kaspersky

Руководство пользователя
Потоки данных об угрозах

Уважаемый пользователь!

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

Дата редакции документа: 01.10.2020

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

О "Лаборатории Касперского": https://www.kaspersky.ru/about/company

kaspersky

Содержание

О Потоках данных об угрозах

Добро пожаловать в документацию для Потоков данных об угрозах.

Что такое Потоки данных об угрозах

Потоки данных об угрозах – это платформа для обработки данных киберразведки, которая интегрирует потоки данных об угрозах с SIEM-системами и другими средствами защиты, например, межсетевыми экранами, системами предотвращения вторжений и т.д. Такая интеграция позволяет пользователям незамедлительно использовать полученные данные для мониторинга безопасности в существующем рабочем процессе.

"Лаборатория Касперского" предлагает постоянно обновляемые потоки данных об угрозах для информирования вашего бизнеса или клиентов о рисках и последствиях, связанных с киберугрозами, помогая вам более эффективно препятствовать угрозам и быть защищенным от кибератак еще до попытки их совершения.

Управление потоками данных происходит через специальную консоль - Kaspersky CyberTrace. Данная консоль поддерживает интеграцию с источниками данных об угрозах (потоками данных об угрозах "Лаборатории Касперского", источниками других поставщиков, потоками из открытых источников (OSINT) или клиентскими источниками), SIEM-системами и источниками журналов. Когда в вашей среде обнаруживаются индикаторы компрометации из потоков данных об угрозах, Kaspersky CyberTrace автоматически отправляет оповещение SIEM-системе для непрерывного мониторинга, оценки, поиска и выявления дополнительных контекстных признаков действующих инцидентов безопасности. Kaspersky CyberTrace предоставляет аналитикам набор инструментов для приоритизации оповещений и реагирований, посредством присвоения категорий и оценки выявленных совпадений.

Ключевые возможности Kaspersky CyberTrace:

- Автоматическое и быстрое сопоставление входящих записей журналов и событий с потоками данных об угрозах "Лаборатории Касперского", потоками OSINT или клиентскими потоками данных в самых популярных форматах (JSON, STIX, XML, CSV). Демонстрационные потоки данных "Лаборатории Касперского" и OSINT доступны из коробки.
- Внутренний процесс анализа и сопоставления входящих данных значительно снижает нагрузку на SIEM-систему. Kaspersky CyberTrace анализирует входящие записи журналов и события, сопоставляет полученные результаты с потоками данных и генерирует собственные оповещения при обнаружении угроз. Таким образом, SIEM-системе нужно обработать меньше данных.
- Генерация статистики использования потоков данных об угрозах для измерения эффективности потоков.
- Глубокое исследование угроз с помощью поиска индикаторов компрометации (хеш-сумм, IPадресов, доменов, веб-адресов) по запросу пользователя. Также поддерживается групповое сканирование журналов и файлов.
- Универсальный подход к интеграции средств сопоставления угроз с SIEM-системами и другими системами управления безопасностью. SIEM-коннекторы для широкого спектра SIEMрешений могут использоваться для визуализации данных об обнаруженных угрозах и управления этими данными.
- Индикаторы компрометации и связанный контекст, которые эффективно хранятся в ОЗУ для быстрого доступа и фильтрации.
- Kaspersky CyberTrace Web, графический интерфейс платформы Kaspersky CyberTrace, который обеспечивает визуализацию данных, поиск индикаторов компрометации по запросу пользователя и доступ к настройке платформы. Графический интерфейс также поддерживает

управление потоками данных, правила анализа записей журнала, черные и белые списки и источники событий.

- Дистрибутивы доступны для операционных систем Windows и Linux®.
- Расширенная фильтрация для потоков данных и событий журнала. Потоки можно преобразовывать и фильтровать, используя широкий набор критериев: время, распространенность, географическое положение, тип угрозы. События журнала можно фильтровать на основе условий, устанавливаемых пользователем.
- Поддержка интеграции с DMZ. Компьютер, на котором данные о событиях сопоставляются с потоками данных об угрозах, может находиться в демилитаризованной зоне и быть изолированным от интернета.
- В автономном режиме, когда платформа не интегрирована с SIEM-системой, Kaspersky CyberTrace получает записи журналов от различных источников (таких как сетевые устройства), обрабатывает эти записи в соответствии с заданными правилами нормализации и анализирует их с помощью указанных регулярных выражений.
- Экспорт результатов поиска, которые совпали с потоками данных, в формат CSV для интеграции с другими системами (брандмауэрами, сетевыми системами обнаружения вторжений, клиентскими программными средствами).
- Выявляет и нейтрализует методы обфускации, которые используются некоторыми угрозами для сокрытия вредоносных действий в журналах.

Основные компоненты Kaspersky CyberTrace: Feed Service, Feed Utility, Log Scanner и графический интерфейс Kaspersky CyberTrace Web.

О потоках данных и сертификатах

В этом разделе описаны потоки данных об угрозах и сертификаты, которые используются в Kaspersky CyberTrace.

В этом разделе

О потоках данных об угрозах "Лаборатории Касперского"

В этом разделе описаны потоки данных об угрозах «Лаборатории Касперского», доступные в Kaspersky CyberTrace.

Основные сведения о потоках данных об угрозах "Лаборатории Касперского"

Поставщики средств безопасности и предприятия первого уровня используют потоки данных об угрозах "Лаборатории Касперского" для создания первоклассных решений безопасности или для защиты своего бизнеса.

Кибератаки случаются ежедневно. Киберугрозы становятся все более частыми, сложными и запутанными, пытаясь поставить под угрозу вашу защиту. Сегодня злоумышленники используют сложные цепочки для осуществления вторжений, кампании, а также специальные тактики, техники и процедуры, чтобы подорвать бизнес или нанести ущерб клиентам.

"Лаборатория Касперского" предлагает постоянно обновляемые потоки данных об угрозах для информирования вашего бизнеса или клиентов о рисках и последствиях, связанных с киберугрозами, помогая вам более эффективно препятствовать угрозам и быть защищенным от кибератак еще до попытки их совершения.

Информация, которая содержится в потоках данных об угрозах "Лаборатории Касперского"

Потоки данных "Лаборатории Касперского" содержат тщательно проверенные данные индикаторов угроз, полученные из реального мира в режиме реального времени.

Каждая запись в каждом потоке данных обогащена актуальным контекстом: имена угроз, временные отметки, местоположение, преобразованные IP-адреса, адреса зараженных веб-ресурсов, хеш-суммы файлов, распространенность и прочее.

Помещенные в контекст данные позволяют более точно ответить на большое количество вопросов, что ведет к выявлению злоумышленников и помогает принимать своевременные решения и действия, необходимые вашей организации.

Доступные группы потоков данных

Потоки данных об угрозах «Лаборатории Касперского», доступные в Kaspersky CyberTrace, делятся на следующие группы:

- Коммерческие потоки данных.

  Эта группа включает потоки, которые доступны с коммерческим сертификатом. Потоки данных этой группы охватывают широкий спектр киберугроз.

- Потоки данных APT.

  Потоки данных APT – это коммерческие потоки данных, которые содержат информацию о киберугрозах, относящихся к целевым кибератакам.

- Демонстрационные потоки данных.

  Демонстрационные потоки данных используют для ознакомительных целей. Для таких потоков данных коммерческий сертификат не нужен. Демонстрационные потоки предоставляют более низкий уровень обнаружения по сравнению с соответствующими коммерческими версиями.

Коммерческие потоки данных

Эта группа включает следующие потоки данных:

- Botnet CnC URL Data Feed.

  Набор веб-адресов и хеш-сумм с контекстом, который охватывает командные центры ботнетов и связанные с ними вредоносные объекты. Доступны маскированные и немаскированные записи.

- IP Reputation Data Feed.

  Набор IP-адресов с контекстом, который охватывает различные категории подозрительных и вредоносных хостов.

- Malicious Hash Data Feed.

  Набор хеш-сумм файлов с контекстом, который охватывает наиболее опасные, распространенные или недавно возникшие вредоносные программы.

- Malicious URL Data Feed.

  Набор веб-адресов с контекстом, который охватывает вредоносные веб-сайты и вебстраницы. Доступны маскированные и немаскированные записи.

- Mobile Botnet CnC URL Data Feed.

  Набор веб-адресов с контекстом, который охватывает командные центры ботнетов, относящиеся к мобильным устройствам.

- Mobile Malicious Hash Data Feed.

  Набор хеш-сумм файлов с контекстом для обнаружения вредоносных объектов, которые заражают мобильные устройства Google™ Android™ и Apple® iPhone®.

- P-SMS Trojan Data Feed.

Набор хеш-сумм троянских программ с контекстом для обнаружения троянских программ, относящихся к SMS-сообщениям. Такие программы позволяют взимать дополнительную плату

с пользователей мобильных устройств с помощью SMS, а также дают возможность злоумышленникам красть, удалять SMS-сообщения и отвечать на них.

- Phishing URL Data Feed.

  Набор веб-адресов с контекстом, который охватывает фишинговые веб-страницы. Доступны маскированные и немаскированные записи.

- Ransomware URL Data Feed.

  Набор веб-адресов, доменов и хостов с контекстом, который охватывает сайты-вымогатели.

- APT Hash Data Feed.

  Набор хеш-сумм объектов, охватывающих вредоносные артефакты, которые злоумышленники используют для проведения целевых атак.

- APT IP Data Feed.

  Набор IP-адресов, которые принадлежат инфраструктуре, используемой в целевых атаках.

- APT URL Data Feed.

  Набор доменов, которые принадлежат инфраструктуре, используемой в целевых атаках.

- Vulnerability Data Feed.

  Набор хеш-сумм файлов с контекстом, который охватывает уязвимости в приложениях и эксплойты, которые используют эти уязвимости.

- IoT URL Data Feed.

  Набор веб-адресов с контекстом, который охватывает ссылки, используемые для загрузки вредоносного ПО, нацеленного на атаку устройств интернета вещей.

Демонстрационные потоки данных

Эта группа включает следующие демонстрационные потоки данных:

- Demo Botnet CnC URL Data Feed.

  Предоставляет более низкий уровень обнаружения по сравнению с Botnet CnC URL Data Feed.

- Demo IP Reputation Data Feed.

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

- Demo Malicious Hash Data Feed.

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

Порядок сортировки записей в потоках данных

Записи в потоках данных отсортированы следующим образом:

- Записи в IP Reputation Data Feed отсортированы по оценке угроз в порядке убывания.
- Записи во всех остальных потоках данных отсортированы по распространенности в порядке убывания.

О потоках данных OSINT

В этом разделе описаны потоки данных OSINT, которые поддерживает Kaspersky CyberTrace.

Потоки OSINT – это общедоступные источники данных об угрозах, предоставляемые организациям и отдельным лицам.

Потоки данных OSINT, поддерживаемые Kaspersky CyberTrace

Kaspersky Feed Utility поддерживает потоки данных OSINT от следующих поставщиков:

- Abuse.ch

  У этого поставщика несколько связанных источников информации:

- Feodo Tracker – это проект abuse.ch, целью которого является совместное использование серверов botnet C&C, связанных с семейством Feodo malware (Dridex, Emotet/Heodo).
- Ransomware Tracker отслеживает и контролирует статусы имен доменов, IP-адресов и веб-адресов, которые связаны с Ransomware, например серверы C&C и платежные вебсайты.
- The SSL Blacklist (SSLBL) – это проект abuse.ch, целью которого является обнаружение вредоносных SSL-соединений путем выявления SSL-сертификатов, используемых серверами botnet C&C, и внесения их в список запрещенных.
- Proofpoint ET intelligence

  Этот поставщик предоставляет информацию о возникающих угрозах.

- BlockList.de

  Бесплатный и добровольный сервис, созданный специалистом Fraud/Abuse, чьи серверы часто подвергались атакам SSH-, Mail-Login-, FTP-, Webserver- и другими службами.

  BlockList.de сообщил о более чем 70 000 атак за 12 часов в режиме реального времени. BlockList.de использует сервис Whois (abuse-mailbox, abuse@, security@, email, remarks), RIPE Abuse Finder и базу данных контактов от abusix.org, чтобы найти сведения о нарушителе по атакующему хосту.

- Cyber Crime Tracker

  Cyber Crime Tracker отслеживает и контролирует семейства вредоносных программ, которые используются для совершения киберпреступлений: например, банковские трояны и программы-вымогатели. Источник содержит, главным образом, вредоносные C&C и хеши файлов Zeus и семейств вредоносных программ, созданных Zeus.

Ниже представлена таблица с поддерживаемыми потоками данных OSINT:

Таблица 1. Потоки данных OSINT

Идентификатор	Ссылка
Abuse.ch_Ransomware_Common	https://ransomwaretracker.abuse.ch/feeds/csv/
Abuse.ch_Ransomware_BlockUrl	https://ransomwaretracker.abuse.ch/downloads/RW_URLBL.txt
Abuse.ch_Ransomware_BlockDomain	https://ransomwaretracker.abuse.ch/downloads/RW_DOMBL.txt
Abuse.ch_Ransomware_BlockIP	https://ransomwaretracker.abuse.ch/downloads/RW_IPBL.txt
Abuse.ch_Feodo_BlockIP	https://feodotracker.abuse.ch/downloads/ipblocklist.txt
Abuse.ch_Feodo_MalwareHash	https://feodotracker.abuse.ch/downloads/malware_hashes.csv
Abuse.ch_SSL_Certificate_BlockIP	https://sslbl.abuse.ch/blacklist/sslipblacklist.csv
Abuse.ch_SSL_Certificate_BlockHash	https://sslbl.abuse.ch/blacklist/sslblacklist.csv
Blocklist.de_BlockIP	https://lists.blocklist.de/lists/all.txt
CyberCrime_Tracker_BlockUrl	http://cybercrime-tracker.net/all.php
EmergingThreats_BlockIP	https://rules.emergingthreats.net/fwrules/emerging-BlockIPs.txt
EmergingThreats_CompromisedIP	https://rules.emergingthreats.net/blockrules/compromisedips.txt

Потоки данных OSINT из таблицы поддерживаются только сторонними разработчиками. По разным причинам некоторые из веб-адресов выше могут стать неактуальными со временем.

О сертификатах

Kaspersky CyberTrace использует сертификат для загрузки потоков данных об угрозах. Этот сертификат определяет, какие потоки данных могут загружены с серверов обновления.

Типы сертификата

Kaspersky CyberTrace может использует два вида сертификата:

- Демо-сертификат.

  Этот сертификат входит в пакет распространения. Он предоставляет доступ к демонстрационным потокам данных об угрозах "Лаборатории Касперского".

- Коммерческий сертификат.

  Этот сертификат предоставляет доступ к одному и более потокам данных об угрозах "Лаборатории Касперского".

  Чтобы приобрести коммерческий сертификат, обратитесь к команде Kaspersky Cybersecurity Service по адресу intelligence@kaspersky.com.

Сертификаты и безопасность

Когда Kaspersky CyberTrace устанавливает соединение с серверами "Лаборатории Касперского", он передает серверам сертификат в зашифрованном виде. Такое соединение зашифровано, чтобы гарантировать защиту всех данных.

Установка и интеграция Kaspersky CyberTrace

В этой главе описана установка и настройка Kaspersky CyberTrace, а также интеграция продукта с SIEM-системой.

В этом разделе

Системные требования

В этом разделе описаны системные требования Kaspersky CyberTrace.

Поддерживаемые операционные системы

Kaspersky CyberTrace работает в следующих операционных системах:

- Linux® x64.
- Microsoft® Windows® 7 x64.
- Microsoft Windows 8 x64.
- Microsoft Windows 8.1 x64.
- Microsoft Windows Server® 2008 R2 x64.
- Microsoft Windows Server 2012 x64.
- Microsoft Windows Server 2012 R2 x64.

Требования для Linux

Для операционной системы Linux должна быть установлена утилита `more`.

Требования к установленному ПО для интеграции с SIEM-системой

При интеграции Kaspersky CyberTrace с SIEM-системой должны соблюдаться следующие требования к установленному ПО.

Таблица 2. Требования к установленному ПО для интеграции с SIEM-системой

SIEM-система	Требования к установленному ПО
Splunk	Splunk® с версии 6.5 до 7.2
ArcSight ESM	ArcSight ESM с версии 6.8 до 7.0 ArcSight SmartConnector
QRadar	IBM® QRadar® версии 7.2.5 или выше
RSA NetWitness	RSA NetWitness® версии 10.5, 10.6, или 11.2
LogRhythm	LogRhythm версии 7.1.7 или выше

Возможна интеграция с другими SIEM-системами. Более подробную информацию вы можете найти на веб-сайте Службы технической поддержки https://support.kaspersky.com/datafeeds.

Поддерживаемые браузеры

Графический интерфейс Kaspersky CyberTrace может быть доступен с помощью следующих браузеров:

- Microsoft Edge версии 42 или выше.
- Microsoft Internet Explorer версии 11 или выше.
- Mozilla™ Firefox™ версии 61 или выше.
- Safari® версии 11 или выше.
- Google Chrome™ версии 68 или выше.

Требования к процессору

Платформа Kaspersky CyberTrace должна поддерживать набор команд x86-64.

Рекомендуется работать с платформой только на высокопроизводительных серверах.

Требования к ОЗУ и месту на жестком диске

Системные требования зависят от сценария использования платформы и используемых потоков данных. Чтобы получить более подробные сведения о системных требованиях, обратитесь к вашему техническому менеджеру.

Фактический объем требуемого места на жестком диске для каждого потока данных зависит от размера исходного файла потока данных. Этот размер меняется при обновлении потоков данных. Со временем размеры файлов потоков могут значительно поменяться, что повлияет на требования к ОЗУ и месту на жестком диске.

Требования к ОЗУ и месту на жестком диске, перечисленные в таблицах ниже, применимы только к потокам данных об угрозах "Лаборатории Касперского". Использование сторонних потоков данных требует дополнительных ресурсов жесткого диска и памяти.

В таблице ниже приведены требования к ОЗУ и месту на жестком диске для использования всех демонстрационных и коммерческих потоков данных в операционной системе Linux.

Таблица 3. Требования к аппаратуре для использования различных потоков данных (Linux)

Используемые потоки данных	HDD, МБ	ОЗУ, МБ
Все демонстрационные потоки данных	100	100
Все коммерческие потоки данных	3400	3000

В таблице ниже приведены требования к ОЗУ и месту на жестком диске для использования всех демонстрационных и коммерческих потоков данных в операционных системах Windows.

Таблица 4. Требования к аппаратуре для использования различных потоков данных (Windows)

Используемые потоки данных об угрозах	HDD, МБ	ОЗУ, МБ
Все демонстрационные потоки данных	100	100
Все коммерческие потоки данных	3200	3300

Сетевые требования

Компьютер, на котором запущена служба Feed Utility, должен иметь доступ к веб-сайту https://wlinfo.kaspersky.com/.

Компьютер, на котором запущена платформа Kaspersky CyberTrace, должен иметь доступ к компьютеру с SIEM-системой.

Пользовательские компьютеры, которым необходим доступ к графическому интерфейсу Kaspersky CyberTrace, должны иметь доступ к IP-адресу и порту интерфейса.

Шаг 1: Установка Kaspersky CyberTrace

Этот раздел содержит информацию о том, как установить Kaspersky CyberTrace на компьютеры с операционными системами Linux и Windows.

В этом разделе

Установка Kaspersky CyberTrace (Linux)

Этот раздел объясняет процесс установки Kaspersky CyberTrace для операционной системы Linux.

Процедура установки программы

Kaspersky CyberTrace будет установлен в директорию `/opt/kaspersky/ktfs`. В документации эта директория называется `%service_dir%`.

Выполнить RPM-установку платформы Kaspersky CyberTrace с помощью файла установки могут только пользователи с правами root.

► *Чтобы выполнить RPM-установку платформы Kaspersky CyberTrace, выполните следующие действия:*

1. Распакуйте архив пакета распространения в любую папку на вашем компьютере. В следующей команде подставьте эту папку вместо `%temp_dir%` и имя вашей SIEM-системы (Splunk, RSA, ArcSight, QRadar, Log_Scanner) вместо `%SIEM%`. Если вашей SIEM-системы нет в упомянутом списке, используйте значение `Log_Scanner`.

   ```
   tar -C %temp_dir% -xvzf
   Kaspersky_CyberTrace_for_%SIEM%_Linuxarchitecture-version-
   Release.rpm.tar.gz --no-same-owner
   ```

2. Запустите установочный скрипт:

   ```
   run.sh install
   ```

   Скрипт установит RPM-пакет и добавит Feed Service в список служб. Feed Service запустится автоматически при загрузке системы.

   После установки RPM-пакета установочный скрипт автоматически запускает конфигуратор.

3. В конфигураторе настройте Feed Service, Feed Utility и Log Scanner.

   Чтобы узнать больше об использовании конфигуратора, обратитесь к разделу "Интерактивная настройка с помощью конфигуратора" ниже.

4. (Рекомендуется) Выполните дальнейшую настройку Kaspersky CyberTrace через графический интерфейс, как описано в разделе "Настройка Kaspersky CyberTrace с помощью графического интерфейса" ниже.

Интерактивная настройка с помощью конфигуратора

Настройка с помощью конфигуратора включает следующие шаги:

1. Принятие условий Лицензионного соглашения.

   Используйте клавиши **PAGE UP** и **PAGE DOWN** для навигации. Чтобы выйти, нажмите **Q**.

   Чтобы принять условия Лицензионного соглашения, напечатайте `Yes`.

2. Определение параметров прокси-сервера.

   Следуйте инструкциям и укажите параметры прокси-сервера. Указанные учетные данные будут храниться в зашифрованном виде.

3. Определение параметров соединения.

   Конфигуратор автоматически определяет, верно ли указаны параметры соединения.

   В зависимости от определенной SIEM-системы, параметры соединения могут включать:

- IP-адрес и порт для входящих событий.

  Feed Service будет прослушивать указанные IP-адрес и порт или сокет домена UNIX для получения входящих событий.

- IP-адрес и порт SIEM-системы.

  Feed Service будет отправлять исходящие события на указанные IP-адрес и порт или сокет UNIX.

После завершения установки запустится графический веб-интерфейс Kaspersky CyberTrace.

Настройка Kaspersky CyberTrace с помощью графического интерфейса

► *Чтобы настроить Kaspersky CyberTrace с помощью графического интерфейса, выполните следующие действия:*

1. Откройте веб-браузер и введите адрес графического интерфейса:

   `https://127.0.0.1`

2. На закладке **Settings** > **Service у**кажите IP-адреса и порты, которые Feed Service будет использовать для входящих и исходящих событий.
3. Если вы хотите использовать Log Scanner, в элементе `Connection` конфигурационного файла Log Scanner укажите IP-адрес и порт, которые утилита будет использовать для взаимодействия с Feed Service.

   Конфигурационный файл Log Scanner расположен в директории `%service_dir%\log_scanner\log_scanner.conf`.

4. Если вы хотите использовать правила нормализации для обработки событий, отправляемых различными источниками, или хотите использовать индивидуальные регулярные выражения, укажите соответствующие параметры на закладке **Matching**.
5. Если вы хотите, чтобы служба Feed Utility имела доступ к серверам "Лаборатории Касперского" через прокси-сервер, укажите параметры соединения на закладке **Settings** > **Service**.
6. Если у вас есть коммерческий лицензионный ключ, добавьте его в Kaspersky CyberTrace на закладке **Licensing**.
7. Если у вас есть коммерческий сертификат для загрузки потоков данных, вы можете импортировать его в разделе **Feeds update period**.
8. В секции **Filtering rules for feeds** выберите потоки данных, которые служба Feed Utility должна загрузить и обработать.

Установка Kaspersky CyberTrace (Windows)

Этот раздел объясняет процесс установки Kaspersky CyberTrace для операционных систем Windows.

Процедура установки программы

► *Чтобы установить Kaspersky CyberTrace, выполните следующие действия:*

1. Запустите файл с расширением .msi из комплекта поставки Kaspersky CyberTrace для Windows.

   Установить Kaspersky CyberTrace с помощью файла MSI могут только пользователи с ролью Администратор.

2. Примите условия Лицензионного соглашения.
3. Укажите параметры соединения с прокси-сервером:
   a. Введите IP-адрес и порт прокси-сервера.
   b. Введите имя пользователя и пароль для аутентификации на прокси-сервере.

   Чтобы проверить указанные параметры, установщик Windows подключается к https://wlinfo.kaspersky.com. Если во время подключения возникает ошибка, обратитесь к разделу "Устранение неисправностей (на стр. 39)" за информацией об импорте корневого сертификата.

4. Укажите параметры соединения для событий:
   a. Введите IP-адрес и порт, которые Kaspersky CyberTrace должен прослушивать для получения входящих событий.
   b. Введите IP-адрес и порт, куда Kaspersky CyberTrace должен отправлять события обнаружения и служебные события.
   c. Чтобы проверить указанные параметры соединения, нажмите **Test connection**.

Запустится графический интерфейс Kaspersky CyberTrace.

Выполните дальнейшую настройку Kaspersky CyberTrace через графический интерфейс, как описано ниже.

Настройка Kaspersky CyberTrace с помощью графического интерфейса

► *Чтобы настроить Kaspersky CyberTrace с помощью графического интерфейса, выполните следующие действия:*

1. Откройте веб-браузер и введите адрес графического интерфейса:

   `https://127.0.0.1`

2. На закладке **Settings** > **Service у**кажите IP-адреса и порты, которые Feed Service будет использовать для входящих и исходящих событий.

3. Если вы хотите использовать Log Scanner, в элементе `Connection` конфигурационного файла Log Scanner укажите IP-адрес и порт, которые утилита будет использовать для взаимодействия с Feed Service.

   Конфигурационный файл Log Scanner расположен в директории `%service_dir%\log_scanner\log_scanner.conf`.

4. Если вы хотите использовать правила нормализации для обработки событий, отправляемых различными источниками, или хотите использовать индивидуальные регулярные выражения, укажите соответствующие параметры на закладке **Matching**.
5. Если вы хотите, чтобы служба Feed Utility имела доступ к серверам "Лаборатории Касперского" через прокси-сервер, укажите параметры соединения на закладке **Settings** > **Service**.
6. Если у вас есть коммерческий лицензионный ключ, добавьте его в Kaspersky CyberTrace на закладке **Licensing**.
7. Если у вас есть коммерческий сертификат для загрузки потоков данных, вы можете импортировать его в секции **Feeds update period**.
8. В секции **Filtering rules for feeds** выберите потоки данных, которые служба Feed Utility должна загрузить и обработать.

Шаг 2: Интеграция Kaspersky CyberTrace с источником событий

На этом шаге вам нужно интегрировать Kaspersky CyberTrace с источником событий. *Источник событий* – это или одна из SIEM-систем, или другой отдельный источник.

Kaspersky CyberTrace поддерживает интеграцию со следующими SIEM-системами:

- Splunk

  За подробными инструкциями по интеграции Kaspersky CyberTrace и Splunk обратитесь к онлайн-справке Kaspersky CyberTrace: https://support.kaspersky.com/CyberTrace/1.0/enUS/162505.htm

- ArcSight

  За подробными инструкциями по интеграции Kaspersky CyberTrace и ArcSight обратитесь к онлайн-справке Kaspersky CyberTrace: https://support.kaspersky.com/CyberTrace/1.0/enUS/162514.htm

- QRadar

  За подробными инструкциями по интеграции Kaspersky CyberTrace и QRadar обратитесь к онлайн-справке Kaspersky CyberTrace: https://support.kaspersky.com/CyberTrace/1.0/enUS/165399.htm

- RSA NetWitness

За подробными инструкциями по интеграции Kaspersky CyberTrace и RSA NetWitness обратитесь к онлайн-справке Kaspersky CyberTrace: https://support.kaspersky.com/CyberTrace/1.0/en-US/166878.htm

- LogRhythm

  За подробными инструкциями по интеграции Kaspersky CyberTrace и LogRhythm обратитесь к онлайн-справке Kaspersky CyberTrace: https://support.kaspersky.com/CyberTrace/1.0/enUS/183778.htm

Возможна интеграция с другими SIEM-системами. Более подробную информацию вы можете найти на веб-сайте Службы технической поддержки https://support.kaspersky.com/datafeeds.

Использование веб-интерфейса Kaspersky CyberTrace

Этот раздел описывает, как использовать веб-интерфейс Kaspersky CyberTrace.

В этом разделе

О веб-интерфейсе Kaspersky CyberTrace

Веб-интерфейс Kaspersky CyberTrace представляет из себя HTTP-сервис и называется Kaspersky CyberTrace Web.

Начиная с Kaspersky CyberTrace 3.1.0 использование приложения без веб-интерфейса не поддерживается.
CyberTrace Web использует токены для аутентификации пользователей. Токены хранятся в файлах cookie и обновляются каждые несколько минут.

Веб-интерфейс содержит следующие страницы:

- Страница входа (см. раздел "Вход в Kaspersky CyberTrace Web" на стр. 21).
- Информационная панель (см. раздел "Информационная панель Kaspersky CyberTrace Web" на стр. 22), которая показывает статистику работы Kaspersky CyberTrace.
- Закладка **Search (**см. раздел "Поиск информации об индикаторах" на стр. 27**)** (поиск информации об индикаторах).

  В Kaspersky CyberTrace 3.0 эта закладка называлась **Lookup**.
- Закладка **Settings** (см. раздел "Настройка Kaspersky CyberTrace Web" на стр. 30), которая содержит следующее:
- Закладку **Service** (настройки сервиса).

- Закладку **Feeds** (настройки потоков данных об угрозах).
- Закладку **Matching** (настройки событий и источников событий).

- Закладку **Events format** (настройки событий, генерируемых Feed Service).
- Закладку **Logging** (настройки журналирования).
- Закладку **Users** (настройки учетных записей).

  Эта страница доступна начиная с Kaspersky CyberTrace 3.1.0.
- Закладку **Licensing** (настройки лицензирования).

  Эта страница доступна начиная с Kaspersky CyberTrace 3.1.0.

Вход в Kaspersky CyberTrace Web

Для входа в Kaspersky CyberTrace Web вам требуется ввести действующие имя пользователя и пароль в форму входа.

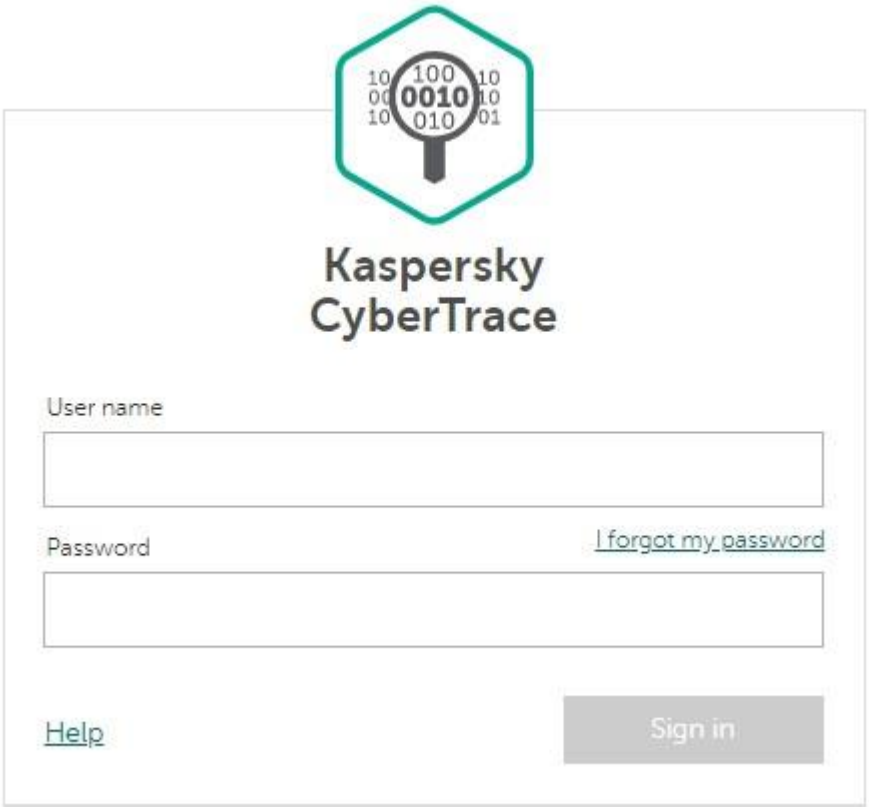

Рисунок 1. Форма входа

Если вы не используете Kaspersky CyberTrace Web больше двух часов, ваша сессия закончится и вам нужно будет войти снова.

Имя пользователя и пароль по умолчанию

После того, как установка Kaspersky CyberTrace завершится, вы сможете войти в Kaspersky CyberTrace Web со следующими учетными данными:

- Имя пользователя: `admin`
- Пароль: `CyberTrace!1`

Рекомендуется сменить пароль по умолчанию из соображения безопасности.

Изменение пароля

Когда вы вошли в Kaspersky CyberTrace Web, вы можете изменить свой пароль в любое время.

► *Чтобы изменить пароль,*

1. Нажмите на ссылку **admin** в верхнем правом углу окна.
2. В открывшемся окне нажмите на ссылку **Change password**.

Новый пароль должен содержать от 6 до 16 символов ASCII: по крайней мере одну латинскую букву верхнего регистра, одну латинскую букву нижнего регистра, одну цифру и один специальный символ.

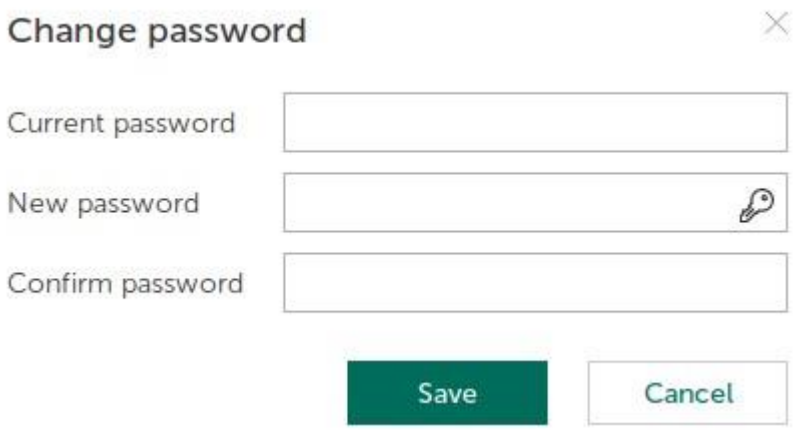

Рисунок 2. Форма **Change password**

Информационная панель Kaspersky CyberTrace Web

Когда вы заходите в Kaspersky CyberTrace, открывается информационная панель (закладка **Dashboard**). Информационная панель показывает статистику работы Kaspersky CyberTrace и состоит из нескольких секций:

- **Statistics overview** (обзор статистики).
- **Feed statistics** (статистика обнаружений, отсортированная по потокам данных об угрозах).
- **Indicator statistics** (статистика обнаружений, отсортированная по индикаторам).

Начиная с Kaspersky CyberTrace 3.1.0 вы можете скачать отчет о статистике обнаружений. Отчет имеет формат HTML.

Отображение статистики за определенный период

Вы можете указать период, за который должна отображается статистика, выбрав одно из следующих значений:

- **Day** (24 часа).
- **Week**.
- **Month** (31 день).
- **3 months** (93 дня).

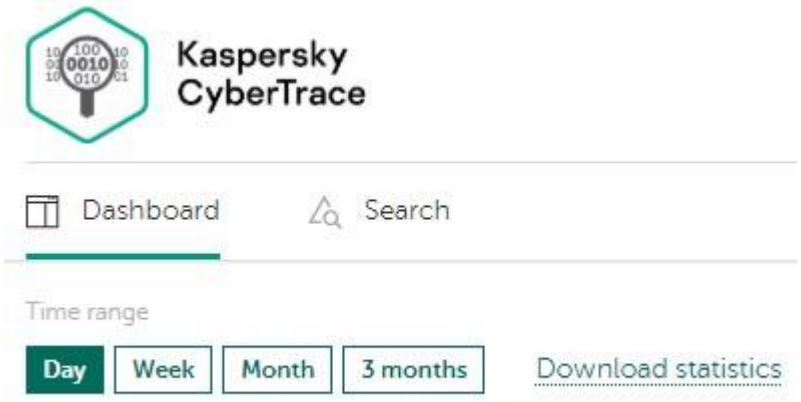

Рисунок 3. Информационная панель Kaspersky CyberTrace Web. Выбор периода отображения статистики

Секция Statistics overview

Эта секция содержит следующее:

- График, показывающий количество обнаружений за указанный период. Ось времени делится на часы, дни или недели в зависимости от выбранного периода.

  Этот график отображается, если выбрана кнопка **Number of detections**.

- График, показывающий количество обнаруженных индикаторов каждого типа (URL, IP-адреса and хеши). Ось времени делится на часы, дни или недели в зависимости от выбранного периода.

Этот график отображается, если выбрана кнопка **Number of detected indicators**.

Рисунок 4. Секция **Statistics overview**

Секция Feed statistics

Эта секция содержит следующее:

- Таблицу со статистикой обнаружений по каждому из используемых потоков данных об угрозах.

Эта таблица содержит следующую информацию:

- **Feed name** – имена используемых потоков данных об угрозах.
- **Indicators** – количество индикаторов в каждом потоке данных об угрозах.
- Отметка о том, загружен ли каждый поток данных об угрозах.
- **Whitelisted** – количество индикаторов, которые входят в список разрешенных в каждом потоке данных об угрозах (ложноположительные обнаружения)
- **Detected** – количество обнаруженных индикаторов по каждому потоку данных об угрозах.

Таблица также показывает общее количество индикаторов в каждом столбце.

Если поток данных об угрозах не загружен или загружен только частично из-за достижения лицензионного ограничения, он будет отмечен символом ( ).

- Диаграмму, которая показывает количество обнаружений по каждому из используемых потоков данных об угрозах.

Эта диаграмма отображается, если выбрана кнопка **Detected**. Если вы наведете курсор мыши на один из секторов диаграммы, вы увидите имя потока данных об угрозах, количество обнаружений и процент обнаружений по потоку данных от общего количества.

Рисунок 5. Диаграмма обнаружений

- Диаграмму, которая показывает количество разрешенных индикаторов для каждого из используемых потоков данных об угрозах.

  Эта диаграмма отображается, если выбрана кнопка **Whitelisted**. Если вы наведете курсор мыши на один из секторов диаграммы, вы увидите имя потока данных об угрозах, количество разрешенных индикаторов и процент разрешенных индикаторов по потоку данных от общего количества.

Если в списке разрешенных индикаторов есть записи, таблица **Feed statistics** содержит строку с именем списка разрешенных индикаторов и размером списка в столбце **Indicators**. Другие столбцы в этой строке содержат значение **0**.

Если в списке запрещенных индикаторов есть записи, таблица **Feed statistics** содержит строку с именем списка запрещенных индикаторов и размером списка в столбце **Indicators**. Столбец **Detected** в этой строке содержит количество обнаружений индикаторов, занесенных в список запрещенных индикаторов.

Если вы выключите или удалите поток данных об угрозах, который использовался ранее, он попрежнему будет отображаться в таблице. Чтобы проверить, выключен ли поток данных об угрозах, наведите курсор мыши на строку с именем потока данных: если поток данных выключен, появится всплывающее окно со статусом потока.

Секция Indicator statistics

Эта секция содержит следующее:

- Таблицу со статистикой проверенных индикаторов.

  Эта таблица содержит следующее:

- **Indicator type** – типы индикаторов.
- **Checked** – количество индикаторов каждого типа (URL, IP-адрес или хеш), которые были проверены Feed Service.

- **Detected** – количество индикаторов каждого типа (URL, IP-адрес или хеш) которые были обнаружены Feed Service.

  Таблица также показывает общее количество индикаторов в каждом столбце.

- Диаграмму, которая отображает количество проверенных индикаторов каждого типа (URL, IPадрес или хеш).

  Эта диаграмма отображается, если выбрана кнопка **Checked**. Если вы наведете курсор мыши на один из секторов диаграммы, вы увидите тип индикаторов, количество индикаторов и процент от общего количества индикаторов.

- Диаграмму, которая отображает количество обнаруженных индикаторов каждого типа (URL, IP-адрес или хеш).

  Эта диаграмма отображается, если выбрана кнопка **Checked**. Если вы наведете курсор мыши на один из секторов диаграммы, вы увидите тип индикаторов, количество индикаторов и процент от общего количества индикаторов.

Загрузка отчета о статистике

► *Чтобы загрузить отчет о статистике,*

нажмите на ссылку **Download statistics**.

Отчет о статистике содержит следующее:

- График, показывающий количество обнаружений.

  Этот график входит в отчет, если на информационной панели выбрана кнопка **Number of detections**.

- График, показывающий количество обнаруженных индикаторов каждого типа.

  Этот график входит в отчет, если на информационной панели выбрана кнопка **Number of detected indicators**.

- Таблицу, показывающая статистику по потокам данных об угрозах.
- Таблицу, показывающую статистику по индикаторам.
- Диаграмму, показывающую количество обнаружений по каждому потоку данных об угрозах.

  Эта диаграмма входит в отчет, если на информационной панели выбрана кнопка **Detected**.

- Диаграмму, показывающую количество разрешенных индикаторов по каждому из используемых потоков данных об угрозах.

  Эта диаграмма входит в отчет, если на информационной панели выбрана кнопка **Whitelisted**.

- Диаграмму, которая показывает количество проверенных индикаторов каждого типа.

Эта диаграмма входит в отчет, если на информационной панели выбрана кнопка **Checked**.

- Диаграмму, которая показывает количество обнаруженных индикаторов каждого типа.

  Эта диаграмма входит в отчет, если на информационной панели выбрана кнопка **Detected**.

Поиск информации об индикаторах

Вы можете найти информацию об индикаторах компроментации, используя закладку **Search** в Kaspersky CyberTrace Web.

Поиск информации об индикаторах может быть отключен из-за достижения лицензионного ограничения.

На закладке **Search** вы можете выбрать нужный вам режим поиска:

- **Indicator** (см. раздел "Поиск одного индикатора" на стр. 28) – поиск информации об одном индикаторе.

  Для поиска введите URL, домен, IP-адрес или хеш и нажмите кнопку **Search**.

- **Log file (**см. раздел "Поиск по файлам журналирования" на стр. 28**) – п**оиск информации об индикаторах из файла журналирования.
- **File (**см. раздел "Поиск по хешу файла" на стр. 30**) – п**оиск информации о файле по хешу файла.

Начиная с Kaspersky CyberTrace 3.1.0 все результаты поиска сохраняются в истории поиска.

Отчеты о результатах поиска

Вы можете сохранить отчет о результатах поиска в текстовый файл.

Отчет будет сохранен в файл с именем `kl_lookup_result_%TYPE%_hhmmss_ddMMyyyy.csv`. Значение `%TYPE%` зависит от выбранного режима поиска.

Первая строка отчета содержит названия полей. Состав полей зависит от режима поиска. Поля для каждого режима описаны в соответствующих разделах этого документа.

Вы также можете отменить поиск.

► *Чтобы отменить поиск, выполните следующие действия:*

1. Нажмите на кнопку **Cancel search**.

   Появится окно подтверждения.

2. Нажмите **Yes**.

В этом разделе

Поиск одного индикатора

Вы можете найти информацию об одиночном индикаторе, выбрав закладку **Indicator** на закладке **Search**.

Поиск объектов

Вы можете искать информацию об индикаторах следующих типов:

- Хеш.
- IP-адрес.
- Домен.
- URL.

Синтаксис поиска

Вы можете искать URL следующими способами:

- указав полный URL;
- указав только доменное имя.

Если вы ищете хеш или IP-адрес, указывайте индикатор полностью.

Результаты поиска

Когда поиск завершен, CyberTrace Web отображает результаты, которые состоят из следующих полей:

- Категория объекта.
- Поля записи в потоке данных об угрозах, по которому был обнаружен индикатор.

  Если объект не был обнаружен в используемых потоках данных, отобразится сообщение об этом.
- Ссылка на информацию об объекте Kaspersky Threat Intelligence Portal.

Регулярные выражения для поиска индикаторов

Для поиска индикаторов CyberTrace Web использует регулярные выражения, указанные в конфигурационном файле Feed Service. Вы можете просматривать и редактировать их в CyberTrace Web (см. раздел "Настройка Kaspersky CyberTrace Web" на стр. 30).

Поиск по файлам журналов

Вы можете найти информацию об индикаторах, присутствующих в файле журнала, выбрав закладку **Log file** на закладке **Search**.

Все файлы журналов, по которым производится поиск, должны быть в кодировке UTF-8.

Поиск объектов

Вы можете искать индикаторы в нескольких файлах журналов одновременно.

Результаты поиска

Когда поиск завершен, CyberTrace Web отображает результаты, которые состоят из следующих полей:

- Общая информация о результатах поиска:
- Количество обработанных файлов журналов.
- Количество обнаруженных индикаторов.
- Количество обработанных строк.
- Количество обнаружений в каждой категории.
- Информация топ-100 обнаруженных индикаторов.
- Ссылка для загрузки отчета о результатах поиска.

Для каждого пункта из топ-100 обнаруженных индикаторов отображается следующая информация:

- Количество вхождений в проверенных файлах журналов.
- Имя файла журнала и строки в нем, которые содержат обнаруженный индикатор.

  По умолчанию отображается до трех строк. Чтобы просмотреть больше строк, нажмите **Show first 100 matches**.

  Вы также можете просмотреть информацию об индикаторе в Kaspersky Threat Intelligence Portal.
- Поля из потока данных об угрозах, в котором был обнаружен индикатор.

Если объект не был обнаружен в используемых потоках данных, отобразится сообщение об этом.

Отчеты о результатах поиска

Отчет о результатах поиска содержит следующие поля:

- `file_name` – название файла журнала.
- `file_line` – строка из файла журнала, которая содержит обнаруженный индикатор.
- `detected_indicator` – обнаруженный индикатор.
- `category` – категория обнаруженного индикатора.

- Контекстные поля, включенные в поток данных об угрозах

Файлы с отчетами сохраняются в директорию `httpsrv`. Только пользователи с правами администратора могу просматривать файлы в этой директории.

Регулярные выражения для поиска по файлам журналов

Для поиска индикаторов CyberTrace Web использует регулярные выражения, указанные в конфигурационном файле Feed Service. Вы можете просматривать и редактировать их в CyberTrace Web (см. раздел "Настройка Kaspersky CyberTrace Web" на стр. 30).

Поиск по хешу файла

Вы можете найти информацию об файле по его хешу, выбрав закладку **File** на закладке **Search**.

Поиск объектов

Вы можете загрузить несколько файлов одновременно. Поиск будет производиться по MD5-хешам этих файлов.

Результаты поиска

Когда поиск завершен, CyberTrace Web отображает результаты, которые состоят из следующих полей:

- Количество обработанных хешей.
- Количество обработанных индикаторов.
- Количество обнаружений в каждой категории.

Для каждого обработанного хеша отображается следующая информация:

- Имя файла.
- MD5-хеш.

  Вы также можете просмотреть информацию об индикаторе в Kaspersky Threat Intelligence Portal.
- Поля из потока данных об угрозах, в котором был обнаружен индикатор.

Если объект не был обнаружен в используемых потоках данных, отобразится сообщение об этом.

Отчеты о результатах поиска

Отчет о результатах поиска содержит следующие поля:

- `file_name` – имя файла, хеш которого был обнаружен в потоках данных об угрозах.
- `detected_indicator` – обнаруженный хеш.

- `category` – категория обнаруженного индикатора.
- Контекстные поля, включенные в поток данных об угрозах

Настройка Kaspersky CyberTrace Web

Вы можете настроить Kaspersky CyberTrace на закладке **Settings** в Kaspersky CyberTrace Web.

Закладка Service

Вы можете настроить параметры Feed Service и Feed Util на закладке **Service** (закладка **Settings**). На этой закладке вы также можете выполнить следующие действия:

- Перезапустить Feed Service (см. раздел "О Feed Service" на стр. 33).
- Экспортировать конфигурационные файлы для Feed Service и Feed Util.
- Провести верификационный тест (самопроверку) потоков данных об угрозах "Лаборатории Касперского".

  Если тестирование не показывает ожидаемый результат, см. раздел "Устранение неисправностей (на стр. 39)", подраздел "Проблема: неожиданный результат верификационного теста (самопроверки)". Если проблему не удается устранить, обратитесь к вашему техническому менеджеру.
- Обнулить статистику обнаружений, отображаемую на информационной панели

Если вы измените параметры на этой странице Feed Service, перезапустится и ваша сессия CyberTrace Web будет закрыта. Вам нужно будет зайти в CyberTrace Web снова.

Закладка Feeds

Вы можете настроить параметры потоков данных об угрозах на закладке **Feeds** (закладка **Settings**).

Закладка **Feeds** содержит следующие секции:

- Feeds update period (настройка периода обновления потоков данных об угрозах).
- Filtering rules for feeds (настройка правил фильтрации потоков данных об угрозах).

На этой закладке вы также можете выполнить следующие действия:

- Добавлять сторонние потоки данных об угрозах
- Управлять белым и черным списками

Добавление и удаление сторонних потоков данных об угрозах или включение потоков данных может быть недоступно из-за достижения лицензионного ограничения.

Закладка Matching

Вы можете настроить параметры событий и источников событий на закладке **Matching** (закладка **Settings**).

На этой закладке вы можете выполнить следующие действия:

- Добавлять источники событий.
- Изменять параметры источников событий.
- Настраивать правила для нормализации входящих событий.
- Настраивать регулярные выражения для парсинга входящих событий.

Закладка Events format

Вы можете настроить параметры исходящих событий на закладке **Events format** (закладка **Settings**).

На этой закладке вы можете выполнить следующие действия:

- Настроить формат исходящих событий, оповещающих о состоянии Feed Service.
- Настроить формат исходящих событий, оповещающих об обнаружении индикаторов компрометации.
- Настроить формат, в котором имена и значения контекстных полей из потоков данных об угрозах будут добавлены в исходящие события.
- Настроить формат, в котором имена и значения неконтекстных полей из потоков данных об угрозах будут добавлены в исходящие события.

Закладка Users

Вы можете управлять учетными записями пользователей на закладке **Users** (закладка **Settings**).

Вы можете добавлять новые учетные записи, а также удалять и изменять существующие.

Форма настройки учетных записей может быть отключена из-за достижения лицензионного ограничения. В этом случае будет доступна только учетная запись `admin`.

Закладка Logging

Вы можете настроить параметры журналирования на закладке **Logging** (закладка **Settings**).

На этой закладке вы можете настроить следующие параметры:

- **Log directory** – директория, в которой сохраняются файлы журналов.
- **Log level** – уровень подробности журналирования.
- **Maximum log file size (MB)** – максимальный размер файла журналирования в мегабайтах.
- **Delete old log files when Feed Service starts** – удаление файлов журналов, оставшихся от предыдущей сессии.
- **Write to syslog** – использование сервера Syslog для журналирования.

  Если этот параметр включен, все другие параметры игнорируются.

Закладка Licensing

Вы можете управлять лицензионными ключами на закладке **Licensing** (закладка **Settings**).

На этой закладке вы можете просмотреть информацию о лицензионных ключах и выполнить следующие действия:

- Добавить лицензионные ключи.
- Удалить лицензионные ключи.

Работа с Feed Service

Этот раздел описывает, как работает Feed Service.

В этом разделе

О Feed Service

Feed Service – это один из компонентов Kaspersky CyberTrace. Он запускается как служба и работает следующим образом:

1. Feed Service слушает порт, на который приходят события от источников событий.
2. Feed Service сопоставляет индикаторы, полученные в событиях, с индикаторами из используемых потоков данных об угрозах.
3. Feed Service генерирует события, которые содержат обнаруженные индикаторы. Эти события генерируются на основе входящих событий и потоков данных об угрозах, которые использовались в обнаружении индикаторов.
4. Feed Service отправляет сгенерированные события указанному программному обеспечению.

Работа с Feed Utility

Этот раздел описывает, как работать с Feed Utility.

В этом разделе

Работа с потоками данных об угрозах

Feed Utility – инструмент для загрузки, фильтрации и компиляции потоков данных об угрозах "Лаборатории Касперского". Все операции производятся по правилам, указанным в конфигурационном файле (см. раздел "Настройка Feed Utility" на стр. 37). Вы также можете настроить эти правила через Kaspersky CyberTrace Web (см. раздел "Настройка Kaspersky CyberTrace Web" на стр. 30).

Загрузка

Feed Utility загружает архивы, содержащие потоки данных об угрозах, с серверов обновлений. Каждый загруженный архив содержит один поток. Прежде чем загрузить потоки данных об угрозах "Лаборатории Касперского", Feed Utility проверяет, новее ли архивы на серверах чем уже используемые архивы. Когда Feed Utility загружает потоки данных OSINT или сторонние потоки данных такая проверка не производится.

Feed Utility использует сертификат (см. раздел "О сертификатах" на стр. 10) для аутентификации. Сертификат также определяет, какие из потоков данных об угрозах "Лаборатории Касперского" могут быть загружены с помощью Feed Utility. Например, если вы используете демо-сертификат, Feed Utility может загружать только демонстрационные потоки данных об угрозах.

Обработка и фильтрация

После того, как архивы с потоками данных об угрозах загружены, Feed Utility распаковывает архивы и обрабатывает файлы потоков. Файлы изменяются по правилам, указанным в конфигурационном файле. Эти правила определяют информацию, которая должна быть включена в потоки в результате обработки, формат файла потока после обработки и максимальное количество записей в потоке после обработки.

Фильтрация – это процесс изменения фалов потоков в соответствии с указанными критериями фильтрации. Критерии фильтрации определяются в правилах фильтрации для каждого потока. Например, вы можете создать поток, который будет использовать только часть информации из оригинального потока.

Компиляция

Если вы используете Feed Utility вместе с Feed Service, потоки данных об угрозах, содержащие маски URL, должны быть сконвертированы в бинарный формат. Feed Utility компилирует эти маски и создает бинарные файлы, которые затем используются Feed Service для быстрого сравнения URL, полученных во входящих событиях, с масками URL. Feed Utility компилирует маски автоматически, если параметр `UrlMatcherField` указан в правилах.

Перезагрузка

Когда Feed Service получает от Feed Utility оповещение, он перезагружает потоки данных об угрозах, то есть выгружает старые потоки из памяти и загружает туда новые.

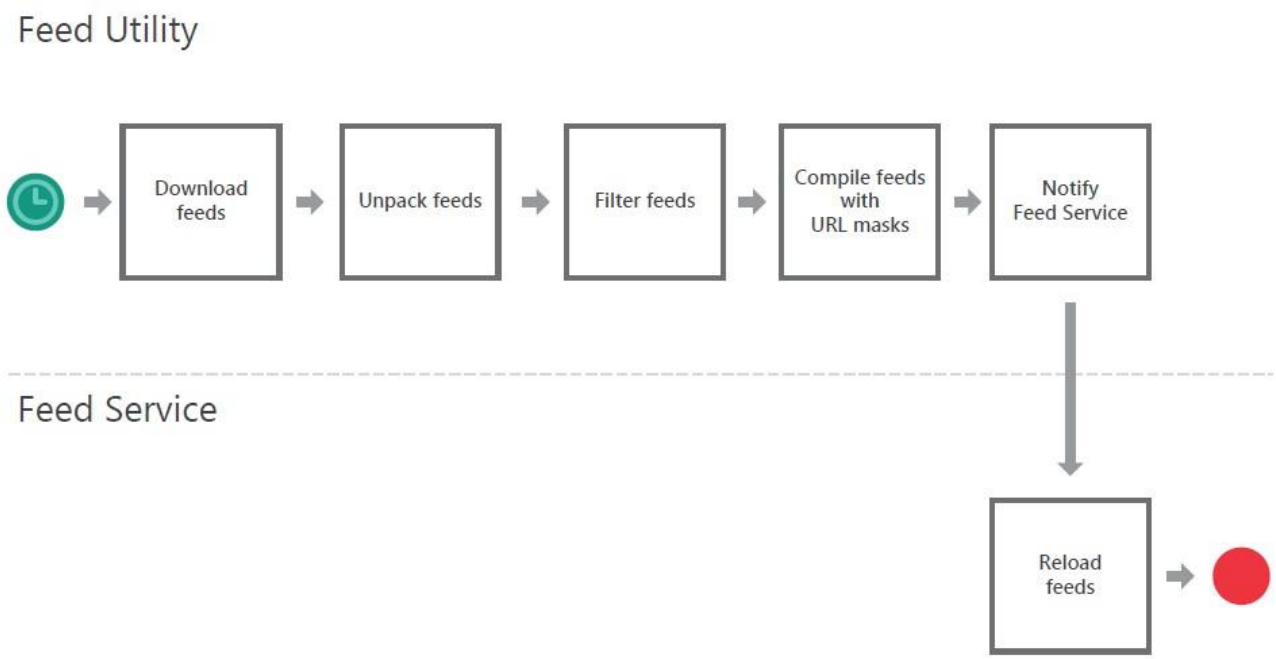

Рисунок 6. Процесс обновления потоков данных об угрозах

Параметры командной строки Feed Utility

Feed Utility является консольным приложением. Вы можете вызвать его из командной строки.

Синтаксис

В операционной системе Linux Feed Utility использует следующий синтаксис:

```
./kl_feed_util [параметры]
```

В операционных системах Windows Feed Utility использует следующий синтаксис:

```
kl_feed_util.exe [параметры]
```

Параметры

Доступны следующие параметры:

- `-h [ --help ]`

  Выводит список доступных параметров.

- `-v [ --verbose ]`

  Если указан этот параметр, Feed Utility выводит подробную информацию о своей работе в командную строку.

- `-s [ --silent ]`

Если указан этот параметр, Feed Utility не выводит информацию о своей работе в командную строку.

- `-c [ --config ] arg`

  Указывает путь к файлу конфигурации. Путь должен быть указан в аргументе `arg`.

  Путь может быть относительным или абсолютным. Относительный путь рассчитывается от исполняемого файла Feed Utilty.

  По умолчанию значение этого параметра – `kl_feed_util.conf`. Feed Utilty ищет этот файл в директории, в которой расположен исполняемый файл.

- `-d [ --download ]`

  Если указан этот параметр, Feed Utility загружает потоки данных об угрозах, но не обрабатывает их.

  Загруженные файлы будут расположены в директории, указанной в параметре `WorkDir` конфигурационного файла Feed Utility.

- `-u [ --unpack ]`

  Если указан этот параметр, Feed Utility распаковывает архивы с потоками данных об угрозах после загрузки.

  Может быть использован только с параметром `-d` или `-p`.

- `-p [ --processing ]`

  Если указан этот параметр, Feed Utility обрабатывает потоки данных об угрозах, но не загружает и не распаковывает их. Feed Utility не удаляет оригинальные файлы потоков.

  Feed Utility ищет файлы потоков в директории, указанной в параметре `WorkDir` конфигурационного файла Feed Utility.

Из-за того, что Feed Utility не удаляет оригинальные файлы потоков, может сложиться ситуация, когда в `WorkDir` будет находиться больше одной версии файла потока. В этом случае Feed Utility выведет сообщение об ошибке. Чтобы избежать этой ошибки, удалите оригинальные файлы потоков вручную после того, как Feed Utility закончит обработку.

- `-f [--feed] arg`

  Загружает или обрабатывает указанный поток данных об угрозах. Имя потока должно быть указано в аргументе `arg`. Если вы хотите указать больше одного потока, разделите их имена точкой с запятой (`;`).

  Может быть использован только с параметром `-d` или `-p`.

- `-i [--input]`

Парсит сторонний поток данных об угрозах и конвертирует его в формат JSON в соответствии с правилами.

Имя потока должно быть указано с помощью параметра `-f`.

- `--set-proxy username:password@host:port`

  Записывает информацию о прокси-сервере в конфигурационный файл Feed Utility. Имя пользователя и пароль записываются в зашифрованном виде.

  Если прокси-сервер не требует аутентификации, используйте формат `--set-proxy host:port`.

- `--set-taxii username:password@feedname@taxii-address@collectionname`

  Записывает информацию о TAXII-сервере в конфигурационный файл Feed Utility. Имя пользователя и пароль записываются в зашифрованном виде.

  Если TAXII-сервер не требует аутентификации, используйте формат `feedname@taxiiaddress@collectionname`.

- `--speedtest`

  Измеряет среднюю скорость с которой Feed Utility загружает потоки данных об угрозах с серверов "Лаборатории Касперского".

  Вы можете использовать этот параметр вместе с параметром `-c`, чтобы указать, какой конфигурационный файл будет использоваться.

Настройка Feed Utility

Feed Utility считывает настройки из конфигурационного файла.

Редактирование конфигурационного файла

Если конфигурационный файл отсутствует или не соответствует указаниям, описанным в этом разделе, Feed Utility не запустится и выведет сообщение об ошибке.

Рекомендуется сделать копию конфигурационного файла, прежде чем менять его содержимое.

Расположение конфигурационного файла (Linux)

В операционной системе Linux конфигурационный файл Feed Utility называется `kl_feed_util.conf` и расположен в директории `%service_dir%/etc`, где `%service_dir%` – директория, в которую был установлен Kaspersky CyberTrace.

Расположение конфигурационного файла (Windows)

В операционных системах Windows конфигурационный файл Feed Utility называется `kl_feed_util.conf` и расположен в папке `%service_dir%/bin`, где `%service_dir%` – папка, в которую был установлен Kaspersky CyberTrace.

Требования к кодировке

Конфигурационный файл Feed Utility должен иметь кодировку UTF-8. Если конфигурационный файл содержит не ASCII-символы и имеет кодировку, отличную от UTF-8, Feed Utility не запустится.

Абсолютные и относительные пути

Вы можете указывать и абсолютные, и относительные пути в качестве параметров. Относительные пути рассчитываются от исполняемого файла Feed Utilty.

Устранение неисправностей

Этот раздел содержит описание возможных неисправностей в работе Kaspersky CyberTrace и способов их устранения.

Проблема: неожиданный результат верификационного теста (самопроверки) Чтобы решить эту проблему, выполните следующие действия:

Если используете Kaspersky CyberTrace Web:

1. Если один или несколько потоков данных об угрозах не прошли верификационный тест, который вы запустили на закладке **Settings** > **Service** по нажатию на **Run Self-test**:

   - Если вы указывали правила фильтрации на закладке **Settings** > **Feeds**, удалите эти правила и нажмите **Save** в нижней части страницы.
   - В секции **Feeds update** закладки **Settings** > **Feeds** нажмите на кнопку **Launch update now**, чтобы обновить потоки данных.

   Перезапустите самопроверку. Если все потоки данных прошли проверку, при необходимости добавьте правила фильтрации снова. Если проблема сохраняется, обратитесь к вашему техническому менеджеру.

2. Если один или несколько потоков данных об угрозах не прошли верификационный тест, который вы запустили для проверки работоспособности интеграции Kaspersky CyberTrace и вашей SIEM-системы:

   a. Проверьте потоки данных через Kaspersky CyberTrace Web:

      - Если вы указывали правила фильтрации на закладке **Settings** > **Feeds**, удалите эти правила и нажмите **Save** в нижней части страницы.
      - В секции **Feeds update** закладки **Settings > Feeds** нажмите на кнопку **Launch update now**, чтобы обновить потоки данных.

      Перезапустите самопроверку. Если все потоки данных прошли проверку, при необходимости добавьте правила фильтрации снова.

   b. Проверьте соединение между компьютером с установленным Kaspersky CyberTrace и компьютером с вашей SIEM-системой (в обе стороны). В командной строке введите команду:

      ```
      ping %ip%
      ```

      где `%ip%` – это IP-адрес компьютера с установленным Kaspersky CyberTrace (если команда вызвана на компьютере с вашей SIEM-системой) или IP-адрес компьютера с SIEM-системой (если команда вызвана на компьютере с Kaspersky CyberTrace).

c. В зависимости от результата выполнения команды `ping` возможно следующее:

- Если выполнение не удалось ни на одном из компьютеров, обратитесь к своему системному администратору для проверки и при необходимости повторной настройки сетевого устройства защиты.
- Если выполнение удалось на обоих компьютерах и вы пробовали все решения, предложенные на шаге 2a, но по-прежнему получаете неправильные результаты, обратитесь к вашему техническому менеджеру.

Если вы не используете Kaspersky CyberTrace Web и один или несколько потоков данных об угрозах не прошли верификационный тест, который вы запустили для проверки работоспособности интеграции Kaspersky CyberTrace и вашей SIEM-системы:

- Если вы указывали правила фильтрации в конфигурационном файле Feed Utility, удалите их и запустите Feed Utility, чтобы изменения вступили в силу.

  Перезапустите самопроверку. Если все потоки данных прошли проверку, при необходимости добавьте правила фильтрации снова.

- Проверьте соединение между компьютером с установленным Kaspersky CyberTrace и компьютером с вашей SIEM-системой (в обе стороны). В командной строке введите команду:

  ```
  ping %ip%
  ```

  где `%ip%` – это IP-адрес компьютера с установленным Kaspersky CyberTrace (если команда вызвана на компьютере с вашей SIEM-системой) или IP-адрес компьютера с SIEM-системой (если команда вызвана на компьютере с Kaspersky CyberTrace).

- В зависимости от результата выполнения команды `ping` возможно следующее:
- Если выполнение не удалось ни на одном из компьютеров, обратитесь к своему системному администратору для проверки и при необходимости повторной настройки сетевого устройства защиты.
- Если выполнение удалось на обоих компьютерах и вы отредактировали конфигурационный файл и перезапустили Feed Utility, но по-прежнему получаете неправильные результаты, обратитесь к вашему техническому менеджеру.

Проблема: Feed Service не запускается

Чтобы решить эту проблему, выполните следующие действия:

- Убедитесь, что порт, указанный в параметрах входа, открыт.
- Проверьте параметры конфигурационного файла службы Feed Service.

Проблема: Feed Service не сохраняет данные в журнал Чтобы

решить эту проблему, выполните следующие действия:

- Убедитесь, что служба Feed Service запущена.
- Проверьте параметры конфигурационного файла kl_feed_service_log.conf.
- Обратитесь к вашему техническому менеджеру.

Проблема: потоки данных не загружаются

Чтобы решить эту проблему, выполните следующие действия:

- Убедитесь, что аутентификация прокси-сервера прошла успешно.

- Убедитесь, что у сертификата, предоставленного техническим менеджером, не истек срок действия.

Проблема: сертификат не может пройти аутентификацию

В этом случае вы увидите сообщение "peer certificate cannot be authenticated with given CA certificates".

Чтобы решить эту проблему, выполните следующие действия:

Убедитесь, что установлен правильный корневой сертификат. Если у вас нет нужного сертификата, выполните следующие действия:

1. По ссылке https://wlinfo.kaspersky.com/ авторизуйтесь со своим сертификатом.
2. В левой крайней части адресной строки вашего браузера нажмите на значок защищенного соединения и выберите **Certificate**.

   Откроется окно **Certificate**.
3. В окне **Certificate** выберите закладку **Certification Path**.
4. Выберите корневой сертификат и нажмите на кнопку **View Certificate**.

   Откроется окно **Certificate**.
5. В окне **Certificate** выберите закладку **Details**.
6. В открывшейся таблице введите значение для поля **Serial number**. Не закрывайте окно.
7. Используйте серийный номер из предыдущего шага, чтобы найти нужный корневой сертификат по ссылке https://www.digicert.com/digicert-root-certificates.ht.
8. Загрузите этот сертификат и следуйте стандартной процедуре для вашей операционной системы, чтобы установить его в хранилище сертификатов.

При выполнении этой процедуры убедитесь, что используете корневой сертификат, загруженный на шагах 7 и 8, а не тот, который вы экспортировали через браузер, нажав **Copy to File**.

Используйте эту процедуру, чтобы устранить ту же проблему с `https://127.0.0.1` (или `https://localhost`) и другими сайтами, с которых Kaspersky CyberTrace загружает индивидуальные и сторонние потоки данных.

Проблема: Microsoft Internet Explorer 11 неправильно отображает шрифты и стили шрифтов

Причиной неполадки могут быть параметры специальных возможностей Internet Explorer.

Чтобы решить эту проблему, выполните следующие действия:

1. Откройте Internet Explorer
2. Нажмите на кнопку **Tools** и выберите **Internet options**.

3. На закладке **General** выберите **Accessibility**.
4. Убедитесь, что флажки **Ignore font styles specified on webpages** и **Ignore font sizes specified on webpages** сняты.
5. Нажмите **OK**, затем снова **OK**.

Уведомления о товарных знаках