kaspersky

Kaspersky Endpoint Detection and Response Optimum

Руководство по эксплуатации

Версия программы: 4.0

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 10.07.2025

https://www.kaspersky.ru
https://support.kaspersky.ru

О «Лаборатории Касперского» (https://www.kaspersky.ru/about/company)

Содержание

Справка Kaspersky Endpoint Detection and Response Optimum 4.0

Ключевые функции:

- Сетевая изоляция устройства
- Запрет запуска объектов
- Поиск IOC
- Просмотр списка алертов в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console
- Виджет EDR-алертов в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console

Что нового

Аппаратные и программные требования

Лицензирование

Развертывание и первоначальная настройка решения

Обновление предыдущей версии

Обращение в Службу технической поддержки

О Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum – решение, предназначенное для защиты IT-инфраструктуры организации от сложных кибернетических угроз. Решение сочетает автоматическое обнаружение угроз с возможностью для вас реагировать на эти угрозы для противостояния сложным атакам, в том числе новым эксплойтам (англ. exploits), программам-вымогателям (англ. ransomware), бесфайловым атакам (англ. fileless attacks), а также методам, использующим законные системные инструменты.

Kaspersky Endpoint Detection and Response Optimum выполняет обзор и анализ развития угрозы и предоставляет Специалисту по безопасности или администратору информацию о потенциальной атаке, необходимую для принятия своевременных действий по реагированию, или применяет заданные вами действия по реагированию автоматически.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в ПО на территории США.

Что нового

Kaspersky Endpoint Detection and Response Optimum 4.0 расширяет функциональные возможности Kaspersky Endpoint Security для Mac 12.2:

- Повышено удобство работы с действиями по реагированию для деталей алерта.
- Добавлены сводки алертов.
- IOC-файлы теперь можно редактировать непосредственно в Web Console при создании или изменении параметров задачи Поиск IOC.
- Обнаруженные объекты теперь можно помещать на карантин из деталей алерта.
- Теперь в порядке действий по реагированию на алерт можно поместить файл на карантин, запретить запуск файла или завершить процесс, даже если соответствующий файл относится к категории SCO (System Critical Object).
- Добавлены предупреждения об ограничениях действий задачи «Сетевая изоляция».

Программные требования

Kaspersky Endpoint Detection and Response Optimum 4.0 работает со следующими версиями приложений "Лаборатории Касперского":

- EPP-программа Kaspersky Endpoint Security для Windows со встроенной поддержкой Kaspersky Endpoint Detection and Response Optimum: версии 11.7.0–12.9.

  Kaspersky Endpoint Security для Windows версии или более поздней можно развернуть в режиме Легкого агента в составе решения Kaspersky Security for Virtualization Light Agent. При развертывании в режиме Легкого агента Kaspersky Endpoint Security для Windows также поддерживает функциональность Kaspersky Endpoint Detection and Response Optimum 4.0.

- EPP-программа Kaspersky Endpoint Security для Mac со встроенной поддержкой Kaspersky Endpoint Detection and Response Optimum: 12.1 или более новой версии.

Kaspersky Endpoint Security для Mac требует наличия Kaspersky Security Center Windows 14.2 или более новой версии, Kaspersky Security Center Linux 15.1 или более новой версии или Kaspersky Security Center Cloud Console.

- EPP-программа Kaspersky Endpoint Security для Linux со встроенной поддержкой Kaspersky Endpoint Detection and Response Optimum: 12.1 или более новой версии.

  Вы можете развернуть Kaspersky Endpoint Security для Linux в режиме Легкого агента в составе решения Kaspersky Security для виртуальных сред 6.2 Легкий агент. При развертывании в режиме Легкого агента Kaspersky Endpoint Security для Linux также поддерживает функциональность Kaspersky Endpoint Detection and Response Optimum 4.0.

  Kaspersky Endpoint Security для Linux требует наличия Kaspersky Security Center Windows 14.2 или более новой версии, Kaspersky Security Center Linux 15.1 или более новой версии или Kaspersky Security Center Cloud Console.

- Если ранее использовалась EPP-программа Kaspersky Security for Virtualization 5.2 Light Agent, требующая установки отдельного агента для поддержки Kaspersky Endpoint Detection and Response Optimum, необходимо выполнить миграцию с Kaspersky Security for Virtualization 5.2 Light Agent на Kaspersky Endpoint Security for Windows версии 12.8 или более новой. Более подробную информацию см. в Руководстве по миграции с Легкого агента KSVLA на Легкий агент KES.

- Приложения для централизованного управления безопасностью сети:
  - Kaspersky Security Center Windows версии 13.2 или более поздней;
  - Kaspersky Security Center Linux версии 15.1 или более поздней;
  - Kaspersky Security Center Cloud Console.

Информацию об аппаратных и программных требованиях поддерживаемых приложений см. в справках соответствующих приложений "Лаборатории Касперского":

- Kaspersky Endpoint Security для Windows;
- Kaspersky Endpoint Security для Mac;
- Kaspersky Endpoint Security для Linux;
- Kaspersky Security Center Windows:
  - Kaspersky Security Center Web Console;

    - Сервер администрирования Kaspersky Security Center.
- Kaspersky Security Center Linux;
- Kaspersky Security Center Cloud Console;

Если вы ранее использовали решение совместно с Kaspersky Security для Windows Server, рекомендуем вам выполнить миграцию с Kaspersky Security для Windows Server на версию Kaspersky Endpoint Security для Windows 12.0 или более позднюю, которая содержит встроенный агент. Подробнее о миграции см. в *справке приложения Kaspersky Endpoint Security для Windows* .

Архитектура решения

В состав решения Kaspersky Endpoint Detection and Response Optimum 4.0 входят следующие компоненты:

- EPP-программы с поддержкой функциональности Kaspersky Endpoint Detection and Response Optimum, которые устанавливаются на отдельные устройства, входящие в IT-инфраструктуру. Эти программы осуществляют постоянное наблюдение за процессами, запущенными на защищаемых устройствах, открытыми сетевыми соединениями и изменяемыми файлами.
- Решение для централизованного управления сетевой безопасностью (Kaspersky Security Center или Kaspersky Security Center Cloud Console).
- Kaspersky Sandbox (опциональный компонент, приобретается отдельно), предназначенный для дополнительной проверки подозрительных объектов, обнаруженных EPP-программой. Подробную информацию о Kaspersky Sandbox см. в *справке Kaspersky Sandbox*.
- Средства анализа угроз (Threat Intelligence):
    - Облачная инфраструктура Kaspersky Security Network (далее также KSN), 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.
    - Интеграция с решением Kaspersky Private Security Network (далее также KPSN), предоставляющим возможность получать доступ к репутационным базам KSN, а также другим статистическим данным, не отправляя в KSN данные со своих устройств.

- Интеграция с платформой Kaspersky Threat Intelligence Portal, которая содержит и отображает информацию о репутации файлов и веб-адресов.

- База угроз Kaspersky Threats.

Известные ограничения

Kaspersky Endpoint Detection and Response Optimum версии 4.0 имеет следующие ограничения:

- Для работы с деталями алерта требуется веб-плагин Kaspersky Endpoint Security для Windows версии 11.7.0 или более поздней версии. Детали алерта доступны только в Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console.

- Плагин управления Kaspersky Endpoint Detection and Response версии 15.4 и выше не поддерживает работу с Kaspersky Security Center версии 14.0. Для обновления плагина необходимо использовать Kaspersky Security Center версии 14.2 и выше.

- Детали алерта и подробные результаты выполнения задачи Поиска IOC удаляются по истечении одного месяца после создания.

- При использовании Kaspersky Endpoint Security для Mac:

  - Детали алертов по угрозам, обнаруженным в составных объектах, содержат информацию только о самом обнаруженном объекте без графа цепочки развития угрозы.

  - В Kaspersky Endpoint Security для Mac 12.1 Резервное хранилище используется как файловое хранилище при выполнении задач *Получить файл* и *Помещение файла на карантин*.

- При использовании Kaspersky Endpoint Security для Linux:

  - Вы не можете создавать, запускать или настраивать задачи Kaspersky Endpoint Detection and Response Optimum из командной строки.

- При использовании Kaspersky Endpoint Security для Windows:

  - Вы не можете проверить объект, помещенный на карантин в результате выполнения задачи *Помещения файла на карантин*.

  - Невозможно поместить в карантин альтернативный поток данных (ADS), размер которого превышает 4 МБ. Kaspersky Endpoint Security для Windows пропускает ADS такого размера без уведомления пользователя.

- Kaspersky Endpoint Security для Windows не запускает задачи *Поиска IOC* на сетевых дисках, если путь в свойствах задачи начинается с буквы диска. Kaspersky Endpoint Security для Windows поддерживает только UNC-путь для задач *Поиска IOC* на сетевых дисках. Например, `\\server\shared_folder`.

- При обнаружении индикатора компрометации во время выполнения задачи *Поиска IOC* приложение помещает файл на карантин только терминов FileItem. Помещение файла на карантин для других терминов не поддерживается.

Поддержка мультитенантности в Kaspersky Endpoint Detection and Response Optimum имеет ряд ограничений:

- В Kaspersky Security Center Cloud Console распределение прав возможно только для учетных записей, зарегистрированных через Active Directory.

- При использовании Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console версии 14 и более ранних:

  - Права администратора для организации-тенанта необходимо назначить до создания виртуального Сервера администрирования. После создания виртуального Сервера добавить или удалить учетную запись администратора невозможно.

  - Администраторам виртуальных Серверов администрирования доступны права чтения на основном Сервере.

Подробную информацию об известных ограничениях при использовании Kaspersky Endpoint Security для Windows см. в справке соответствующей версии приложения:

- Kaspersky Endpoint Security для Windows 12.9
- Kaspersky Endpoint Security для Windows 12.8
- Kaspersky Endpoint Security для Windows 12.7
- Kaspersky Endpoint Security для Windows 12.6
- Kaspersky Endpoint Security для Windows 12.5
- Kaspersky Endpoint Security для Windows 12.4
- Kaspersky Endpoint Security для Windows 12.3
- Kaspersky Endpoint Security для Windows 12.2
- Kaspersky Endpoint Security для Windows 12.1
- Kaspersky Endpoint Security для Windows 12.0

- Kaspersky Endpoint Security для Windows 11.11.0
- Kaspersky Endpoint Security для Windows 11.10.0

Подробная информация об известных ограничениях при работе с Kaspersky Endpoint Security для Mac приведена в справке Kaspersky Endpoint Security для Mac .

Лицензирование

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием решения.

Подробнее о лицензировании приложений, входящих в состав решения Kaspersky Endpoint Detection and Response Optimum 4.0 см. в справках приложений:

- Kaspersky Endpoint Security для Windows;
- Kaspersky Endpoint Security для Mac;
- Kaspersky Endpoint Security для Linux;
- Kaspersky Security Center Windows;
- Kaspersky Security Center Linux;
- Kaspersky Security Center Cloud Console;

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 программ, совместимых с Kaspersky Endpoint Detection and Response Optimum.
- При создании нового рабочего пространства в Kaspersky Security Center Cloud Console.
- Прочитав документ license.txt. Этот документ входит в состав дистрибутивов программ, совместимых с Kaspersky Endpoint Detection and Response Optimum.

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 лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Endpoint Detection and Response Optimum, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

- *Пробная*

  Бесплатная лицензия, предназначенная для ознакомления с приложением. Пробная лицензия имеет небольшой срок действия.

  По истечении срока действия пробной лицензии EDR Optimum прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

  Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая*

  Платная лицензия.

  По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Kaspersky Endpoint Detection and Response Optimum вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.

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

О Лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

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

О лицензионном ключе

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

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

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

Лицензионный ключ может быть активным и дополнительным (или резервным).

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы приложения. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В приложении не может быть больше одного активного лицензионного ключа.

Дополнительный (или резервный) лицензионный ключ – лицензионный ключ, подтверждающий право на использование приложения, но не используемый в текущий момент. Дополнительный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Дополнительный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

О коде активации

Код активации – это уникальная последовательность из 20 латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky Endpoint Detection and Response Optimum. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Endpoint Detection and Response Optimum или после заказа пробной версии Kaspersky Endpoint Detection and Response Optimum.

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, обратитесь к партнеру "Лаборатории Касперского", у которого вы приобрели лицензию.

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 Endpoint Detection and Response Optimum или после заказа пробной версии Kaspersky Endpoint Detection and Response Optimum.

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 Kaspersky Security Network

Kaspersky Security Network (далее также *KSN*) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать на веб-сайте "Лаборатории Касперского" .

Инфраструктура KSN

В Kaspersky Security Network есть следующие инфраструктурные решения:

- *Глобальный KSN* – это решение, которое используют большинство приложений "Лаборатории Касперского". Участники KSN получают информацию от Kaspersky Security Network, а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз Kaspersky Security Network.

- *Локальный KSN* – это решение, позволяющее пользователям устройств, на которые установлено приложение Kaspersky Endpoint Detection and Response Optimum или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в KSN со своих устройств. Локальный KSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

    - отсутствие подключения локальных рабочих мест к интернету;

    - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

О предоставлении данных

Для корректной работы компонентов Kaspersky Endpoint Detection and Response Optimum требуется обработка данных на стороне "Лаборатории Касперского".

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

Подробную информацию о данных, предоставляемых при использовании решения Kaspersky Endpoint Detection and Response Optimum 4.0, см. в справке приложений "Лаборатории Касперского", установленных в вашей IT-инфраструктуре:

- Kaspersky Endpoint Security 12.9 для Windows

- Kaspersky Endpoint Security 12.8 для Windows

- Kaspersky Endpoint Security 12.7 для Windows
- Kaspersky Endpoint Security 12.6 для Windows
- Kaspersky Endpoint Security 12.5 для Windows
- Kaspersky Endpoint Security 12.4 для Windows
- Kaspersky Endpoint Security 12.3 для Windows
- Kaspersky Endpoint Security 12.2 для Windows
- Kaspersky Endpoint Security 12.1 для Windows
- Kaspersky Endpoint Security 12.0 для Windows
- Kaspersky Endpoint Security 11.11.0 для Windows
- Kaspersky Endpoint Security 11.10.0 для Windows
- Kaspersky Endpoint Security 11.9.0 для Windows
- Kaspersky Endpoint Security 11.8.0 для Windows
- Kaspersky Endpoint Security 11.7.0 для Windows
- Kaspersky Endpoint Security 12.2 для Mac
- Kaspersky Endpoint Security 12.1 для Mac
- Kaspersky Endpoint Security 12.3 для Linux
- Kaspersky Endpoint Security 12.2 для Linux
- Kaspersky Endpoint Security 12.1 для Linux
- Kaspersky Security Center 15.1 Windows
- Kaspersky Security Center 14.2 Windows
- Kaspersky Security Center 14 Windows
- Kaspersky Security Center 13.2 Windows
- Kaspersky Security Center 15.4 Linux

- Kaspersky Security Center 15.3 Linux
- Kaspersky Security Center 15.2 Linux
- Kaspersky Security Center 15.1 Linux
- Kaspersky Security Center 15 Linux
- Kaspersky Security Center Cloud Console

Активация Kaspersky Endpoint Detection and Response Optimum

Активация решения Kaspersky Endpoint Detection and Response Optimum 4.0 заключается в активации EPP-программ, установленных на защищаемых устройствах, по лицензии, которая включает функциональность Kaspersky Endpoint Detection and Response Optimum 4.0.

Вы можете приобрести лицензию на использование функциональности Kaspersky Endpoint Detection and Response Optimum 4.0 следующими способами:

- в составе лицензии на использование EPP-программы;
- отдельно, но в дополнение к ранее приобретенной лицензии на использование EPP-программы.

Если вы приобрели лицензию Kaspersky Endpoint Detection and Response Optimum 4.0 в составе лицензии на использование EPP-программ, то использование решения станет доступно после того, как вы выполните первоначальную настройку.

Если ранее использовалась EPP-программа Kaspersky Security for Virtualization 5.2 Light Agent, требующая установки отдельного агента для поддержки Kaspersky Endpoint Detection and Response Optimum, необходимо выполнить миграцию с Kaspersky Security for Virtualization 5.2 Light Agent на Kaspersky Endpoint Security for Windows версии 12.8 или более новой. Более подробную информацию см. в Руководстве по миграции с Легкого агента KSVLA на Легкий агент KES.
Если вы ранее использовали решение совместно с Kaspersky Security для Windows Server, рекомендуем вам выполнить миграцию с Kaspersky Security для Windows Server на версию Kaspersky Endpoint Security для Windows 12.0 или более позднюю, которая содержит встроенный агент. Подробнее о миграции см. в *справке Kaspersky Endpoint Security для Windows*.

Если лицензия Kaspersky Endpoint Detection and Response Optimum 4.0 приобреталась отдельно, в дополнение к ранее приобретенной лицензии на использование каких-либо приложений "Лаборатории Касперского" уже после их установки и активации на устройствах, такие приложения на устройствах необходимо активировать заново с помощью нового кода активации или файла ключа — в зависимости от способа приобретения лицензии Kaspersky Endpoint Detection and Response Optimum 4.0. После этого необходимо выполнить первоначальную настройку решения.

Подробнее об активации решения см. в документации EPP-программ "Лаборатории Касперского":

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

Поддерживаемые конфигурации и сценарии развертывания

Возможны следующие сценарии развертывания:

- Первичная установка и развертывание приложений для защиты IT-инфраструктуры и решения Kaspersky Endpoint Detection and Response Optimum 4.0, либо установка Kaspersky Endpoint Detection and Response Optimum 4.0 в инфраструктуре, в которой ранее уже были установлены поддерживаемые версии приложений для защиты IT-инфраструктуры.

- Развертывание в инфраструктуре, где уже используется версия Kaspersky Endpoint Detection and Response Optimum 1.1 или более ранняя, с приложениями для защиты IT-инфраструктуры разных версий и предназначенными для разных типов устройств с разными операционными системами.

Развертывание и первоначальная настройка Kaspersky Endpoint Detection and Response Optimum 4.0

В этом разделе содержится информация о развертывании и первоначальной настройке Kaspersky Endpoint Detection and Response Optimum 4.0 на основе EPP-программ со встроенным агентом.

Развертывание решения Kaspersky Endpoint Detection and Response Optimum 4.0 включает в себя следующие этапы:

1. **Установка решения для централизованного управления безопасностью сети**

Установите Kaspersky Security Center Windows, Kaspersky Security Center Linux или используйте Kaspersky Security Center Cloud Console для управления Kaspersky Endpoint Detection and Response Optimum в вашей инфраструктуре.

> Для Kaspersky Endpoint Security для Mac версии 12.1 или более поздней, Kaspersky Endpoint Security для Linux версии 12.1 или более поздней и Kaspersky Endpoint Security для Windows версии 12.6 или более поздней необходим Kaspersky Security Center Windows 14.2 или более поздней версии или Kaspersky Security Center 15.1 или более поздней версии. Подробную информацию о поддерживаемых версиях программ см. в разделе Программные требования.

2 Установка EPP-программ

Установите EPP-приложения с поддержкой функциональности Kaspersky Endpoint Detection and Response Optimum 4.0 на устройства, которые требуется защищать.

> Подробную информацию о поддерживаемых версиях программ см. в разделе Программные требования.

Информацию об установке см. в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* и в *справке Kaspersky Endpoint Security для Linux*.

3 Установка веб-плагина

Установите веб-плагин EPP-программы для Kaspersky Security Center Web Console.

> Веб-плагины EPP-программы встроены в Kaspersky Security Center Cloud Console по умолчанию.

Подробную информацию об установке веб-плагинов см. в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* и в *справке Kaspersky Endpoint Security для Linux*.

4 Активация Kaspersky Endpoint Detection and Response Optimum

Если ваша лицензия на использование EPP-программ на устройствах включает функциональность Kaspersky Endpoint Detection and Response Optimum 4.0, дополнительных действий не требуется.

Если вы приобрели лицензию на использование Kaspersky Endpoint Detection and Response Optimum 4.0 после установки приложений "Лаборатории Касперского" на устройства, активируйте решение.

5. **Установка плагина Endpoint Detection and Response**

   Установите плагин Endpoint Detection and Response версии 15.4.58 или более поздней для Kaspersky Security Center. Подробнее об установке плагинов см. в *справке Kaspersky Security Center Windows* и в *справке Kaspersky Security Center Linux*.

6. **Создание политики в Kaspersky Security Center**

   Создайте политики, которые будут распространяться на группы устройств, защищаемых EPP-программами.

   Подробную информацию о создании политики см. в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* и в *справке Kaspersky Endpoint Security для Linux*.

7. **Включение Kaspersky Endpoint Detection and Response Optimum на устройствах**

   Выполните интеграцию с EPP-программами и включите решение Kaspersky Endpoint Detection and Response Optimum в параметрах EPP-программы на устройствах. Подробную информацию см. в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* и в *справке Kaspersky Endpoint Security для Linux*.

8. **Настройка отчета об угрозах**

   Настройте отчет об угрозах для просмотра деталей алерта.

9. **Добавление виджета**

   Добавьте виджет EDR-алертов на информационную панель для мониторинга алертов.

10. **Отображение списка алертов**

    Включите отображение раздела **Алерты** в Kaspersky Security Center Web Console, Kaspersky Security Center Linux или Kaspersky Security Center Cloud Console.

Обновление предыдущей версии Kaspersky Endpoint Detection and Response Optimum

Если требуется обновить Kaspersky Endpoint Security для Windows до версии 11.7 или более поздней, Kaspersky Endpoint Detection and Response Optimum также необходимо обновить.
Если ранее решение использовалось совместно с Kaspersky Security для Windows Server, рекомендуется выполнить миграцию с Kaspersky Security для Windows Server на Kaspersky Endpoint Security для Windows версии 12.0 или более поздней, который включает в себя встроенный агент. Подробнее о миграции см. в *справке приложения Kaspersky Endpoint Security для Windows*.

Если Kaspersky Endpoint Detection and Response Optimum 1.1 (или более ранней версии) используется совместно с какими-либо приложениями для защиты IT-инфраструктуры, порядок обновления зависит от того, какое решение используется для централизованного управления безопасностью сети: локальное (Kaspersky Security Center) или облачное (Kaspersky Security Center Cloud Console). Подробнее см. в *справке Kaspersky Security Center*.

Сценарий: локальное обновление через Kaspersky Security Center Web Console

Локальное обновление решения Kaspersky Endpoint Detection and Response Optimum 4.0 включает в себя следующие этапы:

1. **Обновление решения для централизованного управления безопасностью сети**

   Обновите Kaspersky Security Center Windows до версии 15.1 или Kaspersky Security Center Linux до версии 15.4, включая Агенты администрирования на компьютерах пользователей и Kaspersky Security Center Web Console для Windows или Linux.

2. **Установка новой версии веб-плагина**

   Установите веб-плагин Kaspersky Endpoint Security 12.9 для Windows, Kaspersky Endpoint Security 12.2 для Mac или Kaspersky Endpoint Security 12.3 для Linux.

   > Подробную информацию о поддерживаемых версиях программ см. в разделе Программные требования.

   Подробнее об установке веб-плагина см. в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* или в *справке Kaspersky Endpoint Security для Linux*.

3. **Выполнение шагов мастера миграции политик и задач**

   > Если Kaspersky Endpoint Detection and Response Optimum обновляется с версии 2.0 или более поздней, пропустите этот шаг.

   Запустите мастер миграции политик и задач и выполните все шаги мастера.

4. **Обновление EPP-программ**

   Обновите EPP-программы до версии с поддержкой функциональности Kaspersky Endpoint Detection and Response Optimum 4.0 на устройствах, которые требуется защищать.

Подробную информацию о поддерживаемых версиях программ см. в разделе Программные требования.

Информацию об обновлении приложения см. в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* или в *справке Kaspersky Endpoint Security для Linux*. Информацию о миграции конфигурации на Kaspersky Endpoint Security см. в справке *Kaspersky Endpoint Security для Windows*.

5 **Установка плагина Endpoint Detection and Response**

Установите плагин Endpoint Detection and Response версии 15.4.58 или более поздней для Kaspersky Security Center. Подробнее об установке плагинов см. в *справке Kaspersky Security Center Windows* и в *справке Kaspersky Security Center Linux*.

Сценарий: облачное обновление через Kaspersky Security Center Cloud Console

Облачное обновление решения Kaspersky Endpoint Detection and Response Optimum 4.0 включает в себя следующие этапы:

1 **Обновление Агента администрирования**

Обновите Агент администрирования Kaspersky Security Center до версии с поддержкой Kaspersky Endpoint Detection and Response Optimum.

Информацию об Агенте администрирования см. в *Справке Kaspersky Security Center Cloud Console*.

2 **Выполнение шагов мастера миграции политик и задач**

Если Kaspersky Endpoint Detection and Response Optimum обновляется с версии 2.0 или более поздней, пропустите этот шаг.

Запустите мастер миграции политик и задач и выполните все шаги мастера.

3 **Обновление EPP-программ**

Обновите EPP-программы до версии с поддержкой функциональности Kaspersky Endpoint Detection and Response Optimum 4.0 на устройствах, которые требуется защищать.

Подробную информацию о поддерживаемых версиях программ см. в разделе Программные требования.

Информацию об обновлении приложения см. в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* или в *справке Kaspersky Endpoint Security для Linux*. Информацию о миграции конфигурации на Kaspersky Endpoint Security см. в справке *Kaspersky Endpoint Security для Windows*.

Совместная работа с другими решениями "Лаборатории Касперского"

Совместная работа с предыдущими версиями Kaspersky Endpoint Detection and Response Optimum

Если вы обновите Kaspersky Endpoint Detection and Response Optimum 4.0 только на выборочных устройствах в вашей инфраструктуре, то остальные устройства останутся под защитой более ранних версий Kaspersky Endpoint Detection and Response Optimum.

Совместная работа с Kaspersky Sandbox

Приложения Kaspersky Endpoint Security для Windows начиная с версии 11.7 в составе решения Kaspersky Endpoint Detection and Response Optimum 4.0 совместимы с Kaspersky Sandbox версии 2.0 и более поздних. При этом для синхронных обнаружений Kaspersky Sandbox вы сможете открыть детали алерта, предоставляемые функциональностью Kaspersky Endpoint Detection and Response Optimum.

При совместной работе разных EPP-программ в составе решения Kaspersky Endpoint Detection and Response Optimum и Kaspersky Sandbox внутри одной инфраструктуры необходимо обеспечить отдельный сервер Kaspersky Sandbox для версии 1.0 для тех устройств, которые находятся под защитой Kaspersky Security для виртуальных сред 5.2 Легкий агент или Kaspersky Endpoint Security для Windows версий 11.2-11.6, и отдельный сервер Kaspersky Sandbox 2.0 для тех устройств, которые работают под защитой Kaspersky Endpoint Security для Windows начиная с версии 11.7.

Совместная работа с Kaspersky Managed Detection and Response

Лицензия на использование решения Kaspersky Managed Detection and Response позволяет также использовать и решение Kaspersky Endpoint Detection and Response Optimum. Однако только некоторые действия по реагированию, обеспеченные решением Kaspersky Endpoint Detection and Response Optimum, доступны для реагирования на инциденты Kaspersky Managed Detection and Response. Если оба решения одновременно пытаются применить одно и то же действие по реагированию, то оно применяется только в рамках работы одного из решений.

Действия по реагированию, предложенные аналитиками SOC и предпринятые экспертами по безопасности в Kaspersky Managed Detection and Response, не отображаются в параметрах, политиках и задачах Kaspersky Endpoint Detection and Response Optimum.

Действия по реагированию

Этот раздел содержит информацию о действиях по реагированию на обнаруженные угрозы, доступных в рамках Kaspersky Endpoint Detection and Response Optimum 4.0.

О Сетевой изоляции

Kaspersky Endpoint Detection and Response Optimum предоставляет возможность изолировать устройства от сети по требованию (вручную) или в качестве автоматического действия по реагированию на обнаруженные угрозы.

После включения Сетевой изоляции приложение разрывает все активные соединения TCP/IP и блокирует все новые сетевые соединения TCP/IP на изолированных устройствах, кроме следующих соединений:

- соединений, указанных в исключениях из Сетевой изоляции;
- соединений, инициированных службами совместимой EPP-программы;
- соединений, инициированных Агентом администрирования Kaspersky Security Center.

Вы можете применить Сетевую изоляцию устройства вручную в настройках EPP-программы на устройстве или в деталях алерта. Сетевая изоляция устройства также может применяться автоматически в результате ответных действий на алерты при выполнении задачи Поиска IOC. Вы можете разблокировать изолированное устройство вручную из деталей алерта, в параметрах EPP-программы на устройстве или из командной строки. Вы также можете настроить период, по истечении которого Сетевая изоляция будет автоматически отключена.

Вы можете настроить исключения из Сетевой изоляции. Сетевые соединения, подпадающие под заданные исключения, не будут заблокированы на устройствах после включения Сетевой изоляции.

Подробнее об управлении Сетевой изоляцией вручную через параметры EPP-программы на устройстве, настройке параметров автоматического применения Сетевой изоляции через политику Kaspersky Security Center, настройке исключений и возможностях управления Сетевой изоляцией через командную строку см. в *справке Kaspersky Endpoint Security для Windows*, *справке Kaspersky Endpoint Security дял Mac* и в *справке Kaspersky Endpoint Security для Linux*.

Помещение файла на карантин

Одно из возможных действий по реагированию при обнаружении угрозы – помещение файла на карантин.

Карантин представляет собой специальное локальное хранилище на устройстве с EPP-программой, поддерживающей функциональность Kaspersky Endpoint Detection and Response Optimum. Карантин предназначен для хранения обнаруженных файлов, возможно зараженных вирусами или не поддающихся лечению. На защищаемом устройстве файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства.

Вы можете поместить файл на карантин вручную или задать помещение на карантин автоматически в качестве ответных действий на алерты.

Подробные сведения о Карантине приведены в *справке Kaspersky Endpoint Security for Windows*, в *справке Kaspersky Endpoint Security for Mac* и в *справке Kaspersky Endpoint Security for Linux*. Поместить файл на карантин также можно в окне деталей алерта.

Эта функциональность поддерживается в Kaspersky Endpoint Security для Linux 12.2 или более поздней версии.

Если на компьютерах организации установлено приложение Kaspersky Endpoint Security для Windows версии 11.10.0 или более поздней, или Kaspersky Endpoint Security для Mac версии 12.1 или более поздней, это действие по реагированию недоступно для критически важных системных объектов (англ. System Critical Object, далее также SCO). К категории SCO относятся файлы, необходимые для работы операционной системы и Kaspersky Endpoint Security.
В Kaspersky Endpoint Security для Mac версии 12.2 и более поздних это действие по реагированию доступно, даже если соответствующий файл относится к SCO. Рекомендуется использовать эту функцию с осторожностью. По умолчанию для SCO это действие по реагированию отключено, как и в предыдущих версиях Kaspersky Endpoint Security для Mac.

О Cloud Sandbox

Cloud Sandbox – облачная технология, позволяющая обнаруживать сложные угрозы на компьютерах пользователей. Kaspersky Endpoint Security автоматически отправляет требующие проверки файлы в Cloud Sandbox для анализа. Cloud Sandbox запускает эти файлы в изолированной среде для выявления вредоносной активности и принимает решение о репутации этих файлов. Далее данные об этих файлах отправляются в KSN.

В Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Mac вы можете включить отдельный счетчик для угроз, обнаруженных с помощью Cloud Sandbox. Вы можете использовать этот счетчик для составления статистики при анализе обнаруженных угроз.

Для использования этой технологии Cloud Sandbox требуется выполнение следующих условий:

- Для устройств под управлением Windows:
  - на компьютере установлен Kaspersky Endpoint Security для Windows версии 11.10.0 или более поздней;
  - в Kaspersky Security Center установлен плагин Kaspersky Endpoint Security для Windows версии 11.10.0 или более поздней;
  - в Kaspersky Endpoint Security включена поддержка KSN;
  - для просмотра отчетов об алертах в результате срабатывания технологии Cloud Sandbox (в столбце **Cloud Sandbox Отчета об угрозах**), требуется Kaspersky Security Center Windows версии 14 или более поздней, Kaspersky Security Center Linux версии 15.1 или более поздней, или Kaspersky Security Center Cloud Console.
- Для устройств под управлением macOS:
  - на компьютере установлен Kaspersky Endpoint Security для Mac версии 12.1 и более поздней;
  - в Kaspersky Security Center установлен плагин Kaspersky Endpoint Security для Mac версии 12.1 или более поздней;
  - в Kaspersky Endpoint Security включена поддержка KSN;
  - для просмотра отчетов об алертах в результате срабатывания технологии Cloud Sandbox (в столбце **Cloud Sandbox Отчета об угрозах**), требуется Kaspersky Security Center Windows версии 14.2 или более поздней, Kaspersky Security Center Linux версии 15.1 или более поздней, или Kaspersky Security Center Cloud Console.
- Для устройств под управлением Linux:
  - на компьютере установлен Kaspersky Endpoint Security для Linux версии 12.2 и более поздней;
  - в Kaspersky Security Center установлен плагин Kaspersky Endpoint Security для Linux версии 12.2 или более поздней;
  - в Kaspersky Endpoint Security включена поддержка KSN;

- для просмотра отчетов об алертах в результате срабатывания технологии Cloud Sandbox (в столбце **Cloud Sandbox Отчета об угрозах**), требуется Kaspersky Security Center Windows версии 14.2 или более поздней, Kaspersky Security Center Linux версии 15.1 или более поздней, или Kaspersky Security Center Cloud Console.

Дополнительные сведения о включении Cloud Sandbox, запуске проверки файлов с помощью этой технологии вручную и ограничениях на использование технологии Cloud Sandbox см. в разделе Cloud Sandbox справок *Kaspersky Endpoint Security для Windows*, *Kaspersky Endpoint Security для Linux* или *Kaspersky Endpoint Security для Mac*.

Настройка параметров хранения файлов на карантине

Чтобы просмотреть список файлов в карантине,

в главном окне Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Хранилища** → **Карантин**.

Подробнее о работе с Карантином см. в *справке Kaspersky Security Center Windows*, в *справке Kaspersky Security Center Linux* и в *справке Kaspersky Security Center Cloud Console*.

Проверка объектов, помещенных на карантин в рамках работы Kaspersky Endpoint Detection and Response Optimum, недоступна.

Восстановление файлов из карантина также доступно из командной строки. Подробнее см. в справках *Kaspersky Endpoint Security для Windows* и *Kaspersky Endpoint Security для Linux*.

Объекты помещаются на карантин с использованием прав системной учетной записи (SYSTEM). При восстановлении из карантина файл помещается не в исходное расположение, а в специальную папку на устройстве, из которой вы сможете вручную переместить его в папку назначения.

Чтобы настроить параметры хранения файлов в карантине, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики, которую вы хотите настроить.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.

4. В разделе **Репозитории** выберите подраздел **Карантин** и задайте нужные параметры.

   Информация о доступных для настройки параметрах карантина приведена в *справке Kaspersky Endpoint Security для Windows* и в *справке Kaspersky Endpoint Security для Linux*.

Эта функциональность поддерживается в Kaspersky Endpoint Security для Linux 12.2 или более поздней версии.

Kaspersky Endpoint Security для Mac 12.1 использует Резервное хранилище в качестве Карантина. Подробную информацию о параметрах Резервного хранилища см. в *справке Kaspersky Endpoint Security для Mac*.

О задаче Удаления файла

Одно из возможных действий по реагированию при обнаружении угрозы – удаление файла с устройства.

Подробные сведения о создании задачи «Удаление файла» приведены в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* и в *справке Kaspersky Endpoint Security for Linux*.

Если на компьютерах организации установлено приложение Kaspersky Endpoint Security для Windows версии 11.10.0 или более поздней, Kaspersky Endpoint Security для Mac версии 12.1 или более поздней, Kaspersky Endpoint Security для Linux версии 12.1 или более поздней, это действие по реагированию недоступно для критически важных системных объектов (англ. System Critical Object, далее также SCO). К категории SCO относятся файлы, необходимые для работы операционной системы и Kaspersky Endpoint Security. В Kaspersky Endpoint Security для Mac версии 12.2 и более поздних это действие по реагированию доступно, даже если соответствующий файл относится к SCO. Рекомендуется использовать эту функцию с осторожностью. По умолчанию для SCO это действие по реагированию отключено, как и в предыдущих версиях Kaspersky Endpoint Security для Mac.

Запуск проверки важных областей

Одним из возможных действий по реагированию при обнаружении угрозы является запуск проверки важных областей на устройстве.

Вы можете запускать проверку важных областей вручную в Kaspersky Endpoint Security или задать автоматический запуск проверки в качестве ответных действий на алерты.

Автоматический запуск проверки доступен в Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Security для Mac.

Подробная информация о проверке важных областей приведена в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* и в *справке Kaspersky Endpoint Security для Linux*.

О задаче Поиска IOC

Индикатор компрометации (англ. Indicator of Compromise, IOC) – набор данных об объекте или активности, который указывает на несанкционированный доступ к устройству (компрометация данных). Например, индикатором компрометации могут быть неоднократные неудачные попытки входа в систему. Задача Поиска IOC позволяет обнаруживать индикаторы компрометации на устройстве и выполнять действия по реагированию на угрозы.

Файлы IOC используются для поиска IOC. Файлы IOC содержат набор индикаторов, которые сравниваются с индикаторами события. Если сравниваемые показатели совпадают, EPP-программа считает событие алертом. IOC-файлы должны соответствовать стандарту OpenIOC.

Kaspersky Endpoint Detection and Response Optimum позволяет создавать и настраивать вручную групповые и локальные задачи Поиска IOC в Kaspersky Security Center Web Console и Cloud Console. Для запуска задач используются IOC-файлы, которые вы подготовили.

В Kaspersky Endpoint Security для Mac версии 12.2 и более поздних расширены функциональные возможности задачи «Поиск IOC»:

- Поддерживаются IOC-файлы открытого стандарта описания индикаторов компрометации STIX версий 2.0 и 2.1.
- IOC-файлы можно редактировать непосредственно в Web Console при создании или изменении параметров задачи Поиск IOC.
- Задачу «Поиск IOC» можно создать из файла, содержащего хеши файлов (md5 или sha256) или IP-адреса (IPv4 или IPv6).

При обнаружении IOC на устройстве Kaspersky Endpoint Detection and Response Optimum выполняет заданное действие по реагированию. Доступны следующие действия по реагированию на обнаруженные IOC:

- Изолировать устройство от сети.

- Запускать проверку важных областей.
- Копию поместить на карантин, объект удалить.

В Kaspersky Endpoint Security для Mac версии 12.2 и более поздних при просмотре отчета о выполнении задачи «Поиск IOC» можно вручную изолировать устройство или поместить файл на карантин.

Задачу также можно создать вручную в окне деталей алерта или в Kaspersky Endpoint Security для Windows.

Порядок запуска задач «Поиск IOC» подробно описан в в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* и в *справке Kaspersky Endpoint Security для Linux*.

О Запрете запуска

Вы можете настраивать правила запрета запуска исполняемых файлов и скриптов, а также открытия файлов офисного формата на выбранных устройствах. Например, вы можете запретить запуск приложений, которые вы считаете небезопасными, на выбранном устройстве, защищаемом Kaspersky Endpoint Detection and Response Optimum. Приложение идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.

Правило запрета запуска – это набор критериев, которые учитываются при выполнении блокировки объекта. Объект должен соответствовать всем критериям правила запрета запуска, чтобы приложение заблокировало его исполнение.

Kaspersky Endpoint Detection and Response Optimum предусматривает следующие режимы применения правил запрета запуска:

- Блокирование и запись в отчет.

  В этом режиме EPP-программа блокирует исполнение объектов или открытие документов, соответствующих критериям правил запрета запуска.

- Только запись события в отчет.

  В этом режиме Kaspersky Endpoint Security публикует в Журнал событий и Kaspersky Security Center событие о попытках исполнения объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их исполнение или открытие.

Информация о включении и настройке запрета запуска и об управлении правилами запрета запуска из командной строки приведена в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* и в *справке Kaspersky Endpoint Security для Linux*.

Эта функциональность поддерживается в Kaspersky Endpoint Security для Linux 12.2 или более поздней версии.

Вы также можете запретить запуск файла из окна деталей алерта.

Если на компьютерах организации установлено приложение Kaspersky Endpoint Security для Windows версии 11.10.0 или более поздней, или Kaspersky Endpoint Security для Mac версии 12.1 или более поздней, это действие по реагированию недоступно для критически важных системных объектов (англ. System Critical Object, далее также SCO). К категории SCO относятся файлы, необходимые для работы операционной системы и Kaspersky Endpoint Security.
В Kaspersky Endpoint Security для Mac версии 12.2 и более поздних это действие по реагированию доступно, даже если соответствующий файл относится к SCO. Рекомендуется использовать эту функцию с осторожностью. По умолчанию для SCO это действие по реагированию отключено, как и в предыдущих версиях Kaspersky Endpoint Security для Mac. Подробнее см. в *справке Kaspersky Endpoint Security для Windows* или в *справке Kaspersky Endpoint Security для Mac*.

О запуске процесса

Задача Запуска процесса позволяет удаленно запускать файлы на устройстве. Например, вы можете удаленно запустить утилиту, которая создает файл с конфигурацией компьютера. Затем вы можете получить созданный файл с помощью задачи Получить файл.

Подробная информация о создании задачи «Запуск процесса» приведена в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* и в *справке Kaspersky Endpoint Security for Linux*.

О задаче Завершения процесса

Задача Завершения процесса позволяет удаленно завершать процессы на устройстве. Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена с помощью задачи Запуска процесса.

Подробная информация о создании задачи «Завершить процесс» приведена в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* и в *справке Kaspersky Endpoint Security for Linux*.

Если на компьютерах организации установлено приложение Kaspersky Endpoint Security для Windows версии 11.10.0 или более поздней, Kaspersky Endpoint Security для Mac версии 12.1 или более поздней, Kaspersky Endpoint Security для Linux версии 12.1 или более поздней, это действие по реагированию недоступно для критически важных системных объектов (англ. System Critical Object, далее также SCO). К категории SCO относятся файлы, необходимые для работы операционной системы и Kaspersky Endpoint Security. В Kaspersky Endpoint Security для Mac версии 12.2 и более поздних это действие по реагированию доступно, даже если соответствующий файл относится к SCO. Рекомендуется использовать эту функцию с осторожностью. По умолчанию для SCO это действие по реагированию отключено, как и в предыдущих версиях Kaspersky Endpoint Security для Mac.

О задаче Получения файла

Задача Получения файла позволяет получать файлы с устройств пользователей. Например, вы можете настроить получение файла журнала событий, который создает стороннее приложение. Задача помещает файл на карантин. Вы можете загрузить этот файл на устройство из карантина в Kaspersky Security Center Web Console. При этом на устройстве пользователя файл остается в исходной папке.

Когда задача Получения файла выполняется в Kaspersky Endpoint Security для Linux 12.1 или в Kaspersky Endpoint Security для Mac 12.1, файлы сохраняются в Резервном хранилище.

Подробнее о том, как создать задачу Получения файла, см. в *справке Kaspersky Endpoint Security для Windows*, в *справке Kaspersky Endpoint Security для Mac* и в *справке Kaspersky Endpoint Security for Linux*.

Работа с деталями алерта

Этот раздел содержит информацию о действиях, которые можно выполнять непосредственно из окна деталей алерта.

О деталях алерта

Детали алерта содержат всю доступную информацию об обнаруженной угрозе и позволяют управлять действиями по реагированию на алерт.

В деталях алерта приведена следующая информация:

- Граф цепочки развития угрозы, который предоставляет визуальную информацию о задействованных объектах, например, о ключевых процессах на устройстве, сетевых соединениях, библиотеках и кустах реестра.

- Рекомендации по реагированию на алерт. Каждая рекомендация снабжена ссылкой, по которой вы можете перейти к применению выбранного способа реагирования.

  > Для алертов, полученных от Kaspersky Endpoint Security для Windows, этот раздел доступен только в том случае, если на компьютерах организации установлено приложение Kaspersky Endpoint Security для Windows версии 11.9.0 или более поздней, а в Kaspersky Security Center используется плагин Kaspersky Endpoint Security for Windows версии 11.9.0 или более поздней.

- Общая информация об алерте, включая режим обнаружения (например, обнаружение при проверке по требованию или при автоматической проверке).

- Информация о защищаемом устройстве, на котором произошел алерт (например, имя устройства, IP-адрес, MAC-адрес, список пользователей, операционная система).

- Информация об обнаруженном объекте.

- Изменения в реестре, связанные с алертом.

- История появления файлов на устройстве.

- Принятые приложением действия по реагированию.

- Информация о группе доверия, цифровой подписи, данные о распространении файла и другая информация.

  > Эта информация доступна только в том случае, если Kaspersky Security Network был включен до обнаружения угрозы. Для алертов, полученных от Kaspersky Endpoint Security для Windows, эта информация доступна только в том случае, если на устройствах организации установлен Kaspersky Endpoint Security для Windows 11.10.0 или более поздней версии и в Kaspersky Security Center используется плагин Kaspersky Endpoint Security 11.10.0 или более поздней версии.

Если в Kaspersky Security Center вместе с Kaspersky Endpoint Security для Mac версии 12.2 или более поздней используется плагин Kaspersky Endpoint Detection and Response Optimum 15.4.58 или более поздней версии, в деталях алерта дополнительно приводится информация о действиях по реагированию, примененных к объектам, входящим в цепочку развития угрозы, а также сводка цепочки развития угрозы.

Эти данные в деталях алерта указаны на момент обнаружения угрозы. Решение не обновляет эту информацию, поэтому она может отличаться от данных и показателей, отображаемых на Kaspersky Threat Intelligence Portal. Для просмотра актуальных данных воспользуйтесь ссылками на данные Kaspersky Threat Intelligence Portal в деталях алерта.

Из деталей алерта вы можете выполнить следующие действия по реагированию:

- изолировать устройство, на котором произошел алерт;
- поместить файл на карантин;

  > Эта функциональность не поддерживается в Kaspersky Endpoint Security для Linux 12.1.

- создать задачу Поиска IOC;
- запретить запуск обнаруженного файла.

  > Эта функциональность не поддерживается в Kaspersky Endpoint Security для Linux 12.1.

> Детали алерта автоматически удаляются через один месяц после того, как были сформированы.

Если на устройстве с установленным приложением Kaspersky Endpoint Security для Windows объем информации в деталях алерта превышает 1 МБ или если за сутки на устройстве появилось больше пяти алертов, то данные алерта хранятся на этом устройстве локально и для доступа к ним необходимо подключение к этому устройству.

Настройка отчета об угрозах для отображения деталей алертов

Чтобы настроить возможность перейти в окно деталей алерта из отчета об угрозах, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. В списке отчетов установите флажок для отчета шаблона **Отчет об угрозах** и нажмите на кнопку **Открыть свойства шаблона отчета**.
3. В открывшемся окне изменения отчета перейдите на вкладку **Графы**.

4. Убедитесь, что в блоке параметров **Детальные данные** в списке полей отчета присутствует поле с именем **Открыть алерт**.

5. Если поле **Открыть алерт** отсутствует в списке, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

   b. В правой части окна в раскрывающемся списке выберите поле с именем **Открыть алерт**.

   c. Нажмите на кнопку **OK**.

6. Нажмите на кнопку **Сохранить**.

Возможность просмотра деталей алерта настроена в параметрах отчета об угрозах.

Просмотр деталей алерта

Детали алерта доступны в окне со списком алертов. Список алертов доступен в отчете **Отчет об угрозах** или в подразделе **Алерты** в разделе **Мониторинг и отчеты** в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console.

> Если вы добавите лицензионный ключ для Kaspersky Endpoint Detection and Response Optimum, подраздел **Алерты** автоматически отобразится в главном меню в разделе **Мониторинг и отчеты**. Вы также можете настроить отображение подраздела **Алерты** в параметрах интерфейса в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console.

*Чтобы просмотреть детали алерта в разделе **Мониторинг и отчеты**:*

1. В главном окне Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Мониторинг и отчеты** → **Алерты**.

2. Выберите алерт и нажмите на ссылку **Подробнее**.

   Отобразятся детали алерта.

Чтобы просмотреть детали алерта в отчете об угрозах:

1. В главном окне Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.

2. Выберите отчет шаблона **Отчет об угрозах** и нажмите на кнопку **Показать отчет**.

3. В окне отчета на вкладке **Подробнее** выберите алерт и нажмите на ссылку **Открыть детали алерта**.

   Отобразятся детали алерта.

Чтобы открыть детали алерта, Kaspersky Endpoint Detection and Response Optimum необходимо получить данные с устройства, на котором произошел алерт. Если данные или устройство недоступны, отобразится сообщение об ошибке. Время ожидания ответа от устройства может составить несколько минут.

При использовании Kaspersky Security Center Cloud Console для просмотра могут быть доступны только первые пять деталей обнаружения. Чтобы иметь возможность просматривать все отображаемые в отчете детали обнаружения, необходимо использовать в сети точку распространения и настроить ее в качестве извещающего сервера, а в свойствах политики Агента администрирования включить параметр **Использовать точку распространения для принудительного подключения к Серверу администрирования**.

Подробнее о просмотре деталей алерта в Kaspersky Security Center Linux см. в *справке Kaspersky Security Center Linux*.

Применение и снятие Сетевой изоляции устройства

Чтобы изолировать устройство от сети или снять Сетевую изоляцию устройства из окна деталей алерта, выполните следующие действия:

1. Откройте окно деталей алерта.

2. В блоке **Компьютер** нажмите на кнопку:

   - **Изолировать компьютер от сети** – чтобы применить Сетевую изоляцию к этому устройству.

     В Kaspersky Endpoint Security для Mac версии 12.2 и более поздних можно настраивать параметры включения Сетевой изоляции устройства.

   - **Разблокировать изолированный от сети компьютер** – чтобы снять Сетевую изоляцию с этого устройства.

Кнопка **Разблокировать изолированный от сети компьютер** доступна, если получен алерт от Kaspersky Endpoint Security для Windows версии 11.7 или более поздней, Kaspersky Endpoint Security для Linux версии 12.1 или более поздней, Kaspersky Endpoint Security для Mac версии 12.1 или более поздней.

Помещение файла на карантин из деталей алерта

Чтобы поместить файл на карантин из деталей алерта, выполните следующие действия:

1. Откройте детали алерта.
2. В блоке **Файл** нажмите на кнопку **Поместить на карантин**.

   Файл будет удален с устройства. Его копия будет помещена на карантин.

Эта функциональность поддерживается в Kaspersky Endpoint Security для Linux 12.2 или более поздней версии.

Создание задачи Поиска IOC из деталей алерта

Чтобы создать задачу Поиска IOC из деталей алерта, выполните следующие действия:

1. Откройте детали алерта.
2. На вкладке **Все события алерта** выберите элементы списка, на основе которых вы хотите создать задачу Поиска IOC.
3. Нажмите на кнопку **Создать IOC**.
4. Выберите условие срабатывания индикатора компрометации:
   - Если вы хотите, чтобы IOC срабатывал при обнаружении любого из выбранных объектов, в правой части экрана выберите **ИЛИ**.
   - Если вы хотите, чтобы IOC срабатывал только при обнаружении всех выбранных объектов, в правой части экрана выберите **И**.
5. Выберите действия, которые необходимо применять при срабатывании IOC:
   - Изолировать устройство от сети.
   - Запускать проверку важных областей.

- Поместить копию на карантин, объект удалить.

6. Нажмите на кнопку **Создать задачу**.

Вы можете просмотреть созданные задачи в разделе **Устройства** → **Задачи**.

При создании задачи Поиска IOC из деталей алерта для выбранного объекта (файла или процесса) будет автоматически создан IOC с термином **FileItem**. Подробные сведения о терминах IOC приведены в *справке Kaspersky Endpoint Security для Windows*, *справке Kaspersky Endpoint Security для Mac* и *справке Kaspersky Endpoint Security для Linux*.

Запрет запуска файла из деталей алерта

Чтобы правила запрета запуска файла могли применяться на устройстве, на котором произошел алерт, к этому устройству должна быть применена активная политика приложения с поддержкой функциональности Kaspersky Endpoint Detection and Response Optimum. Если устройство, на котором произошел алерт, не находится под управлением активной политики, то правило запрета запуска не будет создано. Например, если на устройстве установлена EPP-программа Kaspersky Endpoint Security для Windows, к этому устройству должна применяться политика Kaspersky Endpoint Security для Windows.

Чтобы запретить запуск файла из деталей алерта, выполните следующие действия:

1. Откройте детали алерта.

2. В блоке **Файл** нажмите на кнопку **Запретить запуск**.

Запуск файла будет запрещен. Правило запрета запуска будет добавлено в политику для группы, в которую входит устройство.

Эта функциональность поддерживается в Kaspersky Endpoint Security для Linux 12.2 или более поздней версии.

Мониторинг и отчеты

Для наблюдения за работой Kaspersky Endpoint Detection and Response Optimum доступны следующие возможности:

- виджет EDR-алертов;
- список алертов;
- отчеты и выборки Kaspersky Security Center.

Добавление виджета EDR-алертов

В виджете EDR-алертов отображается информация о количестве алертов на устройствах за последний месяц. Виджет доступен для отображения на вкладке **Панель мониторинга** в Kaspersky Security Center Web Console или в Kaspersky Security Center Cloud Console. Из виджета вы можете перейти в раздел **Алерты** со списком алертов на устройствах.

Чтобы добавить виджет EDR-алертов на информационную панель:

1. Перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.
2. Нажмите на кнопку **Добавить или восстановить веб-виджет**.
3. В списке доступных веб-виджетов выберите веб-виджет **Алерты** в категории **Статистика угроз**.
4. Нажмите на кнопку **Добавить**.

   Веб-виджет будет добавлен в конец информационной панели.

Подробнее о работе с виджетами см. в *справке Kaspersky Security Center Web Console* или в *справке Kaspersky Security Center Cloud Console*.

Просмотр списка алертов

Чтобы просмотреть все алерты в виде списка,

в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Алерты**.

Раздел **Алерты** появляется автоматически при активации Kaspersky Endpoint Detection and Response Optimum. Вы также можете включить отображение этого раздела в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console.

Из списка алертов вы можете перейти в детали выбранного алерта.

Проверка работоспособности Kaspersky Endpoint Detection and Response Optimum на устройствах

Kaspersky Security Center позволяет получить информацию о текущем статусе защиты на устройствах и о том, на каких устройствах в вашей инфраструктуре не установлена EPP-программа с поддержкой Kaspersky Endpoint Detection and Response Optimum.

Вы можете получить эту информацию, построив выборку устройств по статусу компонента EDR Optimum.

Чтобы построить выборку устройств по статусу компонента EDR Optimum:

1. В Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Устройства** → **Выборки устройств**.

2. Создайте новую выборку устройств со следующим условием:

    a. Выберите раздел **Информация о программах "Лаборатории Касперского".**

    b. В списке **Компоненты программы** выберите компонент **Endpoint Detection and Response** для EPP-программ, установленных на ваших устройствах.

    c. В раскрывающемся списке **Статус** выберите необходимое значение критерия выборки. Отобразятся устройства с выбранным статусом работы Kaspersky Endpoint Detection and Response Optimum.

    d. Нажмите на кнопку **Сохранить**.

    Новая выборка отобразит список устройств с выбранным статусом Kaspersky Endpoint Detection and Response Optimum.

Просмотр информации о срабатывании правил запрета запуска

Kaspersky Security Center позволяет получить информацию о приложениях, запуск которых был заблокирован решением Kaspersky Endpoint Detection and Response Optimum в результате срабатывания правила запрета запуска объектов.

Чтобы просмотреть отчет о приложениях, запуск которых был запрещен:

1. В Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.

2. В списке отчетов выберите нужный отчет:

    - **Отчет о запрещенных приложениях**

      Выберите эту опцию, чтобы просмотреть информацию о приложениях, запуск которых был запрещен в режиме *Блокировать и записывать в отчет*.

- **Отчет о запрещенных приложениях в тестовом режиме**

  Выберите эту опцию, чтобы просмотреть информацию о приложениях, запуск которых был запрещен в режиме *Только записывать в отчет*.

Получение списка изолированных устройств

Kaspersky Security Center позволяет получить информацию об устройствах, к которым была применена Сетевая изоляция.

Вы можете получить эту информацию, построив выборку устройств по тегу `ISOLATED FROM NETWORK`.

Чтобы построить выборку устройств, изолированных от сети:

1. Если вы хотите построить выборку устройств главного сервера или подчиненных серверов, выполните предварительную дополнительную настройку:

   1. В Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Устройства** → **Теги** → **Теги устройств**.

   2. Нажмите на кнопку **Добавить** и добавьте тег `ISOLATED FROM NETWORK` в список тегов устройств.

2. В Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Устройства** → **Выборки устройств**.

3. Создайте новую выборку устройств со следующим условием:

   a. Выберите раздел **Теги**.

   b. Нажмите на кнопку **Добавить** и создайте условие выборки всех устройств, обозначенных тегом `ISOLATED FROM NETWORK`.

   c. Для выборки устройств подчиненных серверов, дополнительно установите флажок **Включать данные подчиненных Серверов администрирования**.

Новая выборка отобразит список устройств, изолированных от сети.

Мультитенантность

Мультитенантность – это режим, при котором решение используется для защиты инфраструктуры нескольких организаций одновременно.

Вы можете использовать Kaspersky Endpoint Detection and Response Optimum для защиты инфраструктуры нескольких организаций одновременно с помощью Kaspersky Security Center. Для этого вам требуется создать виртуальные Серверы администрирования организаций, для защиты которых вы хотите использовать Kaspersky Endpoint Detection and Response Optimum. Эти виртуальные Серверы администрирования должны быть созданы на Сервере администрирования организации-провайдера. Подробнее о создании виртуальных Серверов администрирования см. в *справке Kaspersky Security Center Windows*, в *справке Kaspersky Security Center Linux* и в *справке Kaspersky Security Center Cloud Console*.

Для каждой организации-тенанта необходимо создать отдельный виртуальный Сервер администрирования и создать учетные записи администраторов виртуальных Серверов. Сведения о настройке учетных записей администратора см. в *справке Kaspersky Security Center Windows* и в *справке Kaspersky Security Center Cloud Console*.

Администратор основного Сервера администрирования может управлять решением на всех устройствах, которые управляются этим Сервером. Администратор виртуального Сервера администрирования может управлять решением только на устройствах, подключенных к серверу, который он администрирует.

Поддержка мультитенантности в Kaspersky Endpoint Detection and Response Optimum имеет ряд ограничений:

- В Kaspersky Security Center Cloud Console распределение прав возможно только для учетных записей, зарегистрированных через Active Directory.
- При использовании Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console версии 14 и более ранних:
  - Права администратора для организации-тенанта необходимо назначить до создания виртуального Сервера администрирования. После создания виртуального Сервера добавить или удалить учетную запись администратора невозможно.
  - Администраторам виртуальных Серверов администрирования доступны права чтения на основном Сервере.

Работа с Kaspersky Endpoint Detection and Response Optimum через Kaspersky Security Center OpenAPI

При локальном развертывании Kaspersky Endpoint Detection and Response Optimum с использованием Kaspersky Security Center Web Console доступна автоматизация и пользовательская настройка ряда рабочих сценариев и задач с помощью Kaspersky Security Center OpenAPI.

Подробнее о работе с OpenAPI см. в *справке Kaspersky Security Center Windows* и в *справке Kaspersky Security Center Linux*.

В примере ниже представлен скрипт для применения изоляции компьютера от сети с помощью Kaspersky Security Center OpenAPI.

Пример скрипта:

```
# #!/usr/bin/python -tt
# -*- coding: utf-8 -*-

import sys
import os
import argparse
import socket
import time
import getpass
import urllib3
from sys import platform
from urllib.parse import urlparse
from KlAkOAPI.Params import KlAkParams, KlAkArray, paramParams,
strToBin
from KlAkOAPI.AdmServer import KlAkAdmServer
from KlAkOAPI.Error import KlAkError, KlAkResponseError
from KlAkOAPI.CgwHelper import KlAkCgwHelper
from KlAkOAPI.GatewayConnection import KlAkGatewayConnection
from KlAkOAPI.HostGroup import KlAkHostGroup
from KlAkOAPI.ChunkAccessor import KlAkChunkAccessor
from KlAkOAPI.Tasks import KlAkTasks
from KlAkOAPI.HostTasks import KlAkHostTasks
from KlAkOAPI.NagHstCtl import KlAkNagHstCtl

# For basic authentication, you should either state '-user' and '-
password' arguments or the following credentials must be applied:
KSCServerUserAccountDefault / KSCServerUserPasswordDefault
# You should create an internal user with these credentials in advance
in Kaspersky Security Center by using Kaspersky Security Center Web
Console or MMC-based Administration Console and grant this user
required privileges, such as 'Main Administrator' role.
# For Windows platform, NTLM authentication is applied when '-user'
and '-password' arguments are omitted.
```

Источники информации о приложении

Страница Kaspersky Endpoint Detection and Response Optimum на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Endpoint Detection and Response Optimum вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

Страница Kaspersky Endpoint Detection and Response Optimum в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Endpoint Detection and Response Optimum 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 Endpoint Detection and Response Optimum, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

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 Endpoint Detection and Response Optimum, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского". Сотрудники Службы технической поддержки ответят на все ваши вопросы об установке и использовании Kaspersky Endpoint Detection and Response Optimum.

> "Лаборатория Касперского" предоставляет поддержку Kaspersky Endpoint Detection and Response Optimum в течение жизненного цикла (см. страницу жизненного цикла приложений). Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетив сайт Службы технической поддержки;
- отправив запрос в Службу технической поддержки 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 ваших электронных запросов, а также хранить их историю.

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

Endpoint Protection Platform (EPP)

Интегрированная система комплексной защиты конечных устройств (например, мобильных устройств, компьютеров или ноутбуков) с помощью различных технологий безопасности. Примером Endpoint Protection Platform является Kaspersky Endpoint Security для бизнеса.

EPP-программа

Программа, входящая в состав системы защиты конечных устройств (англ. Endpoint Protection Platform, EPP). EPP-программы устанавливаются на конечные устройства внутри IT-инфраструктуры организации (например, мобильные устройства, компьютеры или ноутбуки). Примером EPP-программы является Kaspersky Endpoint Security для Windows в составе EPP-решения Kaspersky Endpoint Security для бизнеса.

IOC

Индикатор компрометации (или IOC) показывает наличие на устройстве признаков, свидетельствующих о нарушении безопасности.

IOC-файл

Файл, содержащий набор индикаторов компрометации, которые сравниваются с индикаторами события. Если сравниваемые показатели совпадают, программа считает событие алертом. Вероятность алерта может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

OpenIOC

Открытый стандарт описания индикаторов компрометации (Indicator of Compromise, IOC), созданный на базе XML и содержащий более 500 различных индикаторов компрометации.

TLS-шифрование

Шифрование соединения между двумя серверами, обеспечивающее защищенную передачу данных между серверами через интернет.

Действие по реагированию

Действие по реагированию на инцидент – это структурированная методология обработки инцидентов и нарушений системы безопасности и киберугроз.

Тенант

Тенант – это организация, которой предоставляется решение Kaspersky Endpoint Detection and Response Optimum.

Трассировка

Отладочное выполнение программы, при котором после выполнения каждой инструкции происходит остановка и отображается результат.

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 совместимых приложений.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Mac, macOS – товарные знаки Apple Inc.

Active Directory, Windows и Windows Server являются товарными знаками группы компаний Microsoft.

OpenAPI – товарный знак компании The Linux Foundation.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.