуру организации с одновременным использованием различных методов проникновения в сеть, закрепления в сети и получения регулярного доступа к конфиденциальным данным.

Anti-Malware Engine

Ядро приложения. Выполняет проверку файлов и объектов на вирусы и другие программы, представляющие угрозу IT-инфраструктуре организации, с помощью антивирусных баз.

Backdoor-программа

Программа, которую злоумышленники устанавливают на взломанном компьютере для того, чтобы повторно получать доступ к этому компьютеру.

Central Node

Компонент приложения. Выполняет проверку данных, исследование поведения объектов, а также публикацию результатов исследования в веб-интерфейс приложения.

CSRF-атака

Cross-Site Request Forgery (также "XSRF-атака"). Атака на пользователей веб-сайтов, использующая уязвимости HTTP-протокола. Атака позволяет производить действия от имени авторизованного пользователя уязвимого веб-сайта. Например, от имени авторизованного пользователя уязвимого веб-сайта злоумышленник может тайно отправлять запрос на сервер сторонней платежной системы для перевода денег на счет злоумышленника.

End User License Agreement

Юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать приложение.

ICAP-данные

Данные, полученные по протоколу ICAP (Internet Content Adaptation Protocol). Протокол позволяет фильтровать и изменять данные HTTP-запросов и HTTP-ответов. Например, производить антивирусную проверку данных, блокировать спам, запрещать доступ к персональным ресурсам. В качестве ICAP-клиента обычно выступает прокси-сервер, который взаимодействует с ICAP-сервером, используя протокол ICAP. Kaspersky Anti Targeted Attack Platform получает данные с прокси-сервера вашей организации после их обработки на ICAP-сервере.

ICAP-клиент

Система, через которую Kaspersky Anti Targeted Attack Platform получает трафик.

Intrusion Detection System

Модуль приложения. Выполняет проверку интернет-трафика на наличие признаков вторжения в IT-инфраструктуру организации.

IOA

Indicator of Attack (индикатор атаки). Описание подозрительного поведения объектов в IT-инфраструктуре организации, которое может являться признаком целевой атаки на эту организацию.

IOC

Indicator of Compromise (индикатор компрометации). Набор данных о вредоносном объекте или действии.

IOC-файл

Файл, содержащий набор индикаторов IOC, при совпадении с которыми приложение считает событие обнаружением и создает алерт. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

Kaspersky Anti Targeted Attack Platform

Решение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как *атаки "нулевого дня"*, *целевые атаки* и сложные целевые атаки *advanced persistent threats* (далее также "*APT*").

Kaspersky Private Security Network

Решение, позволяющее пользователям антивирусных приложений "Лаборатории Касперского" получать доступ к данным Kaspersky Security Network, не отправляя информацию на серверы Kaspersky Security Network "Лаборатории Касперского" со своей стороны.

Kaspersky Secure Mail Gateway

Решение, предназначенное для защиты входящей и исходящей электронной почты от вредоносных объектов и спама, а также выполняющее контентную фильтрацию сообщений. Решение позволяет развернуть виртуальный почтовый шлюз и интегрировать его в существующую почтовую инфраструктуру организации. На виртуальном почтовом шлюзе предустановлена операционная система, почтовый сервер и антивирусное приложение "Лаборатории Касперского".

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Kaspersky Threat Intelligence Portal

Информационная система "Лаборатории Касперского". Содержит и отображает информацию о репутации файлов и URL-адресов.

KATA

Kaspersky Anti Targeted Attack. Функциональный блок приложения Kaspersky Anti Targeted Attack Platform, обнаруживающий угрозы по периметру IT-инфраструктуры предприятия.

KEDR

Kaspersky Endpoint Detection and Response. Функциональный блок приложения Kaspersky Anti Targeted Attack Platform, обеспечивающий защиту компьютеров локальной сети организации.

Kerberos-аутентификация

Механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, позволяющий передавать данные через незащищенные сети. Механизм основан на использовании билета (ticket), который выдается пользователю доверенным центром аутентификации.

Keytab-файл

Файл, содержащий пары уникальных имен (principals) для клиентов, которым разрешается Kerberos-аутентификация, и зашифрованные ключи, полученные из пароля пользователя. Keytab-файлы используются в системах, поддерживающих Kerberos, для аутентификации пользователей без ввода пароля.

MIB (Management Information Base)

Виртуальная база данных, используемая для управления объектами, которые передаются по протоколу SNMP.

MITM-атака

Man in The Middle (человек посередине). Атака на IT-инфраструктуру организации, при которой злоумышленник перехватывает канал связи между двумя точками доступа, ретранслирует и при необходимости изменяет связь между этими точками доступа.

NTP-сервер

Сервер точного времени, использующий протокол Network Time Protocol.

OpenIOC

Открытый стандарт описания индикаторов компрометации (Indicator of Compromise, IOC), созданный на базе XML и содержащий свыше 500 различных индикаторов компрометации.

Sandbox

Компонент приложения. Запускает виртуальные образы операционных систем. Запускает файлы в этих операционных системах и отслеживает поведение файлов в каждой операционной системе для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации.

Sensor

Компонент приложения. Выполняет прием данных.

SIEM-система

Система Security Information and Event Management. Решение для управления информацией и событиями в системе безопасности организации.

SPAN

Switch Port Analyzer. Технология зеркалирования трафика с одного порта на другой.

Syslog

Стандарт отправки и записи сообщений о происходящих в системе событиях, используемый на платформах UNIX™ и GNU/Linux.

Targeted Attack Analyzer

Модуль приложения. Выполняет анализ и проверку сетевой активности программного обеспечения, установленного на компьютеры локальной сети организации, на основе правил TAA (IOA). Выполняет поиск признаков сетевой активности, на которую пользователю Kaspersky Anti Targeted Attack Platform рекомендуется обратить внимание, а также признаков целевых атак на IT-инфраструктуру организации.

TLS-шифрование

Шифрование соединения между двумя серверами, обеспечивающее защищенную передачу данных между серверами сети Интернет.

YARA

Модуль приложения. Выполняет проверку файлов и объектов на наличие признаков целевых атак на IT-инфраструктуру организации с помощью баз YARA-правил, создаваемых пользователями Kaspersky Anti Targeted Attack Platform.

Алерт

Запись об обнаружении или совокупности обнаружений, выполненных в результате проверки объекта модулями и технологиями Kaspersky Anti Targeted Attack Platform. Отображается в таблице алертов.

Альтернативный поток данных

Потоки данных файловой системы NTFS (alternate data streams), предназначенные для размещения дополнительных атрибутов или информации к файлу.

Каждый файл в файловой системе NTFS представляет собой набор потоков (streams). В основном потоке находится содержимое файла. Остальные (альтернативные) потоки предназначены для размещения метаинформации. Потоки можно создавать, удалять, сохранять отдельно, переименовывать и даже запускать как процесс.

Альтернативные потоки могут использоваться злоумышленниками для скрытой передачи или получения данных с компьютера.

Атака "нулевого дня"

Атака на IT-инфраструктуру организации, использующая уязвимости "нулевого дня" в программном обеспечении, которые становятся известны злоумышленникам до момента выпуска производителем программного обеспечения обновления, содержащего исправления.

Вредоносные веб-адреса

Веб-адреса ресурсов, распространяющих вредоносное программное обеспечение.

Дамп

Содержимое рабочей памяти процесса или всей оперативной памяти системы в определенный момент времени.

Зеркалированный трафик

Копия трафика, перенаправляемая с одного порта коммутатора на другой порт этого же коммутатора (локальное зеркалирование) или на удаленный коммутатор (удаленное зеркалирование). Администратор сети может настроить, какую часть трафика зеркалировать для передачи в Kaspersky Anti Targeted Attack Platform.

Kaspersky Anti Targeted Attack Platform поддерживает получение зеркалированного трафика от агрегирующих устройств: брокера сетевых пакетов и сетевого отвода (Network tap). Если к трафику, подаваемому с помощью агрегирующих устройств, применяется фильтрация, аппаратные требования Kaspersky Anti Targeted Attack Platform меняются. Для определения фактических аппаратных требований решения рекомендуется предварительно провести его пилотирование.

Имя субъекта-службы (SPN)

Уникальный идентификатор службы в сети для проверки подлинности по протоколу Kerberos.

Компонент Endpoint Agent

Компонент приложения. Устанавливается на рабочие станции и серверы, входящие в IT-инфраструктуру организации и работающие под управлением операционных систем Microsoft Windows, Linux и macOS. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

Локальная репутационная база KPSN

База данных репутаций объектов (файлов или URL-адресов), которая хранится на сервере Kaspersky Private Security Network, а не на серверах Kaspersky Security Network. Управление локальными репутационными базами осуществляется администратором KPSN.

Мультитенантность

Режим работы, при котором Kaspersky Anti Targeted Attack Platform используется для защиты инфраструктуры нескольких организаций или филиалов одной организации одновременно.

Обнаружение

Результат проверки объекта одним модулем или компонентом приложения.

Правила YARA

Общедоступная классификация вредоносных программ, содержащая сигнатуры признаков целевых атак и вторжений в IT-инфраструктуру организации, по которым Kaspersky Anti Targeted Attack Platform производит проверку файлов и объектов.

Правило TAA (IOA)

Один признак подозрительного поведения объекта в IT-инфраструктуре организации, при совпадении с которым Kaspersky Anti Targeted Attack Platform считает событие обнаружением и создает алерт. Правило TAA (IOA) содержит описание признака атаки и рекомендации по противодействию.

Пропускная способность канала связи

Наибольшая возможная в данном канале связи скорость передачи информации.

Распределенное решение

Двухуровневая иерархия серверов с установленными компонентами Central Node, в которой выделяется главный сервер управления – *Primary Central Node (PCN)* и подчиненные серверы – *Secondary Central Node (SCN)*.

Сигнатура

Код в базах систем защиты информации, содержащий описание известных угроз.

Статус VIP

Статус алертов с особыми правами доступа. Например, алерты со статусом VIP недоступны для просмотра пользователям с ролью **Сотрудник службы безопасности**.

Тенант

Отдельная организация или филиал организации, которому предоставляется решение Kaspersky Anti Targeted Attack Platform.

Техника MITRE

База знаний MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge – Тактики, техники и общеизвестные знания о злоумышленниках) содержит описание поведения злоумышленников, основанное на анализе реальных атак. Представляет собой структурированный список известных техник злоумышленников в виде таблицы.

Трассировка

Отладочное выполнение приложения, при котором после выполнения каждой команды происходит остановка и отображается результат этого шага.

Угрозы нового поколения

Угрозы IT-инфраструктуре организации, способные перезаписывать, изменять, зашифровывать или искажать свои коды так, чтобы невозможно было обнаружить совпадение с сигнатурой в системе защиты информации.

Уязвимость "нулевого дня"

Уязвимость в программном обеспечении, обнаруженная злоумышленниками до момента выпуска производителем программного обеспечения обновления, содержащего исправленный код программы.

Фишинговые URL-адреса

URL-адреса ресурсов, занимающихся получением неправомерного доступа к конфиденциальным данным пользователей. Как правило, целью фишинга является кража различных финансовых данных.

Целевая атака

Атака, направленная на конкретного человека или организацию. В отличие от массовых атак компьютерными вирусами, направленных на заражение максимального количества компьютеров, целевые атаки могут быть направлены на заражение сети определенной организации или даже одного сервера в IT-инфраструктуре организации. Для каждой целевой атаки может быть написана специальная троянская программа.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Flash являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

AMD – товарный знак или зарегистрированный товарный знак Advanced Micro Devices, Inc.

Apple, Mac, Macintosh, macOS и Safari – товарные знаки Apple Inc.

Ubuntu является зарегистрированным товарным знаком Canonical Ltd.

Cisco является зарегистрированным товарным знаком или товарным знаком Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Citrix является зарегистрированным товарным знаком или товарным знаком Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Google, Google Chrome, Android – товарные знаки Google LLC.

Intel, Core и Xeon являются товарными знаками Intel Corporation или ее дочерних компаний.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Excel, Internet Explorer, PowerPoint, PowerShell, Win32, Windows, Windows PowerShell, Windows Server и Windows XP являются товарными знаками группы компаний Microsoft.

Mozilla и Firefox являются товарными знаками Mozilla Foundation в США и других странах.

NVIDIA является зарегистрированным товарным знаком NVIDIA Corporation.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

Java – зарегистрированный товарный знак компании Oracle и/или аффилированных компаний.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

CentOS – товарный знак или зарегистрированный в США и других странах товарный знак Red Hat, Inc. или дочерних компаний.

Schneider Electric – товарный знак компании Schneider Electric.

Siemens – зарегистрированный товарный знак Siemens AG.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.