kaspersky

# Аналитические отчеты о финансовых угрозах

Краткое руководство администратора

# Содержание



kaspersky

# Kaspersky Threat Intelligence Portal

Kaspersky Threat Intelligence Portal позволяет оперативно получать надежные аналитические данные о киберугрозах, объектах, на которые они направлены, их взаимосвязях и индикаторах угроз. Используя этот веб-портал, ваша компания или клиенты узнают о возникающих рисках, возможных последствиях и о том, как их избежать. Благодаря этим данным вы сможете эффективнее реагировать на угрозы, защищая систему от атак еще до их запуска.

Kaspersky Threat Intelligence Portal – это онлайн-платформа, которая предоставляет удобный доступ ко всем накопленным «Лабораторией Касперского» знаниям об угрозах и их взаимосвязях. Цель этой платформы – обеспечить, например, сотрудников службы информационной безопасности как можно большим количеством данных об угрозах для предотвращения кибератак, которые могут нанести вред организации. Платформа объединяет подробные актуальные сведения об угрозах по вебадресам, доменам, IP-адресам, хешам файлов, статистику и информацию об активности, данные WHOIS/DNS и так далее. В результате вы получаете глобальное представление о различных угрозах, что помогает вам обеспечить защиту вашей организации и повысить эффективность мер реагирования на инциденты.

Информация об угрозах агрегируется из большого количества высоконадежных источников. Затем в режиме реального времени все агрегированные данные тщательно проверяются и уточняются с использованием различных методов и технологий предварительной обработки, таких как статистические системы, инструменты выявления похожести объектов, обработка в изолированной среде, профилирование поведения, проверка на основе списков разрешенных объектов и анализ экспертных систем, включая ручной анализ.

### Основные возможности

Ниже перечислены основные возможности Kaspersky Threat Intelligence Portal.

- **Аналитические отчеты об APT-угрозах (APT Intelligence Reporting) и об угрозах в финансовой индустрии (Financial Threat Intelligence Reporting)**

  Детальные отчеты «Лаборатории Касперского» об APT-угрозах помогут вам повысить осведомленность о масштабных кампаниях кибершпионажа. Отчеты можно загружать в любом доступном формате.

- **Аналитические отчеты об угрозах промышленной кибербезопасности (ICS Threat Intelligence Reporting)**

  Детальные аналитические данные, повышающие осведомленность о вредоносных кампаниях, нацеленных на промышленные организации, а также информация об уязвимостях, обнаруживаемых в наиболее распространенных промышленных системах управления и сопутствующих технологиях

- **Аналитические отчеты об угрозах для конкретной организации (Digital Footprint Intelligence)**

Мониторинг распределенных цифровых ресурсов и отправка уведомлений о выявленных угрозах и атаках.

- **Потоки данных об угрозах (Threat Data Feeds)**

  «Лаборатория Касперского» предлагает инструменты для анализа угроз с доступом к информации, предоставляемой нашими аналитиками и исследователями мирового класса. Эти данные помогут вам противостоять киберугрозам.

- **Надежные аналитические данные об угрозах**

  Ключевым преимуществом аналитики угроз является надежность данных, дополняемых практическими рекомендациями.

- **Широкий охват в реальном времени**

  Аналитика угроз генерируется автоматически в режиме реального времени на основе наблюдений со всего мира, что обеспечивает широкий охват и высокую точность.

- **Разнообразие данных**

  Аналитические данные об угрозах, предоставляемые веб-порталом Kaspersky Threat Intelligence Portal, включают разнообразные типы данных, такие как хеши, веб-адреса, IPадреса, WHOIS, GeoIP, pDNS, атрибуты файлов, статистику и информацию об активности, цепочки загрузок, метки времени и другое. Вооружившись этой информацией, вы сможете противостоять разнообразным угрозам.

- **Постоянная доступность**

  Аналитические данные об угрозах, предоставляемые Kaspersky Threat Intelligence Portal, генерируются и отслеживаются мощной отказоустойчивой инфраструктурой, которая обеспечивает постоянную доступность и бесперебойную работу веб-портала.

- **Постоянное сотрудничество с экспертами по безопасности**

  В подготовке аналитических данных участвуют сотни экспертов, включая аналитиков безопасности со всего мира, специалистов Центра глобальных исследований и анализа угроз (GReAT), а также ведущие команды R&D.

- **Простота использования через веб-портал или API**

  Получайте доступ к данным через веб-портал Kaspersky Threat Intelligence Portal либо с помощью простого API-интерфейса (Kaspersky Threat Intelligence Portal API).

- **Программное обеспечение как услуга (SaaS)**

  Используя программное обеспечение как услугу (SaaS), не требуется интегрировать дополнительные системы или службы в инфраструктуру компании. Начните использовать Kaspersky Threat Intelligence Portal прямо сейчас.

**Ключевые преимущества**

Kaspersky Threat Intelligence Portal обеспечивает следующие преимущества.

- Улучшение и ускорение анализа и реагирования на инциденты. Отделы ИБ или SOC получают ценную информацию об угрозах, а также результаты глобальных исследований

источников целевых атак. Это позволяет более эффективно диагностировать и анализировать инциденты безопасности на серверах и в сети, а также приоритизировать сигналы внутренних систем о различных видах угроз, сводя к минимуму время реагирования на инциденты и предотвращая компрометацию критически важных систем и данных.

- Выявление индикаторов угроз (IP-адреса, вредоносные веб-адреса, хеши файлов) на основе контекстной информации, проверенной экспертами. Это позволяет приоритизировать атаки, оптимально распределять персонал и затраты на IT и ресурсы и устранять в первую очередь те угрозы, которые наиболее опасны для организации.
- Выявление вредоносного содержимого в ваших сетях и центрах обработки данных с помощью аналитических данных об угрозах.

- Защита от целевых атак. Тактические и стратегические данные об угрозах позволяют усовершенствовать защитные механизмы, адаптируя стратегию безопасности для противодействия конкретным угрозам, с которыми может столкнуться ваша организация.

# О зонах и статусах

Все исследуемые объекты распределяются по *зонам*. Зона указывает на уровень опасности объекта. Все объекты, связанные с исследуемым объектом, распределяются по собственным зонам. Их зоны могут не совпадать с зоной исследуемого объекта.

Список зон является общим для всех типов объектов, но не все зоны могут применяться к любым типам объектов.

Каждый тип объектов имеет собственный набор статусов, наиболее точно описывающий уровень опасности объектов этого типа.

Взаимосвязь зон и статусов для всех типов объектов приведена в таблице.

*Зоны и статусы*

| Зона | Уровень опасности | Статус хеша | Статус IPадреса | Статус домена | Статус вебадреса |
|---|---|---|---|---|---|
| Красная | Высокий | Вредоносный | Опасный | Опасный | Опасный |
| Оранжевая | Средний | н. п.* | Недоверенный | Недоверенный | Недоверенный |
| Желтая | Средний | Рекламная или другая программа | Рекламная или другая программа | Рекламная или другая программа | Рекламная или другая программа |
| Серая | Информационный | Категория не определена | Категория не определена | Категория не определена | Категория не определена |

| | | | | | |
|---|---|---|---|---|---|
| Зеленая | Низкий | Безопасный / Угрозы не обнаружены | Безопасный | Безопасный | Безопасный |

* н. п. – не применимо

# Поддерживаемые способы работы

Вы можете работать с Kaspersky Threat Intelligence Portal одним из следующих способов:

**Веб-интерфейс Kaspersky Threat Intelligence Portal**

Можно работать с Kaspersky Threat Intelligence Portal онлайн с помощью любого из поддерживаемых браузеров.

**Плагин Kaspersky Threat Intelligence Portal**

Плагин Kaspersky Threat Intelligence Portal предназначен для пользователей корпоративного уровня, подписанных на коммерческую версию Kaspersky Threat Intelligence Portal. Он позволяет выполнять проверку веб-адресов, IP-адресов, хешей (MD5, SHA-1 и SHA-256) и доменов непосредственно с просматриваемых веб-страниц с помощью функции Kaspersky Threat Intelligence Portal для проверки угроз. Этот плагин также предоставляет подписчикам доступ к обширным контекстным данным об индикаторах компрометации, чтобы быстро принимать решения о приоритизации атак. Плагин способен незамедлительно предоставлять специалистам по безопасности максимально подробные данные об индикаторах компрометации (IoC) для любой веб-страницы, что позволяет ускорить процессы расследования инцидентов. Индикаторы компрометации подсвечиваются автоматически.

Вы можете добавить плагин Kaspersky Threat Intelligence Portal в браузер Chrome™ через интернетмагазин Chrome.

**Kaspersky Threat Intelligence Portal API**

С помощью Kaspersky Threat Intelligence Portal API вы можете создавать запросы для проверки угроз и получения отчетов об угрозах, а также запускать объекты на выполнение в Kaspersky Cloud Sandbox. Также доступны методы API для получения аналитических отчетов об угрозах в финансовой индустрии и об APT-угрозах, для службы отслеживания APT C&C, для получения аналитических отчетов об угрозах промышленной кибербезопасности (ICS) и отчетов об угрозах для конкретной организации (Digital Footprint Intelligence).

# Требования к аппаратному и программному обеспечению

Программные и аппаратные требования для работы с Kaspersky Threat Intelligence Portal:

Минимальные общие требования:

- 2 ГБ свободного места на жестком диске;
- соединение с интернетом для работы с Kaspersky Threat Intelligence Portal в онлайн-режиме;
- открытые порты 443 (HTTPS) и 80 (HTTP);
- монитор, поддерживающий разрешение экрана 1366x768.

Минимальные аппаратные требования:

- Intel® Pentium® 1 ГГц (или совместимый аналог) для 32-разрядной операционной системы;
- Intel Pentium 2 ГГц (или совместимый аналог) для 64-разрядной операционной системы;

  1 ГБ свободной оперативной памяти.

Поддерживаемые браузеры (последние версии):

- Microsoft® Internet Explorer®;
- Mozilla™ Firefox™;
- Google Chrome™;
- Microsoft Edge®;
- Safari®.

Требования к программному обеспечению для работы с Kaspersky Threat Intelligence Portal API:

- Python® 3.5.3.

# Начало работы с Kaspersky Threat Intelligence Portal

## Получение сертификата, имени пользователя и пароля

Для работы с Kaspersky Threat Intelligence Portal требуется сертификат, имя пользователя и пароль.

Вам требуется получить от «Лаборатории Касперского» сертификат, имя пользователя и пароль. Для получения сертификата обратитесь к вашему персональному менеджеру по техническим вопросам «Лаборатории Касперского». Сертификат и учетные данные предоставляются безопасным способом.

После получения сертификата требуется импортировать его на компьютер, предназначенный для работы с Kaspersky Threat Intelligence Portal (при использовании браузеров Microsoft Internet Explorer, Google Chrome или Microsoft Edge). В случае использования браузера Mozilla Firefox дополнительно требуется импортировать сертификат в браузер.

Срок действия сертификата ограничен. Его отсчет начинается с даты выпуска.

Когда срок действия сертификата истечет, Kaspersky Threat Intelligence Portal станет недоступен. Для того чтобы продолжить использование Kaspersky Threat Intelligence Portal, требуется запросить новый сертификат. Новый сертификат и пароль сертификата можно получить у персонального менеджера по техническим вопросам «Лаборатории Касперского». Имя пользователя и пароль остаются прежними и не требуют изменения.

Если во время срока действия сертификата менеджер по техническим вопросам изменит тип доступа к Kaspersky Threat Intelligence Portal (через веб-портал, API или оба способа), сертификат и учетные данные не изменятся.

Сертификат можно установить на неограниченном количестве компьютеров.
Для доступа к Kaspersky Threat Intelligence Portal также можно использовать сертификат WL-info.

# Импорт сертификата

### Импорт сертификата на компьютер

Если вы используете браузеры Microsoft Internet Explorer, Google Chrome или Microsoft Edge, вы можете импортировать сертификат на компьютер с помощью **мастера импорта сертификатов**.

► *Чтобы импортировать сертификат на компьютер, выполните следующие действия:*

1. Сохраните вложение с сертификатом, полученное от персонального менеджера по техническим вопросам «Лаборатории Касперского», на компьютере, который будет использоваться для работы с Kaspersky Threat Intelligence Portal.
2. Откройте сертификат, чтобы запустить **мастер импорта сертификатов**.
3. На странице **Импортируемый файл** выберите нужный сертификат.
4. Введите пароль сертификата, предоставленный персональным менеджером по техническим вопросам «Лаборатории Касперского».
5. Установите флажок **Включить все расширенные свойства**.
6. Укажите расположение для сертификата на компьютере:
   - чтобы операционная система автоматически выбрала хранилище сертификатов, выберите **Автоматически выбрать хранилище на основе типа сертификата**;
   - чтобы указать расположение для сертификата вручную, выберите **Поместить все сертификаты в следующее хранилище**.
7. Нажмите **Готово**, чтобы завершить процесс импорта сертификата.

Теперь ваш сертификат импортирован, и вы можете приступить к работе с веб-порталом Kaspersky Threat Intelligence Portal.

### Импорт сертификата в браузер Mozilla Firefox

Если вы используете Mozilla Firefox, требуется также импортировать сертификат в этот браузер.

► *Чтобы импортировать сертификат в Mozilla Firefox, выполните следующие действия:*

1. Откройте браузер Mozilla Firefox.
2. Откройте закладку **Сертификаты** одним из следующих способов.

- Нажмите на кнопку **Настройки** в нижней части начальной страницы Mozilla Firefox, а затем выберите **Дополнительные** → **Сертификаты**.
- Нажмите на кнопку **Меню**, а затем выберите **Настройки** → **Дополнительные** → **Сертификаты**.

3. Нажмите на кнопку **Просмотр сертификатов** и выберите закладку **Ваши сертификаты**.
4. Нажмите на кнопку **Импортировать**.

   Откроется окно **Импортируемый файл сертификата**.
5. Выберите нужный сертификат и нажмите **Открыть**.
6. Введите пароль сертификата в окне **Ввод пароля** и нажмите на кнопку **ОК**.
7. Отобразится сообщение, подтверждающее успешный импорт.

Теперь ваш сертификат импортирован, и вы можете приступить к работе с порталом Kaspersky Threat Intelligence Portal с помощью Mozilla Firefox.

# Просмотр импортированных сертификатов

**Просмотр сертификата на компьютере**

► *Чтобы просмотреть импортированные сертификаты на компьютере, выполните следующие действия:*

1. Нажмите на кнопку **Пуск**, введите `mmc` в поле **Поиск** и нажмите клавишу **Enter**, чтобы открыть Консоль управления (MMC).
2. Выберите **Файл** → **Добавить или удалить оснастку** и дважды щелкните **Сертификаты** в списке **Доступные оснастки**.

   Откроется окно **Оснастка диспетчера сертификатов**.
3. Выберите **Моей учетной записи пользователя** и нажмите на кнопку **Готово**.
4. Нажмите на кнопку **ОК**, чтобы закрыть окно **Добавление и удаление оснасток**.
5. В окне **Корень консоли** выберите **Сертификаты** → **Текущий пользователь** → **Личное** → **Сертификаты**.
6. Удостоверьтесь, что ваш сертификат от «Лаборатории Касперского» отображается в рабочей области консоли.

**Просмотр сертификата в Mozilla Firefox**

► *Чтобы просмотреть сертификат, импортированный в Mozilla Firefox, выполните следующие действия:*

1. Откройте браузер Mozilla Firefox.
2. Откройте закладку **Сертификаты** одним из следующих способов.
   - Нажмите на кнопку **Настройки** в нижней части начальной страницы Mozilla Firefox, а затем выберите **Дополнительные** → **Сертификаты**.
   - Нажмите на кнопку **Меню**, а затем выберите **Настройки** → **Дополнительные** → **Сертификаты**.

3. Нажмите на кнопку **Просмотр сертификатов** и выберите закладку **Ваши сертификаты**.
4. Удостоверьтесь, что ваш сертификат от «Лаборатории Касперского» отображается в окне **Управление сертификатами**.

Если сертификат не импортирован, повторите попытку импорта или обратитесь к администратору.

# Вход в учетную запись Kaspersky Threat Intelligence Portal

В этом разделе описано, как войти в учетную запись Kaspersky Threat Intelligence Portal. При первом входе в учетную запись Kaspersky Threat Intelligence Portal или после приобретения новой услуги Kaspersky Threat Intelligence Portal требуется принять Условия использования и Заявление о предоставлении данных. Также требуется подтверждать принятие условий использования в случае их изменения «Лабораторией Касперского».

Перед входом в учетную запись Kaspersky Threat Intelligence Portal удостоверьтесь, что ваш сертификат импортирован на компьютер и в браузер (в случае использования Mozilla Firefox), который вы планируете использовать для работы с Kaspersky Threat Intelligence Portal в интернете.

Перед работой с Kaspersky Threat Intelligence Portal API требуется принять Условия использования, перейдя в браузере по следующей ссылке: https://tip.kaspersky.com.

► *Чтобы войти в учетную запись Kaspersky Threat Intelligence Portal, выполните следующие действия:*

1. Откройте Kaspersky Threat Intelligence Portal в браузере по ссылке https://tip.kaspersky.com.
2. Выберите нужный сертификат для аутентификации на веб-портале и нажмите на кнопку **ОК**.

   В поддерживаемых браузерах отображаются только сертификаты «Лаборатории Касперского», которые можно использовать для аутентификации на портале Kaspersky Threat Intelligence Portal.

3. Введите имя пользователя и пароль, полученные от «Лаборатории Касперского» после запроса сертификата.

   Имя пользователя и пароль можно использовать для аутентификации только на одном компьютере одновременно.

4. Если вам разрешено работать с Kaspersky Threat Intelligence Portal без сертификата, для входа требуется пройти тест reCAPTCHA.

   Установите флажок **Я не робот** в виджете reCAPTCHA и следуйте инструкциям для прохождения теста reCAPTCHA.

5. Нажмите **Sign In**.
6. Если хотите узнать больше о возможностях продукта, перейдите по ссылке **Get more info about Kaspersky Threat Intelligence Portal**.

   Эта ссылка недоступна для пользователей Kaspersky Anti Targeted Attack и Kaspersky Endpoint Detection and Response.

7. Если требуется связаться с представителями «Лаборатории Касперского», нажмите на кнопку **Request Access**.

   Заполните форму на открывшейся странице, и представитель «Лаборатории Касперского» свяжется с вами в течение одного рабочего дня.

Если на компьютер не импортирован действительный сертификат, Kaspersky Threat Intelligence Portal возвращает ошибку 403 (*Доступ запрещен*).

Сбой при входе в учетную запись Kaspersky Threat Intelligence Portal может произойти по одной из следующих причин:

- неверное имя пользователя или пароль;
- сертификат недействителен, поврежден или просрочен;
- учетная запись пользователя или группа, к которой она принадлежит, заблокирована.

Количество попыток аутентификации на веб-портале не ограничено.

# Принятие Условий использования и Заявления о предоставлении данных

В этом разделе описан порядок принятия Условий использования и Заявления о предоставлении данных.

Перед первым входом в учетную запись Kaspersky Threat Intelligence Portal или использованием нового решения требуется принять Условия использования и Заявление о предоставлении данных. Также требуется принять Условия использования в случае их изменения.

Перед работой с Kaspersky Threat Intelligence Portal API требуется принять Условия использования в интернете, перейдя в браузере по ссылке https://tip.kaspersky.com.

► *Чтобы принять Условия использования и Заявление о предоставлении данных, выполните следующие действия:*

1. В окне, которое открывается после нажатия на кнопку **Sign In** на странице https://tip.kaspersky.com в браузере, внимательно прочитайте Условия использования и Заявление о предоставлении данных.

Если это ваш первый вход в учетную запись Kaspersky Threat Intelligence Portal, отображаются Условия использования и Заявление о предоставлении данных для всех приобретенных решений.

Если вы открываете страницу для нового приобретенного решения, отображаются Условия использования и Заявление о предоставлении данных только для этого решения.

2. Если вы согласны с Условиями использования и Заявлением о предоставлении данных, в блоке **I confirm I have fully read, understood, and accept the following** установите следующие флажки:
   - **Terms and Conditions of <название решения> (Условия использования)**
   - **Statement About Data Provision (Заявление о предоставлении данных)**

   Если вы не согласны с Условиями использования и Заявлением о предоставлении данных, нажмите на ссылку **Cancel**, чтобы отменить вход.
3. Нажмите на кнопку **Confirm**.

   Кнопка **Confirm** становится доступна только после прокрутки текста Условий использования и установки обоих флажков.
4. Если требуется, в любой момент вы можете перейти по ссылке **Terms and Conditions** в нижней части страницы Kaspersky Threat Intelligence Portal, чтобы прочитать Условия использования и Заявление о предоставлении данных.

# Лицензирование

## Об Условиях использования

Условия использования – это обязательное соглашение между вами и АО «Лаборатория Касперского», в котором изложены условия, на которых вы можете пользоваться Kaspersky Threat Intelligence Portal.

Перед началом использования Kaspersky Threat Intelligence Portal внимательно прочитайте Условия использования.

Вы принимаете Условия использования, подтверждая свое согласие с ними при входе в учетную запись Kaspersky Threat Intelligence Portal. Если вы не примете Условия использования, вы не сможете войти в учетную запись Kaspersky Threat Intelligence Portal.

Если требуется, в любой момент вы можете перейти по ссылке **Terms and Conditions** в нижней части страницы Kaspersky Threat Intelligence Portal, чтобы прочитать Условия использования.

# О лицензии

*Лицензия* – это право на использование Kaspersky Threat Intelligence Portal в течение ограниченного времени, предоставляемое согласно контракту с «Лабораторией Касперского».

Лицензия предоставляет права на следующие виды услуг:

- право на использование Kaspersky Threat Intelligence Portal;
- поддержка персонального менеджера по техническим вопросам.

Для использования решений Kaspersky Threat Intelligence Portal требуется приобрести лицензию.

Условия использования решений зависят от типа лицензии.

Доступны следующие типы лицензий.

**Для Kaspersky Cloud Sandbox**

- *Пробная*. Тип лицензии с ограниченным доступом к функциональным возможностям Kaspersky Cloud Sandbox. Пробная лицензия имеет ограниченный срок использования и следующие ограничения.
- Квота на количество выполнений файлов и анализов веб-адресов в Kaspersky Cloud Sandbox предоставляется на весь срок действия лицензии, включая срок действия коммерческой лицензии.
- Сохраняется до 1000 последних результатов выполнений файлов и анализов вебадресов. По достижении максимального числа сохраненных результатов самым старым результатам назначается статус *Discarded*. Для таких задач можно только просмотреть краткую сводку (или удалить ее).
- Пробная лицензия обычно имеет короткий срок действия. После истечения срока действия пробной лицензии нельзя будет выполнять файлы или анализировать вебадреса в Kaspersky Cloud Sandbox. Результаты предыдущих выполнений файлов остаются доступными. Чтобы продолжить использование функциональных возможностей Kaspersky Cloud Sandbox, требуется приобрести коммерческую лицензию.
- *Коммерческая*. Лицензия, которая предоставляется при приобретении решений Kaspersky Threat Intelligence Portal. Выделяются ежедневные квоты для Kaspersky Cloud Sandbox. Сохраняется до 1000 последних результатов выполнений файлов и анализов веб-адресов. По достижении максимального числа сохраненных результатов самым старым результатам назначается статус *Discarded*. Для таких задач можно только просмотреть краткую сводку (или удалить ее).

Выполнение запроса на проверку угроз по хешу не уменьшает квоту на проверку угроз для группы в случае наличия завершенной задачи на выполнение для этого хеша в Cloud Sandbox.

**Аналитические отчеты об угрозах в финансовой индустрии (Financial Threat Intelligence Reporting)**

- *Демонстрационная*. Тип лицензии, предназначенный для пробного использования Аналитических отчетов об угрозах в финансовой индустрии.

Демонстрационная лицензия имеет ограниченный срок использования и следующие ограничения.

- Для загрузки доступен только ограниченный список аналитических отчетов об угрозах в финансовой индустрии.
- Отчеты Master YARA и Master IOC недоступны для загрузки.
- Полнотекстовый поиск доступен только для ограниченного числа аналитических отчетов об угрозах в финансовой индустрии (только для файлов отчетов, доступ к которым предоставлен пользователю).
- Уведомления о новых и обновленных аналитических отчетах об угрозах в финансовой индустрии недоступны.
- В окне выбора тегов **Actor** доступны только теги, используемые для ограниченного списка аналитических отчетов об угрозах в финансовой индустрии.
- *Пробная*. Тип лицензии с ограниченным доступом к Аналитическим отчетам об угрозах в финансовой индустрии. Пробная лицензия имеет ограниченный срок использования и следующие ограничения.
- Доступны только аналитические отчеты об угрозах в финансовой индустрии старше семи дней.
- Уведомления о доступности для загрузки аналитического отчета об угрозах в финансовой индустрии отправляются через семь дней с момента его появления или обновления.
- Можно загрузить до десяти аналитических отчетов об угрозах в финансовой индустрии.
- Отчеты Master YARA и Master IOC недоступны для загрузки.
- Полнотекстовый поиск доступен только по наименованиям и описаниям аналитических отчетов об угрозах в финансовой индустрии, за исключением демонстрационных отчетов. Для демонстрационных отчетов доступен полнотекстовый поиск по наименованиям, описаниям и всем доступным файлам отчетов.
- Пробная лицензия обычно имеет короткий срок действия. По истечении срока действия пробной лицензии доступ может переключиться в ограниченный демонстрационный режим. Чтобы продолжить использование Аналитических отчетов об угрозах в финансовой индустрии, требуется приобрести коммерческую лицензию.
- *Коммерческая*. Лицензия, которая предоставляется при приобретении решений Kaspersky Threat Intelligence Portal. Коммерческая лицензия имеет ограниченный срок действия.

Количество пользователей решения и другие квоты для компании определяются контрактом с «Лабораторией Касперского». Если не продлить срок действия коммерческой лицензии, доступ может переключиться в ограниченный демонстрационный режим. **Аналитические отчеты об APT-угрозах**

- *Демонстрационная*. Тип лицензии, предназначенный для пробного использования Аналитических отчетов об APT-угрозах.

Демонстрационная лицензия имеет ограниченный срок использования и следующие ограничения.

- Для загрузки доступен только ограниченный список аналитических отчетов об APTугрозах.
- Отчеты Master YARA и Master IOC недоступны для загрузки.
- Полнотекстовый поиск доступен только для ограниченного числа аналитических отчетов об APT-угрозах (для файлов отчетов, доступ к которым предоставлен пользователю).
- Уведомления о новых и обновленных аналитических отчетах об APT-угрозах недоступны.
- В окне выбора тегов **Actor** доступны только теги, используемые для ограниченного списка аналитических отчетов об APT-угрозах.
- Профили доступны только для тех группировок, которые связаны с отчетами, входящими в ограниченное число аналитических отчетов об APT-угрозах, доступ к которым предоставлен пользователю.
- *Пробная*. Тип лицензии с ограниченным доступом к Аналитическим отчетам об APT-угрозах. Пробная лицензия имеет ограниченный срок использования и следующие ограничения.
- Доступны только аналитические отчеты об APT-угрозах старше семи дней.
- Уведомления о доступности для загрузки аналитического отчета об APT-угрозах отправляются через семь дней с момента его появления или обновления.
- Можно загрузить до десяти аналитических отчетов об APT-угрозах.
- Отчеты Master YARA и Master IOC недоступны для загрузки.
- Полнотекстовый поиск доступен только по наименованиям и описаниям аналитических отчетов об APT-угрозах, за исключением демонстрационных отчетов. Для демонстрационных отчетов доступен полнотекстовый поиск по наименованиям, описаниям и всем доступным файлам отчетов.
- Профили доступны только для тех группировок, которые связаны с отчетами, входящими в ограниченное число аналитических отчетов об APT-угрозах, доступ к которым предоставлен пользователю.
- Пробная лицензия обычно имеет короткий срок действия. По истечении срока действия пробной лицензии доступ может переключиться в ограниченный демонстрационный режим. Чтобы продолжить использование Аналитических отчетов об APT-угрозах, требуется приобрести коммерческую лицензию.
- *Коммерческая*. Лицензия, которая предоставляется при приобретении решений Kaspersky Threat Intelligence Portal. Коммерческая лицензия имеет ограниченный срок действия. Количество пользователей решения и другие квоты для компании определяются контрактом с «Лабораторией Касперского». Если не продлить срок действия коммерческой лицензии, доступ может переключиться в ограниченный демонстрационный режим.

Если вы не приобрели лицензию на аналитические отчеты об APT-угрозах или аналитические отчеты об угрозах в финансовой индустрии, уведомления будут недоступны.

**Аналитические отчеты об угрозах промышленной кибербезопасности**

- *Демонстрационная*. Тип лицензии, предназначенный для пробного использования Аналитических отчетов об угрозах промышленной кибербезопасности.

Демонстрационная лицензия имеет ограниченный срок использования и следующие ограничения.

- Для загрузки доступен только ограниченный список аналитических отчетов об угрозах промышленной кибербезопасности.
- Отчеты Master YARA и Master IOC недоступны для загрузки.
- Полнотекстовый поиск доступен только для ограниченного числа аналитических отчетов об угрозах промышленной кибербезопасности (для файлов отчетов, доступ к которым предоставлен пользователю).
- Уведомления о новых и обновленных аналитических отчетах об угрозах промышленной кибербезопасности недоступны.
- В окне выбора тегов **Actor** доступны только теги, используемые для ограниченного списка аналитических отчетов об угрозах промышленной кибербезопасности.
- *Пробная*. Тип лицензии с ограниченным доступом к аналитическим отчетам об угрозах промышленной кибербезопасности. Пробная лицензия имеет ограниченный срок использования и следующие ограничения.
- Доступны только аналитические отчеты об угрозах промышленной кибербезопасности старше семи дней.
- Уведомления о доступности для загрузки аналитического отчета об угрозах промышленной кибербезопасности отправляются через семь дней с момента его появления или обновления.
- Можно загрузить до десяти аналитических отчетов об угрозах промышленной кибербезопасности.
- Отчеты Master YARA и Master IOC недоступны для загрузки.
- Полнотекстовый поиск доступен только по наименованиям и описаниям аналитических отчетов об угрозах промышленной кибербезопасности, за исключением демонстрационных отчетов. Для демонстрационных отчетов доступен полнотекстовый поиск по наименованиям, описаниям и всем доступным файлам отчетов.
- Пробная лицензия обычно имеет короткий срок действия. По истечении срока действия пробной лицензии доступ может переключиться в ограниченный демонстрационный режим. Чтобы продолжить использование Аналитических отчетов об угрозах промышленной кибербезопасности, требуется приобрести коммерческую лицензию.
- *Коммерческая*. Лицензия, которая предоставляется при приобретении решений Kaspersky Threat Intelligence Portal. Коммерческая лицензия имеет ограниченный срок действия. Количество пользователей решения и другие квоты для компании определяются контрактом с «Лабораторией Касперского». Если не продлить срок действия коммерческой лицензии, доступ может переключиться в ограниченный демонстрационный режим.

Если вы не приобрели лицензию на Аналитические отчеты об угрозах промышленной кибербезопасности, уведомления будут недоступны.

**Поиск угроз (Threat Lookup) / Поиск по базе WHOIS / Мониторинг по базе WHOIS**

- *Пробная*. Квоты для Поиска угроз и Поиска по базе WHOIS предоставляются на срок действия лицензии. Для Мониторинга по базе WHOIS предоставляется отдельная квота. После истечения срока действия пробной лицензии создание запросов на поиск и правил отслеживания будет недоступно.
- *Коммерческая*. Предоставляются ежедневные квоты для Поиска угроз и Поиска по базе WHOIS. Для Мониторинга по базе WHOIS предоставляется отдельная ежедневная квота. После истечения срока действия коммерческой лицензии создание запросов на поиск и правил отслеживания будет недоступно.

Выполнение запроса на поиск угроз по хешу не уменьшает квоту на проверку угроз для группы в случае наличия завершенной задачи на выполнение для этого хеша в Cloud Sandbox.

Сведения о лицензии можно найти на странице **Licensing**.

Рекомендуется продлевать срок действия лицензии до его истечения. **Служба**

**отслеживания APT C&C**

- *Пробная*. Тип лицензии с ограниченным доступом к службе отслеживания APT C&C. Пробная лицензия имеет ограниченный срок использования и следующие ограничения.
- Потоки данных доступны только для страны, указанной сотрудником «Лаборатории Касперского» при заключении контракта.
- Пробная лицензия обычно имеет короткий срок действия. После истечения срока действия пробной лицензии служба становится недоступной для пользователя. Чтобы продолжить использование Службы отслеживания APT C&C, требуется приобрести коммерческую лицензию.
- *Коммерческая*. Лицензия, которая предоставляется при приобретении решений Kaspersky Threat Intelligence Portal. Коммерческая лицензия имеет ограниченный срок действия. Количество пользователей решения и другие квоты для компании определяются контрактом с «Лабораторией Касперского». После истечения срока действия коммерческой лицензии служба становится недоступной для пользователя.

**Аналитические отчеты об угрозах для конкретной организации (Digital Footprint Intelligence)**

- *Демонстрационная*. Тип лицензии, предназначенный для пробного использования Аналитических отчетов об угрозах для конкретной организации.

Демонстрационная лицензия имеет ограниченный срок использования и следующие ограничения.

- Для просмотра и загрузки доступен только анонимизированный демонстрационный отчет.
- Для просмотра доступен только ограниченный список анонимизированных уведомлений об угрозах.
- Другие функции доступны только для демонстрационных данных.
- *Коммерческая*. Лицензия, которая предоставляется при приобретении решений Kaspersky Threat Intelligence Portal. Коммерческая лицензия имеет ограниченный срок действия.

Количество пользователей решения и другие квоты для компании определяются контрактом с «Лабораторией Касперского». Если срок действия коммерческой лицензии не продлен, сохраняется доступ к данным, полученным в течение периода действия лицензии. Новые данные не будут предоставляться до тех пор, пока не будет продлен срок действия лицензии.

# Приобретение лицензии

Для приобретения лицензии используется следующая процедура.

► *Чтобы приобрести лицензию, выполните следующие действия:*

1. В окне сведений о пользователе перейдите по ссылке **Licensing**.
2. На странице **Licenses** нажмите на кнопку **Purchase license** рядом с решением Kaspersky Threat Intelligence Portal, для которого требуется приобрести лицензию.

Откроется окно **Request form**.

3. Удостоверьтесь, что в запросе указано нужное решение, и нажмите на кнопку **Send**.
4. Либо нажмите на кнопку **Purchase license** на странице нужного решения Kaspersky Threat Intelligence Portal.

   Также вы можете запросить демонстрацию нужного решения.

# Предоставление данных

При использовании Kaspersky Threat Intelligence Portal помимо данных, предоставляемых в соответствии с Условиями использования, следующие типы данных автоматически передаются и обрабатываются для описанных ниже целей.

«Лаборатория Касперского» защищает любую полученную информацию в соответствии с требованиями законодательства и применимыми правилами «Лаборатории Касперского». Для передачи данных используется защищенный канал.

Все полученные данные хранятся в течение периода действия лицензии. По истечении срока хранения данные удаляются из баз данных оперативной обработки транзакций (OLTP).

Вы можете в любое время отозвать согласие на предоставление данных, описанных ниже. Чтобы отозвать согласие, обратитесь к персональному менеджеру по техническим вопросам «Лаборатории Касперского» по адресу ktlsupport@kaspersky.com.

**Обрабатываемые данные**

**Общие действия пользователей**

В целях оптимизации обнаружения угроз и для обработки запросов пользователей к решениям Kaspersky Threat Intelligence Portal *для каждого действия пользователя* во время работы с Kaspersky Threat Intelligence Portal, в соответствии с требованиями лицензии и Условиями использования, портал получает следующие данные:

- дата и время выполнения действия;
- IP-адрес (также используется для блокировки учетных записей, которые слишком часто пытаются войти в систему Kaspersky Threat Intelligence Portal);
- строка User-Agent;
- имя пользователя (имя учетной записи).

**Подтверждение Условий использования**

Для обработки запросов пользователей к решениям Kaspersky Threat Intelligence Portal, в соответствии с требованиями лицензии, портал получает следующие данные:

- подтверждение (установка флажка **I confirm I have fully read, understood, and accept the following: Terms and Conditions of <список доступных решений>**).

**Подтверждение Заявления о предоставлении данных**

Для обработки запросов пользователей к решениям Kaspersky Threat Intelligence Portal, в соответствии с требованиями лицензии, портал получает следующие данные:

- подтверждение (установка флажка **I confirm I have fully read, understood, and accept the following: Statement About Data Provision**).

**Вход в учетную запись Kaspersky Threat Intelligence Portal**

Для аутентификации пользователей и проверки соблюдения требований текущей лицензии *при входе в учетную запись Kaspersky Threat Intelligence Portal*, в соответствии с условиями использования, портал получает следующие данные:

- сертификат;
- пароль (соль и хеш);
- имя пользователя (имя учетной записи);
- идентификатор сессии, который также сохраняется в локальном хранилище браузера пользователя.

**Аналитические отчеты об APT-угрозах, Аналитические отчеты об угрозах в финансовой индустрии и Аналитические отчеты об угрозах промышленной кибербезопасности**

Для генерации подсказок при вводе данных пользователями и поиска запрашиваемого текста (полнотекстовый поиск) *запросы к службе отчетов* принимаются, сохраняются и обрабатываются в соответствии с Условиями использования.

**Поиск угроз (Threat Lookup)**

Для поиска запрашиваемых объектов, отображения последних запросов пользователей и проверки соблюдения требований текущей лицензии *при использовании решения по поиску угроз (Threat Lookup)* портал Kaspersky Threat Intelligence Portal получает следующие данные:

- запрос;
- просмотр последних запросов (только действие, без получения данных);
- результаты запроса.

**Мониторинг по базе WHOIS**

Для расследования проблем, проверки соблюдения требований текущей лицензии и уведомления пользователей *при использовании Мониторинга по базе WHOIS* портал Kaspersky Threat Intelligence Portal, в соответствии с Условиями использования, получает следующие данные:

- 

полное имя пользователя;

- имя пользователя (имя учетной записи).

**Поиск по базе WHOIS**

Для расследования проблем, отображения последних запросов пользователей и проверки соблюдения требований текущей лицензии *при использовании Поиска по базе WHOIS* портал Kaspersky Threat Intelligence Portal получает следующие данные:

- запрос;
- просмотр последних запросов (только действие, без получения данных);
- результаты запроса.

**Cloud Sandbox: выполнение загружаемых или скачиваемых файлов**

Для расследования проблем, отображения последних запросов пользователей и проверки соблюдения требований текущей лицензии *при выполнении файла в Cloud Sandbox* портал Kaspersky Threat Intelligence Portal получает следующие данные:

- запрос (исполняемый файл);
- параметры загрузки файла (веб-адрес, HTTP-запросы, HTTPS-запросы) – только для скачиваемых файлов;
- параметры выполнения файла (среда выполнения, время выполнения, указанное расширение файла, тип выполнения, расшифровка трафика HTTPS);
- результаты выполнения файла (имена детектируемых в изолированной среде объектов, сработавшие сетевые правила, карта выполнения, подозрительные действия, снимки экрана, загруженные образы PE, операции с файлами, операции с реестром, операции с процессами, операции синхронизации, скачанные файлы, внедренные файлы, HTTP-запросы, HTTPSзапросы, DNS-запросы);
- просмотр последних запросов (хеш выполняемого файла, дата и время выполнения и анализа файла, размер файла, тип файла, хеш MD5).

**Cloud Sandbox: динамический анализ веб-адресов**

Для расследования проблем, отображения последних запросов пользователей и проверки соблюдения требований текущей лицензии *при анализе веб-адреса в Cloud Sandbox* портал Kaspersky Threat Intelligence Portal получает следующие данные:

- запрос (веб-адрес);

- параметры анализа веб-адреса (среда браузера, время просмотра веб-страницы, расшифровка трафика HTTPS);
- результаты анализа веб-адреса (имена детектируемых в изолированной среде объектов, сработавшие сетевые правила, подозрительные действия, хосты, данные WHOIS, снимки экрана, HTTP-запросы, HTTPS-запросы, DNS-запросы);
- просмотр последних запросов (анализируемый веб-адрес, дата и время анализа веб-адреса).

**Управление учетными записями**

Для проверки соблюдения требований текущей лицензии *при создании новой учетной записи* портал Kaspersky Threat Intelligence Portal, в соответствии с Условиями использования, получает следующие данные:

- роль (администратор или пользователь);
- тип (доступ с помощью веб-интерфейса, RESTful API или оба варианта доступа);
- полное имя пользователя;
- имя пользователя (имя учетной записи);
- имя пользователя (имя учетной записи) – автора изменений.

**Аналитические отчеты об угрозах для конкретной организации (Digital Footprint Intelligence)**

Для обнаружения непосредственных угроз организации и предоставления сведений о них пользователю, выполнения текстового поиска по запросу пользователя и фильтрации полученных результатов портал Kaspersky Threat Intelligence Portal при использовании Аналитических отчетов об угрозах для конкретной организации (Digital Footprint Intelligence) получает следующие данные:

- сведения об организации;
- сведения об обнаруженных уязвимостях для этой организации;
- поисковые запросы пользователя.

# Аналитические отчеты об APTугрозах

Аналитические отчеты об APT-угрозах предоставляют клиентам эксклюзивный проактивный доступ к описаниям известных кампаний кибершпионажа, включая связанные индикаторы компрометации (IoC). Отчеты доступны в форматах CSV и правил YARA. Теперь аналитические отчеты об APTугрозах и связанные индикаторы компрометации можно запрашивать с помощью RESTful API. Также реализован комплексный полнотекстовый поиск и поиск по тегам.

Kaspersky Threat Intelligence Portal позволяет просматривать профили группировок, их тактики, методы и процедуры (TTP), сопоставленные с данными MITRE ATT&CK, а также полные технические характеристики каждой обнаруженной APT-угрозы в различных форматах, включая угрозы, информация о которых никогда не попадала в общий доступ. Информация в этих отчетах помогает быстро реагировать на различные угрозы и уязвимости: блокировать атаки известными способами, уменьшать ущерб от комплексных атак и оптимизировать общую стратегию безопасности.

Kaspersky Threat Intelligence Portal позволяет выполнять следующие действия с аналитическими отчетами об APT-угрозах.

Находить и просматривать отчеты, которые доступны пользователю в соответствии с лицензией группы и разрешениями.

- Находить и просматривать профили группировок, которые доступны пользователю в соответствии с лицензией группы и разрешениями.
- Загружать мастер-файлы для профилей группировок. Мастер-файлы представляют собой ZIPархивы, содержащие все файлы YARA/IOC из всех отчетов, которые связаны с выбранным профилем киберпреступника и доступны согласно разрешениям пользователя.
- Использовать теги *Industry*, *Geo* и *Actor* для уточнения результатов поиска отчетов.

# Служба отслеживания APT C&C

Служба отслеживания APT C&C предоставляет IP-адреса инфраструктуры, связанной с продвинутыми угрозами. Это помогает ИБ-аналитикам, работающим в группах экстренного реагирования на киберинциденты (CERT), государственных центрах мониторинга и реагирования (SOC) и органах государственной безопасности, отслеживать распространение нового вредоносного ПО, чтобы принимать необходимые меры для противодействия текущим и будущим атакам. Данные службы ежедневно обновляются с учетом последних наблюдений экспертов глобального центра исследования и анализа угроз «Лаборатории Касперского» (GReAT), который известен успешными расследованиями APT-кампаний по всему миру. Для каждого IP-адреса указывается название связанной с ним APT-группы, операции или вредоносного ПО, а также интернет-провайдер, автономная система, набор связанных IP-адресов, на которых размещена информация, и даты первого и последнего наблюдений. Список IP-адресов можно скачивать в машиночитаемом формате, что позволяет клиентам выгружать их в существующие решения безопасности для автоматического обнаружения угроз.

Kaspersky Threat Intelligence Portal позволяет выполнять следующие действия со Службой отслеживания APT C&C.

- Просмотр IP-адресов, связанных с командными центрами APT-угроз (APT C&C).
- Экспорт информации об IP-адресах, связанных с APT C&C.
- Просмотр активности для IP-адресов, связанных с APT C&C.

# Аналитические отчеты об угрозах в финансовой индустрии

Аналитические отчеты об угрозах в финансовой индустрии позволяет финансовым учреждениям реализовывать стратегии защиты благодаря своевременному получению сведений об атаках, направленных на банки, платежные системы, страховые компании и т. д.

Аналитические отчеты об угрозах в финансовой индустрии предоставляют клиентам эксклюзивную информацию по следующим вопросам:

- атаки на инфраструктуры банков;
- атаки на банкоматы;
- атаки на POS-терминалы;
- мобильные банковские троянцы;
- новые методы атак, используемые киберпреступниками для обхода современных защитных решений;
- гибридные атаки с мониторингом активности киберпреступников на раннем этапе (регистрируемые домены и т. д.).

Для каждого отчета доступны краткие сведения, технический анализ атаки и индикаторы компрометации (IOC) в форматах CSV и правил YARA. Также поддерживается RESTful API и комплексный полнотекстовый поиск.

Kaspersky Threat Intelligence Portal позволяет выполнять следующие действия с аналитическими отчетами об угрозах для финансовых организаций.

- Находить и просматривать отчеты, которые доступны пользователю в соответствии с лицензией группы и разрешениями.
- Загружать мастер-файлы. Мастер-файлы представляют собой ZIP-архивы, содержащие все файлы YARA/IOC из отчетов, которые доступны согласно разрешениям пользователя.
- Использовать теги *Industry*, *Geo* и *Actor* для уточнения результатов поиска отчетов.

# Аналитические отчеты об угрозах промышленной кибербезопасности

Аналитические отчеты об угрозах промышленной кибербезопасности предоставляют детальные аналитические данные и повышают осведомленность о вредоносных кампаниях, нацеленных на промышленные организации, а также информацию об уязвимостях, обнаруживаемых в наиболее распространенных промышленных системах управления и сопутствующих технологиях. Предоставляются отчеты о проблемах безопасности, связанных с АСУ ТП, а также правила YARA. Отчеты содержат углубленный технический анализ атак, направленных на промышленные компании, интернет вещей, промышленный интернет вещей и автомобильную промышленность, а также

результаты исследований уязвимостей, описание исследуемого продукта, методику исследований, этапы, выявленные уязвимости и выводы.

Kaspersky Threat Intelligence Portal позволяет выполнять следующие действия с аналитическими отчетами об угрозах промышленной кибербезопасности.

- Находить и просматривать отчеты, которые доступны пользователю в соответствии с лицензией группы и разрешениями.

  Загружать мастер-файлы для профилей группировок. Мастер-файлы представляют собой ZIPархивы, содержащие все файлы YARA/IOC из всех отчетов, которые связаны с выбранным профилем группировки и доступны согласно разрешениям пользователя.

- Использовать теги *Industry*, *Geo* и *Actor* для уточнения результатов поиска отчетов.

# Поиск угроз

Для поиска индикаторов компрометации можно использовать веб-интерфейс или Kaspersky Threat Intelligence Portal API. Kaspersky Threat Intelligence Portal позволяет запрашивать аналитические данные об угрозах для следующих объектов:

- хеши MD5, SHA-1 и SHA-256;
- IP-адреса;
- домены;
- веб-адреса.

Kaspersky Threat Intelligence Portal показывает, относится ли объект к категориям *Безопасный*, *Небезопасный* или *Категория не определена*, а также предоставляет богатый набор контекстных данных для ответа на вопросы «кто?», «что?», «где?» и «когда?», которые помогают более эффективно реагировать на угрозы или расследовать их.

Kaspersky Threat Intelligence Portal позволяет экспортировать результаты исследований для запрашиваемых объектов с целью дополнительного анализа. Можно экспортировать следующие данные:

- результаты исследований из всех таблиц, доступных для запрашиваемого объекта;
- отдельные результаты исследований из выбранной таблицы.

# Поиск по базе WHOIS

С помощью Kaspersky Threat Intelligence Portal можно искать в базе WHOIS информацию о доменах и IP-адресах.

# Мониторинг по базе WHOIS

С помощью Kaspersky Threat Intelligence Portal можно создавать правила для отслеживания по базе WHOIS информации о доменах и IP-адресах.

Можно использовать определенные поля данных WHOIS для регулярного и автоматического поиска записей, соответствующих критериям. Получателям автоматически отправляются уведомления по электронной почте о новых записях в базе данных WHOIS, которые соответствуют критериям поиска. Например, можно получать уведомления о новых доменах, зарегистрированных лицом с определенными контактными данными (имя, адрес электронной почты и т. д.).

# Kaspersky Cloud Sandbox

Kaspersky Cloud Sandbox – усовершенствованная автоматизированная система анализа вредоносного ПО, которая была разработана на основе технологии песочницы «Лаборатории Касперского» и ранее использовалась только во внутренней инфраструктуре «Лаборатории Касперского». Эта технология развивалась в течение более 20 лет, посвященных постоянному исследованию угроз и выпуску самых совершенных решений безопасности. В этом решении используется гибридный подход, сочетающий в себе исследование угроз на основе петабайтов статистических данных (благодаря Kaspersky Security Network), поведенческий анализ и надежные технологии противостояния обходу защиты и моделирования поведения человека, такие как автокликер, прокрутка документов и фиктивные процессы.

В результате Cloud Sandbox обеспечивает высочайший уровень обнаружения – ежедневно выявляются тысячи новых вредоносных файлов. Это преимущество позволяет клиентам обнаруживать комплексные таргетированные угрозы (благодаря экспертам «Лаборатории Касперского» по защите от APT-угроз), а также целевые и сложные угрозы, которые обходят традиционные антивирусные решения.

Песочница Cloud Sandbox предназначена для повышения эффективности реагирования на инциденты и расследования угроз, а также может использоваться как облачная система для автоматической обработки файлов. Также доступны такие возможности, как графики для визуализации данных, экспорт в форматы JSON/STIX™/CSV и поддержка REST API для автоматической интеграции в рабочие процессы клиента.

Удобный интерфейс позволяет легко понимать действия и поведение выполняемых файлов, такие как:

- загрузка и запуск библиотек DLL;
- создание взаимных исключений (мьютексы);
- изменение и создание разделов реестра;
- внешнее соединение с доменными именами и IP-адресами;
- HTTP- и DNS-запросы;

- создание процессов с помощью выполняемого файла;
- создание, изменение и удаление файлов;
- подробная информация об угрозах с контекстными рекомендациями для каждого выявленного индикатора компрометации;
- снимки сетевой активности: файлы дампа, захват пакетов (PCAP);
- интуитивно понятные отчеты (операции с объектами, подозрительная активность);
- человекочитаемый журнал Cloud Sandbox (для продвинутых пользователей);
- статистическая информация;
- снимки экрана;  и многое другое.

Kaspersky Threat Intelligence Portal позволяет выполнять следующие действия с использованием Cloud Sandbox.

- Загрузка и выполнение файла в Cloud Sandbox.
- Скачивание файла с веб-адреса с последующим выполнением в Cloud Sandbox.
- Просмотр веб-адреса в Cloud Sandbox.
- Выполнение извлеченного файла из отчета Cloud Sandbox.
- Экспорт результатов анализа.
- Автоматическое определение типов файлов.
- Управление устаревшими задачами на выполнение.

# Аналитические отчеты об угрозах для конкретной организации

Решение Аналитические отчеты об угрозах для конкретной организации (Digital Footprint Intelligence) осуществляет мониторинг распределенных цифровых ресурсов и отправляет уведомления о выявленных угрозах и атаках. Это помогает ИБ-аналитикам оценивать корпоративную среду и уязвимые цифровые активы с точки зрения злоумышленников, своевременно обнаруживать потенциальные векторы атак и соответствующим образом адаптировать защиту. Наши эксперты составят подробную картину угроз, актуальных для вашей организации, выявят уязвимости в вашей системе защиты и найдут признаки завершенных, текущих и планируемых атак. Доступны человекочитаемые отчеты, а также уведомления практически в режиме реального времени. При необходимости пользователи могут выбирать цифровые активы для мониторинга, а также составлять список игнорируемых активов, которые следует исключить.

## Уведомления об угрозах

Kaspersky Threat Intelligence Portal предоставляет уведомления о выявленных уязвимостях, которые могут уменьшить уровень защиты организации.

*Уведомления об угрозах* могут включать информацию о скомпрометированных учетных данных, утечках информации, незащищенных сервисах в сетевом периметре, угрозах со стороны персонала и т. д.

Уведомления об угрозах отображаются на закладке **Threats** страницы **Digital Footprint**. Круговая диаграмма **Threat risks** представляет общее число выявленных уязвимостей и их уровень опасности (*Critical*, *High*, *Medium*, *Low*, *Info*).

# Аналитические отчеты об угрозах для конкретной организации

Kaspersky Threat Intelligence Portal предоставляет аналитические отчеты об угрозах, специфичных для вашей организации.

*Аналитические отчеты об угрозах для конкретной организации* создаются с использованием анализа открытых источников (OSINT), а также мощных экспертных систем и баз данных «Лаборатории Касперского».

Аналитические отчеты об угрозах для конкретной организации включают следующие сведения.

- **Определение векторов угроз**

  Выявление и анализ состояния критических компонентов вашей сети, доступных извне, – включая банкоматы, системы видеонаблюдения, телекоммуникационное оборудование и другие виды систем, а также профили сотрудников в социальных сетях и личные учетные записи электронной почты. Любой из этих компонентов может стать целью для атаки.

- **Анализ отслеживания вредоносных программ и кибератак**

  Выявление, мониторинг и анализ любых активных и неактивных образцов вредоносных программ, нацеленных на вашу организацию, текущей и зафиксированной ранее активности ботнетов, а также любой другой подозрительной сетевой активности.

- **Атаки на третьи стороны**

  Выявление признаков угроз и активности ботнетов, направленных на ваших клиентов, партнеров и абонентов. Их зараженные системы могут стать источником последующей атаки на вашу организацию.

- **Утечка информации**

  Ведя скрытое наблюдение за подпольными интернет-форумами и сообществами, эксперты «Лаборатории Касперского» могут обнаружить планы атаки на вашу компанию, если злоумышленники обсуждают их, а также выявить нечистоплотных сотрудников, торгующих ценной информацией.

- **Текущая подверженность атакам**

  APT-угрозы могут оставаться незамеченными в течение многих лет. Если мы обнаружим, что вашу инфраструктуру уже атакуют, эксперты «Лаборатории Касперского» предоставят рекомендации по эффективному реагированию на атаку.

# Уведомления об угрозах для конкретной организации

Kaspersky Threat Intelligence Portal уведомляет о новых уязвимостях и отчетах экспертов «Лаборатории Касперского» посредством веб-интерфейса и электронной почты.

**Уведомления в веб-интерфейсе**

При появлении новой уязвимости или отчета Kaspersky Threat Intelligence Portal отображает метку с указанием общего количества обновлений рядом с пунктом **Digital Footprint** в главном меню. На странице **Digital Footprint** количество новых уязвимостей и отчетов отображается отдельно на соответствующих закладках. Уведомление отображается для уязвимостей или отчетов, которые появились с момента последнего посещения страницы **Digital Footprint**.

**Уведомления по электронной почте**

Kaspersky Threat Intelligence Portal позволяет настроить уведомления по электронной почте.

Kaspersky Threat Intelligence Portal позволяет выполнять следующие действия:

- поиск определенного уведомления об угрозах;
- экспорт уведомлений об угрозах;
- просмотр и изменение сведений об организации, которые используются экспертами «Лаборатории Касперского» для исследований.

# Потоки данных о киберугрозах

## О потоках данных о киберугрозах

Раздел **Threat Data Feeds** страницы **Data Feeds** содержит список ссылок и источников данных, которые можно использовать для загрузки потоков данных об угрозах (полной или демонстрационной версии, в соответствии с лицензией).

- **Malicious URL Feed** – набор масок веб-адресов с контекстными данными, охватывающий вредоносные веб-сайты и веб-страницы.
- **Phishing URL Feed** – набор масок веб-адресов с контекстными данными, охватывающий фишинговые веб-сайты и веб-страницы.
- **Botnet C&C URL Feed** – набор масок веб-адресов с контекстными данными, охватывающий командные серверы ботнетов для настольных компьютеров и связанные с ними вредоносные объекты.
- **Malicious Hash Feed** – набор файловых хешей с контекстными данными, охватывающий наиболее опасные и распространенные, а также самые новые вредоносные программы. **Mobile Malicious Hash Feed** – набор файловых хешей с контекстными данными для обнаружения вредоносных объектов, заражающих мобильные платформы Android™ и iPhone®.
- **P-SMS Trojan Feed** – набор хешей троянцев с контекстной информацией для обнаружения SMS-троянцев, которые звонят с мобильных телефонов на платные номера, а также позволяют злоумышленнику перехватывать SMS-сообщения, отвечать на них и удалять их.
- **Mobile Botnet Feed** – набор веб-адресов с контекстными данными, охватывающий командные серверы ботнетов для мобильных устройств.

**IP Reputation Feed** – набор IP-адресов с контекстной информацией, охватывающий вредоносные узлы.

- **Ransomware URL Feed** – набор веб-адресов, доменов и узлов, охватывающий ссылки и вебсайты программ-вымогателей.
- **APT URL Feed** – набор доменов, которые входят в инфраструктуру, используемую во вредоносных APT-кампаниях. Этот поток данных основан на мастер-файлах IOC/YARA, которые доступны в аналитических отчетах об APT-угрозах. Мастер-файлы IOC/YARA обычно обновляются один или два раза в день. Потоки данных обновляются каждый час на случай появления новых данных в мастер-файлах IOC/YARA.
- **APT IP Feed** – набор IP-адресов, которые входят в инфраструктуру, используемую во вредоносных APT-кампаниях. Этот поток данных основан на мастер-файлах IOC/YARA, которые доступны в аналитических отчетах об APT-угрозах. Мастер-файлы IOC/YARA обычно обновляются один или два раза в день. Потоки данных обновляются каждый час на случай появления новых данных в мастер-файлах IOC/YARA.
- **APT Hash Feed** – набор хешей, охватывающий вредоносные артефакты, используемые APTкиберпреступниками для проведения APT-кампаний. Этот поток данных основан на мастерфайлах IOC/YARA, которые доступны в аналитических отчетах об APT-угрозах. Мастерфайлы IOC/YARA обычно обновляются один или два раза в день. Потоки данных обновляются каждый час на случай появления новых данных в мастер-файлах IOC/YARA. **APT YARA Feed** – набор правил YARA для обнаружения и поиска семейств вредоносного ПО, используемых APT-киберпреступниками. Этот поток данных основан на мастер-файлах IOC/YARA, которые доступны в аналитических отчетах об APT-угрозах. Мастер-файлы IOC/YARA обычно обновляются один или два раза в день. Потоки данных обновляются каждый час на случай появления новых данных в мастер-файлах IOC/YARA.
- **Malicious URL Exact Feed** – этот поток данных имеет такую же структуру JSON, как и поток данных Malicious URL Feed, но также включает до трех дополнительных полей для указания точных веб-адресов и полных доменных имен, охватываемых соответствующими масками. Этот поток данных предназначен для интеграции в средства управления защитой (такие как SIEM-системы, сетевые экраны, интернет-шлюзы SWG) или платформы аналитики угроз, когда использование Потоков данных об угрозах «Лаборатории Касперского» недопустимо или невозможно.
- **Phishing URL Exact Feed** – этот поток данных имеет такую же структуру JSON, как и поток данных Phishing URL Feed, но также включает до трех дополнительных полей для указания точных веб-адресов и полных доменных имен, охватываемых соответствующими масками. Этот поток данных предназначен для интеграции в средства управления защитой (такие как SIEM-системы, сетевые экраны, интернет-шлюзы SWG) или платформы аналитики угроз, когда использование потоков данных об угрозах «Лаборатории Касперского» недопустимо или невозможно.
- **Botnet C&C URL Exact Feed** – этот поток данных имеет такую же структуру JSON, как и поток данных Botnet C&C URL Feed, но также включает до трех дополнительных полей для указания точных веб-адресов и полных доменных имен, охватываемых соответствующими масками. Этот поток данных предназначен для интеграции в средства управления защитой (такие как SIEM-системы, сетевые экраны, интернет-шлюзы SWG) или платформы аналитики угроз,

- когда использование потоков данных об угрозах «Лаборатории Касперского» недопустимо или невозможно.

- **IoT URL Data Feed** – набор веб-адресов с контекстными данными, охватывающий веб-сайты, которые использовались для размещения вредоносного ПО, заражающего устройства интернета вещей (IoT). Также предоставляются данные о хешах вредоносного ПО.
- **Vulnerability Data Feed** – перечень уязвимостей с сопутствующими аналитическими данными о киберугрозах (такими как хеши уязвимых приложений/эксплойтов, метки времени, уязвимости CVE, исправления).

- **pDNS Data Feed** – набор записей с практическими контекстными рекомендациями, содержащий результаты разрешений имен DNS для доменов в соответствующие IP-адреса. Этот поток данных создается каждый час и включает только записи, обнаруженные в ответах DNS за этот час.

- **ICS Hashes Feed** – набор файловых хешей с контекстными данными, охватывающий наиболее опасные и распространенные, а также самые новые вредоносные программы, которые угрожают устройствам, используемым в АСУ ТП.

# Сопутствующие материалы

Раздел **Related materials** страницы **Data Feeds** содержит список дополнительных документов, связанных с потоками данных.

- **Evaluation Kit** — набор данных, который позволяет проверить корректность интеграции потоков данных об угрозах в решение. Пароль для распаковки архива – *infected*.

- **Implementation Guide** — подробное описание потоков данных об угрозах и схем их доставки.

- **Threat Data Feeds Leaflet** — подробное описание потоков данных об угрозах и схем их доставки.

- **Threat Data Feeds Presentation** — презентация, описывающая потоки данных об угрозах и схемы их доставки.

# Инструменты для реагирования на инциденты

Раздел **Incident Response Tools** страницы **Tools** содержит список инструментов, разработанных «Лабораторией Касперского» и другими компаниями, которые могут помочь защитить компьютеры.

- **Incident Response Guide** (доступно на английском и русском языках) — руководство Incident Response Guide «Лаборатории Касперского» содержит основные пояснения и рекомендации по реагированию на инциденты информационной безопасности.

- **Kaspersky Virus Removal Tool** — инструмент, который помогает очистить зараженный компьютер.
- **Kaspersky Rescue Disk** — инструмент, который помогает очистить зараженный компьютер в случае невозможности загрузки операционной системы.

**Other free tools** — бесплатные утилиты для уничтожения различных типов вредоносного ПО.

# Дополнительные инструменты

В разделе **Supplementary Tools** страницы **Tools** представлен список утилит для работы с загружаемыми потоками данных об угрозах.

- **Kaspersky Feed Utility** — многофункциональное высокопроизводительное средство, которое позволяет производить загрузку, преобразование и фильтрацию потоков данных об угрозах, предоставляемых «Лабораторией Касперского», в соответствии с заданным набором правил. Например, этот инструмент позволяет преобразовывать потоки данных об угрозах в форматы STIX, OpenIOC, CSV, простого текста, PCRE, разбивать их на несколько файлов, создавать файлы различий и выполнять множество других действий.
- **Kaspersky Data Feed Downloader** — скрипт Python для упрощения загрузки потоков данных об угрозах на основе HTTPS.
- **Kaspersky CyberTrace for Log Scanner** — позволяет моментально проверять веб-адреса, IPадреса и хеши файлов с использованием потоков данных об угрозах для выявления индикаторов вредоносного ПО и получения контекстной информации. Этот инструмент также позволяет сканировать журналы любых форматов, которые включают текстовые строки с вебадресами, IP-адресами и (или) хешами.
- **Kaspersky Transforms for Maltego** — элемент концентратора трансформов Maltego. Предоставляет пользователям Maltego набор трансформов, которые обеспечивают доступ к потокам данных об угрозах «Лаборатории Касперского». Kaspersky Transforms for Maltego позволяет сверять веб-адреса, хеши и IP-адреса с потоками данных об угрозах, предоставляемыми «Лабораторией Касперского». Также с помощью этого инструмента можно визуализировать взаимосвязи между индикаторами угроз. Трансформы помогают определить категорию объекта и предоставляют соответствующие практические контекстные рекомендации.

# SIEM-коннекторы

В разделе **SIEM Connectors** страницы **Tools** представлен список коннекторов для подключения к SIEM-системам, которые предназначены для работы с загружаемыми потоками данных об угрозах. Связанную документацию можно найти в соответствующем архиве дистрибутива. Для средства Connector for IBM® QRadar® доступна встроенная справка.

- **CyberTrace for ArcSight** — набор приложений, который позволяет проверять веб-адреса, хеши файлов и IP-адреса, которые содержатся в событиях, поступающих в SIEM-системы. Веб-адреса, хеши файлов и IP-адреса сверяются с потоками данных, предоставляемыми «Лабораторией Касперского». Категории этих объектов определяются в процессе сопоставления.
- **Kaspersky Threat Feed App for ArcSight ESM** (без CyberTrace) — приложение, которое позволяет сопоставлять результаты из событий, получаемых ArcSight ESM, с потоками данных об угрозах «Лаборатории Касперского», с использованием встроенных возможностей SIEM (без CyberTrace).
- **CyberTrace for Splunk** — приложение Splunk® и сопутствующие служебные модули. Оно сопоставляет веб-адреса, IP-адреса и хеши файлов из событий Splunk с потоками данных, предоставляемыми «Лабораторией Касперского».
- **Threat Feed App for Splunk** (без CyberTrace) — обеспечивает клиенту преимущество в киберпространстве благодаря усилению экземпляра Splunk с помощью постоянно обновляемых индикаторов компрометации и практических контекстных рекомендаций, позволяющих лучше понимать намерения, возможности и цели злоумышленников.
- **CyberTrace for QRadar** — набор приложений, который позволяет проверять веб-адреса, хеши файлов и IP-адреса, которые содержатся в событиях, поступающих в SIEM-системы. Вебадреса, хеши файлов и IP-адреса сверяются с потоками данных, предоставляемыми «Лабораторией Касперского». Категории этих объектов определяются в процессе сопоставления.
- **Connector for IBM QRadar** (без потоков данных) — приложение, которое добавляет в наборы справочников QRadar индикаторы (IP-адреса) из нашего потока IP Reputation Data Feed.
- **CyberTrace for RSA NetWitness** — набор приложений, который позволяет проверять вебадреса, хеши файлов и IP-адреса, которые содержатся в событиях, поступающих в RSA NetWitness. Веб-адреса, хеши файлов и IP-адреса сверяются с потоками данных об угрозах, предоставляемыми «Лабораторией Касперского». Категории этих объектов определяются в процессе сопоставления.
- **Threat Feed App for RSA NetWitness** (без CyberTrace) — приложение, которое позволяет сопоставлять результаты из событий, получаемых RSA NetWitness, с потоками данных об угрозах «Лаборатории Касперского», с использованием встроенных возможностей SIEM (без CyberTrace).
- **CyberTrace for LogRhythm** — набор приложений, который позволяет проверять веб-адреса, хеши файлов и IP-адреса, которые содержатся в событиях, поступающих в LogRhythm. Вебадреса, хеши файлов и IP-адреса сверяются с потоками данных об угрозах, предоставляемыми «Лабораторией Касперского». Категории этих объектов определяются в процессе сопоставления.
- **Connector for McAfee ESM** — загружает, фильтрует и преобразовывает потоки данных об угрозах «Лаборатории Касперского» в формат STIX, который может использоваться McAfee® ESM.

- **Connector for McAfee TIE** — приложение на Python, которое загружает потоки данных «Лаборатории Касперского» и добавляет содержащиеся в них записи в McAfee Threat Intelligence Exchange.
- **Connector for ELK** — набор приложений, который позволяет сверять индикаторы, содержащиеся в событиях, поступающих в Logstash, с потоками данных об угрозах «Лаборатории Касперского».
- **Connect for MISP** — утилита, импортирующая потоки данных об угрозах «Лаборатории Касперского» в экземпляр Malware Information Sharing Platform (MISP).
- **CyberTrace for AlienVault USM/OSSIM** — рекомендации по интеграции потоков данных об угрозах «Лаборатории Касперского» с AlienVault USM, а также с AlienVault OSSIM через CyberTrace.

  **Kaspersky CyberTrace for FortiSIEM** — рекомендации по интеграции потоков данных об угрозах «Лаборатории Касперского» с FortiSIEM через CyberTrace.
- **Data Feeds for Cisco Firepower** — приложение предназначено для загрузки потоков данных об угрозах «Лаборатории Касперского» и их импорта в Cisco®/™ Firepower Management Center с использованием модуля Cisco Threat Intelligence Director. С помощью этого модуля пользователи Cisco Firepower Management Center могут использовать индикаторы, содержащиеся в потоках данных об угрозах «Лаборатории Касперского», как запрещенные списки в поставляемых Cisco решениях Next-Generation Firewall и Next-Generation Intrusion Prevention System.
- **JSON to Suricata Feeds Converter** — инструмент, который позволяет преобразовывать потоки данных об угрозах «Лаборатории Касперского» в правила Suricata (IDS). Этот инструмент представляет собой утилиту на Python, которая загружает потоки данных об угрозах «Лаборатории Касперского» и преобразовывает их в правила Suricata (IDS).
- **Threat Intelligence Portal for IBM Resilient** — приложение, которое обеспечивает самый быстрый и простой способ получения аналитических данных об угрозах из Kaspersky Threat Intelligence Portal для артефактов в инцидентах, сохраненных в IBM Resilient.
- **Threat Intelligence Portal for Splunk Phantom** — приложение, которое позволяет пользователям Phantom SOAR получать доступ к аналитическим данным об угрозах в Kaspersky Threat Intelligence Portal и к отчетам об APT-угрозах из пользовательского интерфейса Phantom или в виде шагов в Phantom Playbooks.

# Управление учетными записями

Администраторы могут управлять учетными записями сотрудников и просматривать настройки учетных записей пользователей.

Поддерживается два типа учетных записей: *Администратор* и *Пользователь*.

С помощью Kaspersky Threat Intelligence Portal администраторы могут выполнять следующие действия:

- просматривать список всех учетных записей;
- просматривать сведения о конкретной учетной записи;
- добавлять новые учетные записи;
- изменять настройки учетных записей;
- просматривать историю учетной записи;  удалять учетные записи.

Страница **Accounts** доступна только для пользователей Kaspersky Threat Intelligence Portal с правами администратора группы.

# Другие возможности

Kaspersky Threat Intelligence Portal позволяет выполнять следующие действия:

- Настраивать уведомления, отправляемые Kaspersky Threat Intelligence Portal по электронной почте при возникновении определенных событий. Список событий для уведомлений зависит от приобретенных организацией лицензий и типа учетной записи.
- Изменять пароль для Kaspersky Threat Intelligence Portal.
- Отправлять команде Kaspersky Threat Intelligence Portal комментарии и предложения о предоставляемых возможностях и работе веб-сайта.
- Запрашивать поддержку, если нужна дополнительная информация о возможностях Kaspersky Threat Intelligence Portal, требуется приобрести лицензию на решения или подать заявку на дополнительные форматы аналитических отчетов об APT-угрозах или аналитических отчетов об угрозах в финансовой индустрии, доступных для загрузки.
- Запрашивать демонстрацию возможностей Kaspersky Threat Intelligence Portal.

# Работа с Kaspersky Threat

# Intelligence Portal API

Kaspersky Threat Intelligence Portal предоставляет API для следующих решений:

- Аналитические отчеты об APT-угрозах.
- Профили группировок.
- Аналитические отчеты об угрозах в финансовой индустрии.
- Служба отслеживания APT C&C.
- Аналитические отчеты об угрозах промышленной кибербезопасности.
- Поиск угроз (Threat Lookup).
- Cloud Sandbox.
- Аналитические отчеты об угрозах для конкретной организации (Digital Footprint Intelligence)

# Ограничения и предупреждения

В Kaspersky Threat Intelligence Portal имеется несколько ограничений.

**Ограничение при использовании Просмотра в режиме совместимости в Microsoft Internet Explorer**

При работе с Kaspersky Threat Intelligence Portal нельзя использовать Просмотр в режиме совместимости в Microsoft Internet Explorer.

**Некорректная печать PDF в Microsoft Internet Explorer 11**

Справка в формате PDF может печататься некорректно, если в Microsoft Internet Explorer 11 выбран параметр **Печатать все**.

# Обращение в службу технической поддержки

Если вам не удалось найти решение проблемы в справке, рекомендуем связаться с вашим персональным менеджером «Лаборатории Касперского» по техническим вопросам, позвонив по телефону +7-495-780-3367 с 8:00 до 17:00 UTC+03:00 или написав по адресу ktlsupport@kaspersky.com.

# Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt.

# Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

iPhone, Safari – товарные знаки Apple Inc., зарегистрированные в США и других странах.

Cisco – зарегистрированный товарный знак или товарный знак компании Cisco Systems, Inc. и (или) ее дочерних компаний в США и некоторых других странах.

Google, Android, Chrome – товарные знаки Google, Inc.

Intel, Pentium – товарные знаки Intel Corporation, зарегистрированные в США и (или) других странах.

IBM, QRadar – товарные знаки корпорации International Business Machines, зарегистрированные во многих странах мира.

McAfee – товарный знак или зарегистрированный товарный знак McAfee, Inc. в США и других странах.

Microsoft, Internet Explorer – зарегистрированные товарные знаки корпорации Microsoft в США и других странах.

Mozilla, Firefox – товарные знаки Mozilla Foundation.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

RSA NetWitness – собственность RSA Security LLC и других сторон.

Splunk – товарный знак и зарегистрированный товарный знак Splunk Inc. в США и других странах.