Тактические, операционные
и стратегические данные
об угрозах

Kaspersky Threat Intelligence

kaspersky активируй будущее

Kaspersky Threat Intelligence

Бесплатная версия Kaspersky OpenTIP

Позволяет проанализировать каждый файл на содержание в нем вредоносного кода и отображает информацию о репутации этого файла.

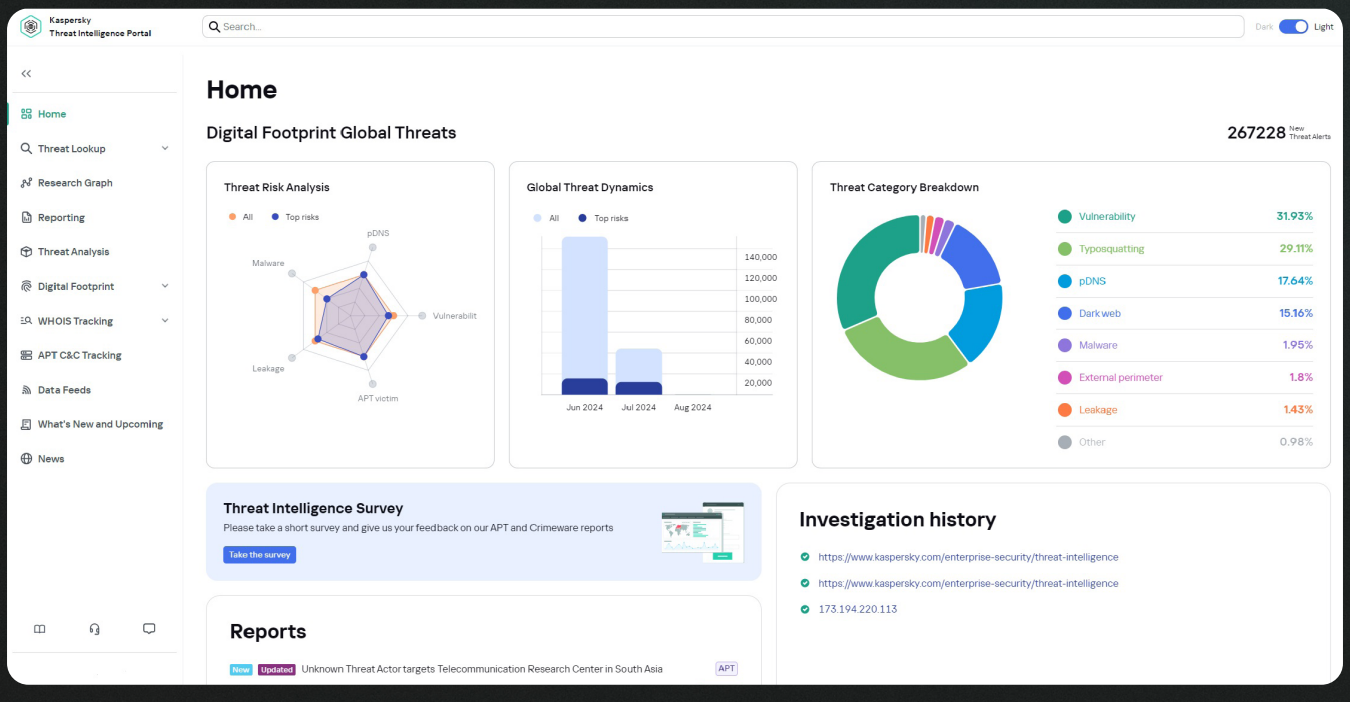
Подробнее

Kaspersky Threat Intelligence

Комплекс продуктов и сервисов информирования об угрозах, обеспечивающий проактивный подход к кибербезопасности ипомогающий обогатить имеющуюся систему защиты актуальными тактическими, операционными и стратегическими данными, необходимыми для борьбы с целевыми и сложными атаками.

Комплекс основан на данных кибербразведки, полученных аналитиками и экспертами Kaspersky Cyber Threat Intelligence, которые анализируют и изучают данные о различных атаках по всему миру и извлекают из них большое количество полезной информации, в том числе тактики, техники и процедуры атакующих (TTPs) злоумышленников.

Благодаря единой точке доступа — Kaspersky Threat Intelligence Portal, сервисы работают взаимосвязанно, обогащая и усиливая друг друга. Портал объединяет экспертизу и все знания «Лаборатории Касперского» о киберугрозах в одном месте,обеспечивает мониторинг угроз, релевантных для конкретной организации, с использованием собственных технологий обработки и нормализации данных, а так же предоставляет возможность исследования образцов вредоносного ПО с их последующей атрибуцией.



Портфолио Kaspersky Threat Intelligence

Kaspersky Threat Intelligence обеспечивает комплексное представление о глобальном ландшафте угроз. Синергия достоверных источников данных об угрозах и непрерывных исследований экспертов «Лаборатории Касперского» помогают организациям защищаться от киберугроз по всему миру.

Виды данных об угрозах

Аналитические данные о киберугрозах делят на три категории: тактические, операционные и стратегические. В зависимости от категории, они могут помогать в расследовании текущей атаки, предотвращении новых, или учитываться при принятии решений руководством высшего звена.

Тактический

Низкоуровневая, быстро устаревающая информация, которая поддерживает операции по обеспечению безопасности и реагированию на инциденты. Примером тактической разведки являются IOC, связанные с проведением недавно обнаруженной атаки.

Лица:
- SOC Analyst

Системы:
- SIEM
- NGFW
- IPS
- IDS
- SOAR

Процессы:
- Threat Hunting
- Monitoring

Операционный

Этот уровень обычно включает данные о кампаниях и TTPs более высокого порядка. Может включать информацию об атрибуции конкретных субъектов, а также о возможностях и намерениях противников.

Лица:
- SOC L3 Analyst
- DFIR Analyst
- IR Analyst

Системы:
- SIEM
- NTA
- EDR/XDR
- TIP

Процессы:
- Incident Response
- Threat Hunting

Стратегический

Этот уровень оказывает поддержку руководителям высшего звена в принятии серьезных решений по оценке рисков, распределению ресурсов и стратегии организации. Эта информация включает в себя тенденции, мотивацию действующих лиц и их классификацию.

Лица:
- CISO
- CTO
- CIO
- CEO

Процессы:
- Выстраивание стратегии ИБ
- Повышение осведомлённости

Преимущества

Проактивное выявление и предотвращение угроз

Kaspersky Threat Intelligence помогает организациям быть в курсе последних угроз и уязвимостей и принимать проактивные меры для защиты своих систем до того, как произойдет атака.

Повышение эффективности обнаружения и реагирования

С помощью Kaspersky Threat Intelligence организации могут дополнить свои существующие решения по обеспечению безопасности аналитикой угроз, улучшая свои процессы обнаружения и реагирования.

Представление о цифровых активах и рисках

Kaspersky Threat Intelligence предоставляет организациям всестороннее представление об их собственном цифровом отпечатке, подсвечивая активы, которые могут быть потенциально уязвимы для атак или компрометации.

Улучшение реагирования на инциденты

Kaspersky Threat Intelligence предоставляет организациям информацию о возникающих угрозах и индикаторах компрометации в режиме реального времени, что позволяет им быстро и эффективно реагировать на инциденты.

Соответствие требованиям регуляторов

Многие отрасли подчиняются правилам и стандартам, которые требуют принятия надежных мер кибербезопасности. Kaspersky Threat Intelligence помогает организациям выполнить эти требования.

Расширение возможностей вашей ИБ команды

В команду экспертов «Лаборатории Касперского» входят одни из самых опытных и экспертных исследователей в отрасли, которые привносят свои знания и опыт в анализ Kaspersky Threat Intelligence.

Kaspersky Threat Data Feeds

Подробнее

Kaspersky Threat Data Feeds

Потоки данных об угрозах

Кибератаки происходят каждый день. Попытки взломать защиту предпринимаются все чаще, при этом сложность и скрытность киберугроз растет. Для кампаний, направленных на нарушение ваших бизнес-процессов и нанесение ущерба вашим клиентам, злоумышленники используют многоступенчатые атаки, а также специально подобранные техники, тактики и процедуры. В этой ситуации необходимы новые методы защиты, основанные на анализе угроз.

Благодаря интеграции потоков данных об угрозах, содержащих подозрительные и вредоносные IP-адреса, веб-адреса и хеши файлов, с существующими системами безопасности, такими как SIEM, SOAR, и платформами Threat Intelligence, службы информационной безопасности могут автоматизировать процесс приоритизации оповещений об угрозах. При этом специалисты по сортировке таких оповещений получают достаточно контекста, чтобы сразу выявлять события, требующие более пристального изучения или эскалации группам реагирования на инциденты для детального расследования.

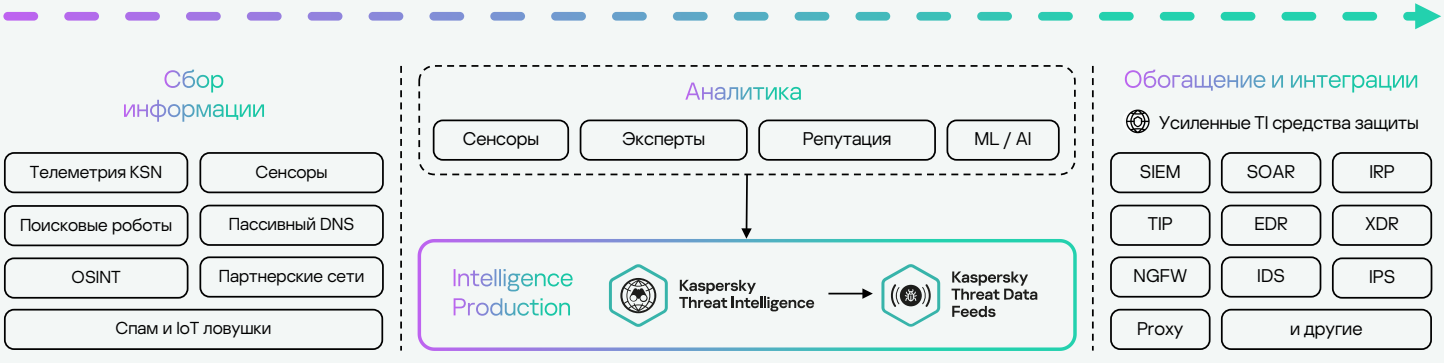
Потоки данных об угрозах — это сервис «Лаборатории Касперского», предоставляющий компаниям информацию об угрозах для защиты их инфраструктуры. В рамках данного сервиса предоставляется информация об известных вредоносных программах, фишинговых веб-сайтах, последних уязвимостях и эксплойтах, а также других типах киберугроз. Эта информация может использоваться организациями для блокировки вредоносного трафика, обновления своих средств обеспечения безопасности и принятия других мер защиты от кибератак.

Контекстные данные

Каждая запись в каждом потоке содержит контекстные данные, позволяющие быстро подтвердить и приоритезировать угрозы:

- Имена угроз
- Тактики, техники и процедуры атак в соответствии с классификацией MITRE ATT&CK
- Метки времени
- Идентификаторы уязвимых и скомпрометированных объектов
- Географическое положение
- Установленные IP-адреса и доменные имена вредоносных веб-ресурсов
- Популярность и прочее
- Хеши вредоносных файлов

Схема работы



Принцип работы

Потоки данных пополняются из множества источников:

Kaspersky Security Network

Сложная облачная инфраструктура, собирающая и анализирующая анонимные данные о киберугрозах от миллионов добровольных участников по всему миру, чтобы обеспечить самую быструю реакцию на новые угрозы за счет использования анализа больших данных, машинного обучения и человеческого опыта.

Веб-краулеры

Собирают новые образцы вредоносных и легитимных программ из самых разных источников: OSINT, исследований аналитиков «Лаборатории Касперского», а также из наших собственных систем автоматической обработки и анализа, которые извлекают URL-адреса из вредоносного ПО.

БотоФермы

Специальная команда исследователей ботнетов извлекает конфигурации ботов, занимается реинжинирингом их коммуникационных протоколов и отслеживает команды из командных центров с целью получить ценные для разведки угроз данные.

Спам-ловушки

Каждый год наши антифишинговые системы предотвращают около 507 миллионов переходов по фишинговым ссылкам, а также около 166 миллионов вредоносных почтовых вложений, из которых мы извлекаем дополнительные данные для обогащения наших потоков данных.

Сенсоры

Ханипоты, «воронки» (sinkholes) и другие методы перехвата ITW-атак (в том числе ханипоты, имитирующие IoT-устройства, уязвимые системы, программное обеспечение и т.д.) Аналитики «Лаборатории Касперского» изучают попытки атак и действия злоумышленников, извлекают индикаторы компрометации и связывают их с другими источниками данных.

OSINT

Данные о противниках автоматически собираются из общедоступных источников, таких как новостные каналы, социальные сети, публичные отчеты, dark web и т.д. Эти данные мы используем для поиска новых вредоносных образцов, изучающих инфраструктуру противника, непрерывно пополняя нашу базу знаний.

Пассивные DNS (Passive DNS)

Данные собираются по всему миру от доверенных третьих лиц, таких как хостинговые организации и интернет-провайдеры.

Партнеры

В рамках партнерской программы мы обмениваемся вредоносными образцами с другими поставщиками и организациями сферы кибербезопасности.

Каждый полученный индикатор проходит многоступенчатый отбор в системе автоматической обработки, где для отсечения ложных срабатываний применяются технологии проверки доверия и репутации и модели машинного обучения, тренируемые на выборках из сотен миллионов актуальных доверенных и вредоносных файлов. Также каждый индикатор проходит анализ во множестве песочниц, из которых извлекаются десятки дополнительных атрибутов, таких как TTPs, сетевое поведение, поведение в операционной системе, и множество других связей.

Всё это превращает потоки данных «Лаборатории Касперского» в мощнейший источник разведданных тактического уровня, который позволяет усилить ваши центры мониторинга угроз и обнаружить противника на первых подступах к вашей организации.

Преимущества

Предотвращение утечек конфиденциальных данных и интеллектуальной собственности

с зараженных машин за пределы организации. Быстрое обнаружение зараженных активов для защиты репутации бренда и сохранения конкурентного преимущества.

Повышение эффективности реагирования и форензики

с помощью автоматизации процессов приоритезации инцидентов и предоставления вашим аналитикам достаточного контекста для немедленного выявления угроз и последующего расследования первопричин.

Усиление решений информационной безопасности

включая SIEM, межсетевые экраны, IPS/IDS, Security Proxy, решения DNS, Anti-APT, постоянно обновляемыми индикаторами компрометации (IOC) и действенным контекстом. Потоки данных об угрозах предоставляют информацию о кибератаках и помогают лучше понимать намерения, возможности и цели ваших противников. Данные можно интегрировать с ведущими системы SIEM, включая KUMA, HP ArcSight, IBM QRadar, MS Sentinel, Splunk и т.д.

Развитие бизнеса в качестве сервисного провайдера

предоставляя своим клиентам ведущую в отрасли информацию об угрозах в качестве услуги премиум-класса. Улучшайте и расширяйте свои возможности обнаружения и идентификации киберугроз в качестве центра мониторинга и реагирования.

Kaspersky CyberTrace

Подробнее

Kaspersky CyberTrace

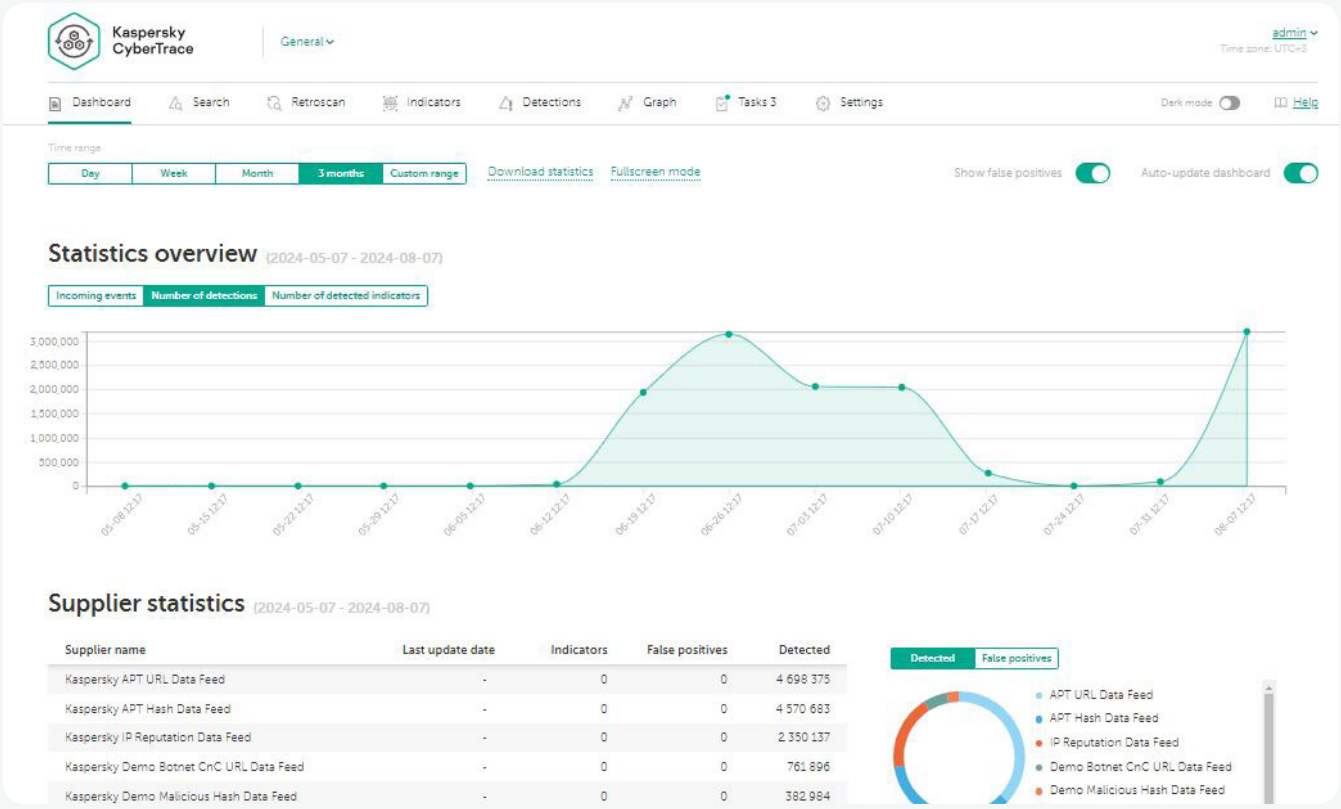
Платформа для управления данными о киберугрозах

Интеграция актуальных машиночитаемых аналитических данных об угрозах в существующие средства управления безопасностью, такие как SIEM-системы, позволяет автоматизировать процесс первоначальной приоритизации и классификации.

Аналитические данные предоставляются в различных форматах и включают большое количество индикаторов компрометации (IoCs), что сильно усложняет их обработку SIEM-системами или другими средствами управления сетевой безопасностью.

Kaspersky CyberTrace — это решение класса Threat Intelligence Platform, которое позволяет упростить интеграцию потоков данных с SIEM-системой для дальнейшего использования аналитики угроз в повседневной работе ИБ-служб. Платформа взаимодействует с любыми типами потоков аналитических данных об угрозах («Лаборатории Касперского», других поставщиков, из открытых источников или иных каналов) в форматах JSON, STIX, XML и CSV и поддерживает настроенную интеграцию со многими SIEM и источниками журналов.

Благодаря автоматическому сопоставлению журналов с потоками аналитических данных об угрозах, Kaspersky CyberTrace обеспечивает ситуационную осведомленность в реальном времени и позволяет аналитикам по безопасности принимать своевременные и взвешенные решения.



Состав

Kaspersky CyberTrace содержит набор инструментов для эффективной классификации событий ИБ и первоначального реагирования:

База данных индикаторов с полнотекстовым поиском и возможностью поиска с использованием расширенных запросов позволяет выполнять сложный поиск по всем полям индикаторов

Статистика использования потоков данных помогает выбрать наиболее ценных поставщиков аналитической информации об угрозах посредством измерения эффективности интегрированных потоков данных и построения матрицы пересечения потоков данных

Назначение тегов индикаторам компрометации упрощает управление ими. Можно создать любой тег, указать его значимость и присваивать его индикаторам компрометации вручную. Можно выполнять сортировку и фильтрацию индикаторов по тегам и их значимости

Research Graph позволяет визуально изучать хранящиеся в CyberTrace сведения и обнаружения и выявлять общие черты угроз

Функция экспорта индикаторов позволяет экспортировать наборы индикаторов и передавать данные об угрозах между экземплярами Kaspersky CyberTrace или другими платформами анализа угроз

Ретроспективная проверка позволяет анализировать объекты в ранее проверенных событиях с использованием новых поступивших данных для поиска не обнаруженных ранее угроз

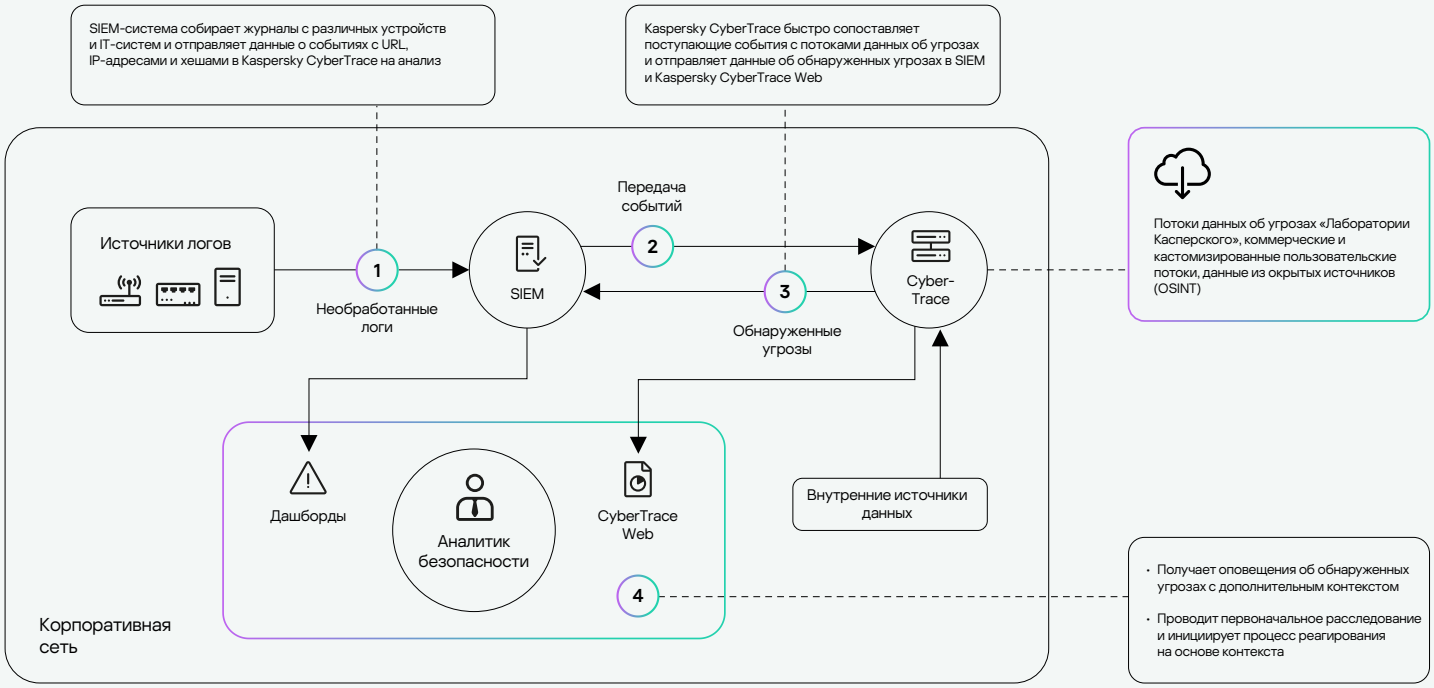
Для поставщиков управляемых услуг безопасности, а также для использования на крупных предприятиях реализована поддержка мультитенантности

Фильтрация событий обнаружения для дальнейшей отправки в SIEM-системы снижает нагрузку как на сами системы, так и на аналитиков

REST API позволяет выполнять поиск и управлять аналитическими данными об угрозах, а также интегрировать Kaspersky CyberTrace в сложные среды для автоматизации и управления

Страницы с подробной информацией о каждом индикаторе обеспечивают более глубокий анализ. Полная информация об индикаторе от всех поставщиков аналитических данных об угрозах (с исключением дублирующихся данных) позволяет аналитикам обсуждать угрозы в комментариях и добавлять внутренние данные к индикатору

Схема работы



Решение использует внутренний процесс анализа и сопоставления поступающих данных, что существенно снижает рабочую нагрузку на SIEM-систему. Kaspersky CyberTrace анализирует поступающие данные, быстро сопоставляет их с потоками и генерирует собственные оповещения при обнаружении угроз.

Преимущества

Эффективная фильтрация и приоритизация огромного количества оповещений систем безопасности

Оптимизация и ускорение процессов классификации и сдерживания угроз

Создание проактивной системы защиты на основе глобальных аналитических данных

Быстрое определение наиболее критичных из оповещений и принятие более взвешенных решений об их дальнейшей передаче группам реагирования

Kaspersky Threat Lookup

Подробнее

Kaspersky Threat Lookup

Поисковый сервис о киберугрозах и их взаимосвязях

Киберпреступность не знает границ, а ее техническая база быстро совершенствуется. Попытки взломать защиту предпринимаются все чаще, при этом сложность и скрытность киберугроз растет. Для кампаний, направленных на нарушение рабочих процессов, кражу активов и нанесение ущерба, злоумышленники используют сложные цепочки поражения, а также специально подобранные тактики, техники и процедуры.

Kaspersky Threat Lookup — это мощная единая онлайн-платформа, открывающая доступ ко всем накопленным «Лабораторией Касперского» знаниям о киберугрозах и их взаимосвязях. Сервис предоставляет специалистам по безопасности максимум информации для предотвращения кибератак до того, как организации будет нанесен вред. Сервис предоставляет самые последние данные по веб-адресам, доменам, IP-адресам, хешам файлов, названиям угроз, статистическим и поведенческим данным, данным WHOIS / DNS, атрибутам файлов, данным геолокации, цепочкам загрузки, временным меткам и прочему. Результатом является глобальная видимость новых и возникающих угроз, что помогает защитить организацию и ускоряет реагирование на инциденты.

Основные возможности

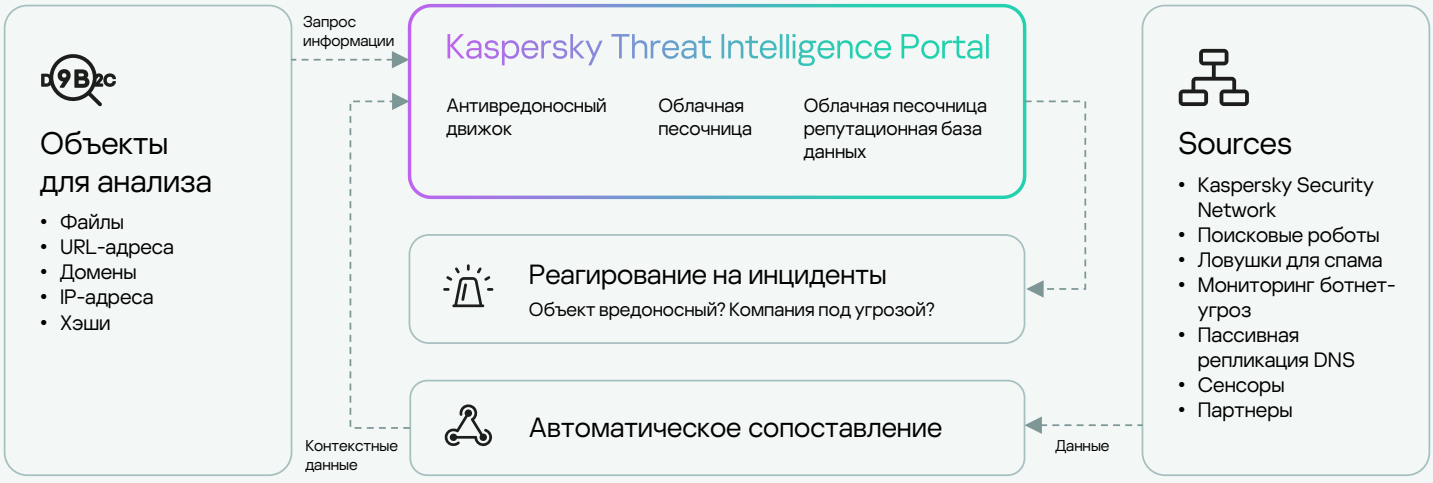
Найдет информацию об индикаторах угроз с помощью веб-интерфейса или REST API

Выяснит, является ли обнаруженный объект распространенным или уникальным

Поймет, почему объект считается вредоносным

Получит подробные сведения об объекте, включая сертификаты, распространенные названия, пути файлов и веб-адреса, для выявления новых подозрительных объектов

Схема работы



Преимущества

Надежные данные об угрозах

«Лаборатория Касперского» предоставляет надежные данные об угрозах детальной контекстной информацией. Продукты «Лаборатории Касперского» демонстрируют наилучшие результаты при тестировании решений для защиты от вредоносных программ. Непревзойденное качество аналитических данных подтверждается высоким уровнем обнаружения с минимальным уровнем ложных срабатываний.

Разнообразие форматов экспорта

Поддерживается экспорт индикаторов компрометации и контекстных данных в популярные машиночитаемые форматы, такие как STIX, OpenIOC, JSON, YARA, Snort и CSV.
Это позволяет применять данные об угрозах с максимальной пользой, автоматизируя рабочие процессы и интегрируя эти сведения в системы управления безопасностью, такие как SIEM.

Расследование инцидентов

Research Graph ускоряет расследование инцидентов, позволяя визуально изучать хранящиеся в Threat Lookup данные и обнаружения; дает графическое представление связей между вебадресами, доменами, IP- адресами, файлами и другими данными для иллюстрации полного масштаба инцидента и выявления его основной причины.

Поиск угроз

Проактивный подход к предотвращению и обнаружению атак и реагированию на них позволяет минимизировать частоту инцидентов и ущерб. Вы сможете отслеживать и устранять атаки на самых ранних этапах. Чем раньше будет обнаружена угроза, тем меньший будет нанесен ущерб и тем быстрее будет восстановлена работоспособность ресурсов и сети.

Простота использования через веб-интерфейс или REST API

Сервисом можно пользоваться в ручном режиме через веб-интерфейс (в браузере) или через REST API.

Мастер-поиск

Поиск информации с использованием всех активных сервисов анализа угроз и внешних источников (включая индикаторы компрометации из открытых источников, а также поиск в теневом и поверхностном интернете) в едином и мощном интерфейсе.

Глубокий анализ индикаторов угроз

с помощью проверенной контекстной информации позволяет приоритизировать атаки и сосредоточиться на устранении угроз, представляющих наибольший риск для бизнеса.

Эффективная и результативная диагностика

и анализ инцидентов безопасности на узлах и в сети. Приоритизация сигналов о неизвестных угрозах от внутренних систем.

Улучшение процесса реагирования на инциденты

и расширение возможностей поиска угроз, позволяющее прервать цепочку развития угрозы до момента компрометации критически важных систем и данных.

Kaspersky Threat Infrastructure Tracking

Подробнее

Kaspersky Threat Infrastructure Tracking

Сервис по отслеживанию инфраструктур кибергруппировок

Сервис Threat Infrastructure Tracking выявляет IP-адреса инфраструктур, являющихся источниками продвинутых угроз. Он помогает аналитикам безопасности, работающим в группах экстренного реагирования на инциденты (CERT), центрах мониторинга и реагирования (SOC) и агентствах национальной безопасности, отслеживать развертывание новых угроз и вредоносных кампаний, а затем принимать меры, необходимые для минимизации ущерба от текущих и предстоящих атак. Информация предоставляется как для определенной страны, так и для всех стран мира. Она ежедневно пополняется последними данными, полученными от Центра глобальных исследований и анализа угроз «Лаборатории Касперского».

Каждый IP-адрес сопровождается следующими вспомогательными данными:

Название группы угроз, операций или вредоносных программ, с которыми он связан

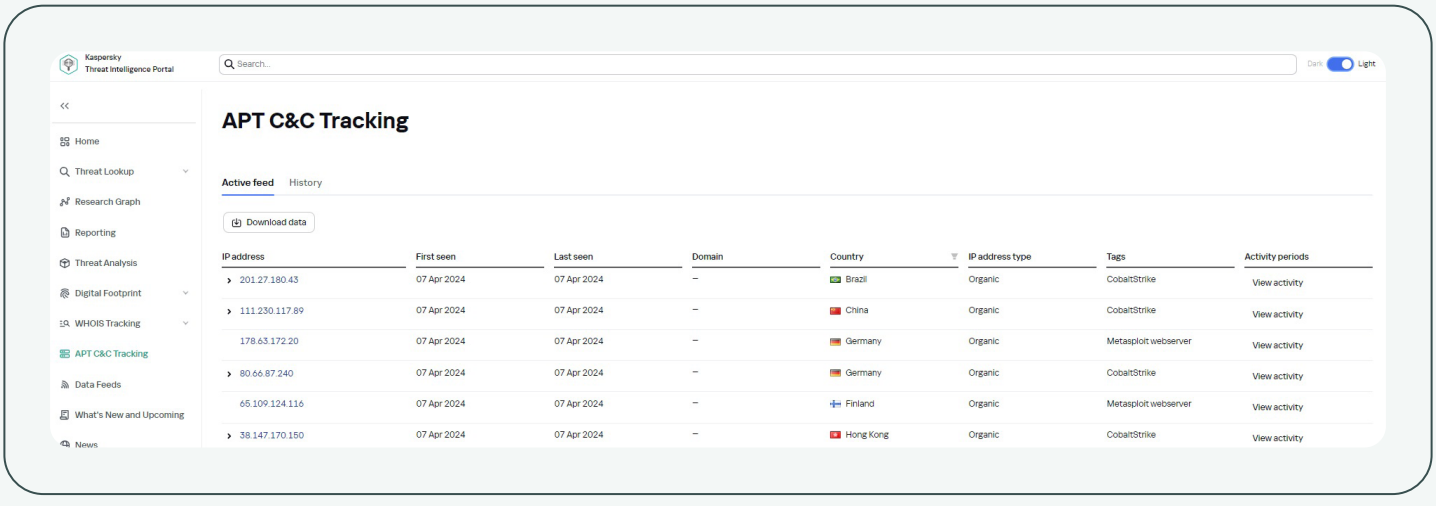
Набор связанных IP-адресов, на которых размещены данные

Информация об интернет-провайдере и автономной системе

Даты первого и последнего обращения к этому IP-адресу

Возможность экспорта

Список IP-адресов можно экспортировать в машиночитаемый формат, чтобы затем их можно было загрузить в существующие решения безопасности для автоматического обнаружения угроз.



Доступ к сервису

Сервис доступен на портале Kaspersky Threat Intelligence Portal через веб-интерфейс или RESTful API.

Компонент	Веб-интерфейс	API
Просмотр списка опасных IP-адресов	●	●
Фильтрация списка опасных IP-адресов по дате	●	
Фильтрация списка опасных IP-адресов по странам	●	●
Экспорт списка опасных IP-адресов	●	

Преимущества

Уровень безопасности

Понимание уровня безопасности в стране в соответствии с распространением таких инфраструктур

Выявление угроз

Выявление новых активных инфраструктур, используемых злоумышленниками в конкретной стране

Атрибуция

Определение, кто именно из известных злоумышленников стоит за конкретными атаками

Быстрое реагирование

Обеспечение быстрого реагирования на инциденты и проактивный поиск угроз в регионах

Kaspersky Threat Analysis

Kaspersky Threat Analysis

Подробнее

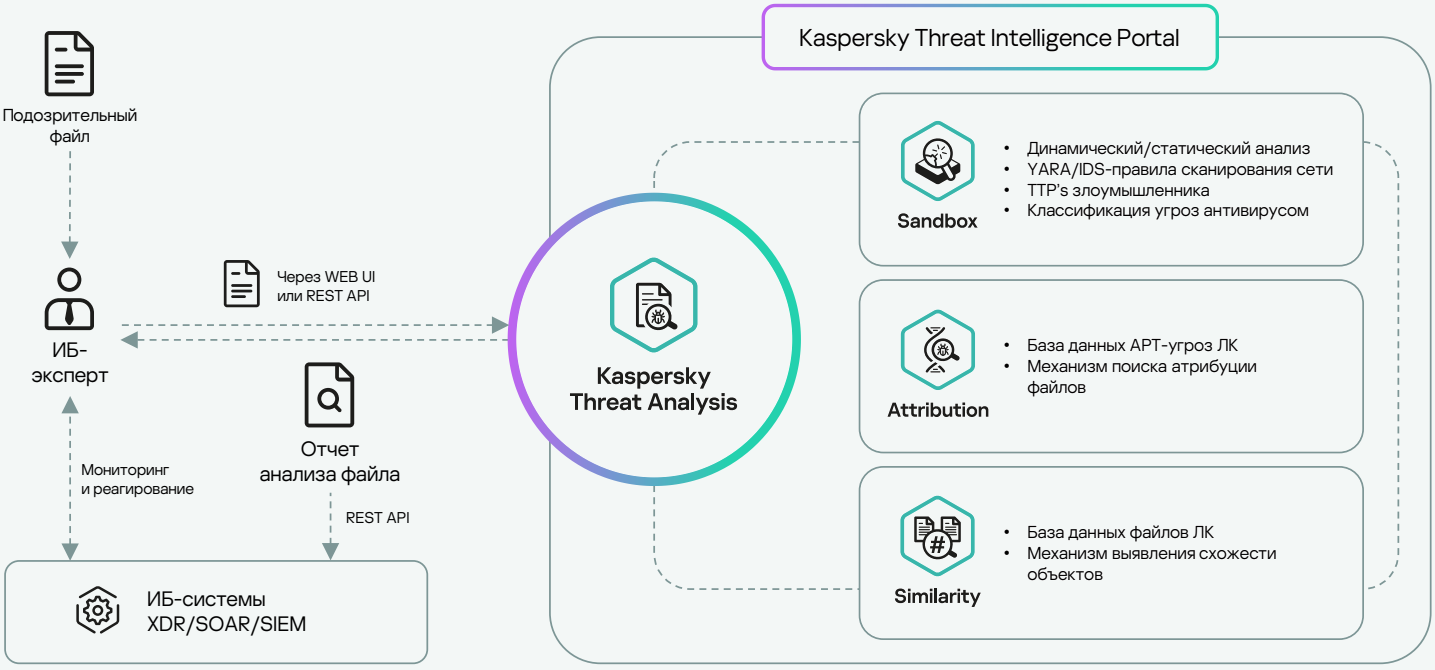
В борьбе с киберугрозами критически важно быстро и эффективно принять решение по противодействию им. Уже невозможно предотвратить современные целевые атаки только с помощью традиционного антивируса. Стандартные механизмы антивирусной защиты способны блокировать в основном известные угрозы (с минимальным поведенческим анализом), в то время как целенаправленно действующие злоумышленники используют все имеющиеся в их арсенале средства с целью избежать автоматического обнаружения. Количество ИБ-событий, ежедневно обрабатываемых SOC, растет в геометрической прогрессии. Учитывая количество ежедневно появляющихся образцов ВПО, эффективная приоритезация и своевременная работа по инцидентам без современных автоматизированных средств анализа становится практически невыполнимой задачей.

Kaspersky Threat Analysis предоставляется в виде облачного сервиса с доступом через Kaspersky Threat Intelligence Portal. Благодаря единой точке доступа, технологии работают взаимосвязанно, обогащая и усиливая друг друга.

Мощный инструмент для комплексного анализа угроз Kaspersky Threat Analysis предоставит данные для принятия обоснованных решений, эффективного сдерживания угроз и выведет процесс расследования инцидентов на новый уровень. Помимо облачной песочницы, сервис предоставляет доступ к самым современным технологиям атрибуции кибератак и выявления схожести подозрительных файлов с другими известными вредоносными объектами.

С помощью технологий, входящих в Kaspersky Threat Analysis, ваши аналитики смогут всесторонне оценить ситуацию, получить полное представление о ландшафте угроз и принять эффективные и своевременные меры реагирования.

Схема работы Kaspersky Threat Analysis



Kaspersky Threat Analysis

Sandbox

Мощный инструмент динамического анализа, позволяющий исследовать исходные образцы файлов, находить индикаторы компрометации на основании поведенческого анализа и обнаруживать вредоносные объекты, которые не встречались ранее.

Sandbox

Песочница «Лаборатории Касперского» объединяет все знания о поведении вредоносного ПО, полученные более чем за 25 лет непрерывного исследования угроз, что позволяет обнаруживать более 420 000 новых вредоносных объектов каждый день. Sandbox сочетает в себе поведенческий анализ, надежные техники предотвращения уклонения от анализа и технологии моделирования поведения человека.

Какую проблему решает?

Подозрительные файлы, не обнаруженные антивирусными средствами, могут проявить свое вредоносное поведение только в процессе выполнения. Sandbox позволяет воспроизвести поведение файла и выявить любую потенциально опасную активность.

Особенности продукта

Автоматизированный анализ объектов в средах Windows, Linux и Android

Поддержка анализа более 200 типов файлов с подробными аналитическими отчетами

Более 1000 правил классификации вредоносного поведения файла по тактикам и техникам MITRE ATT&CK

Защита от уклонения вредоносных файлов от анализа и передовые технологии эмуляции активности пользователей

Определение рейтинга угроз и уровня опасности анализируемого объекта по метрикам и данным, полученным в результате исполнения файла

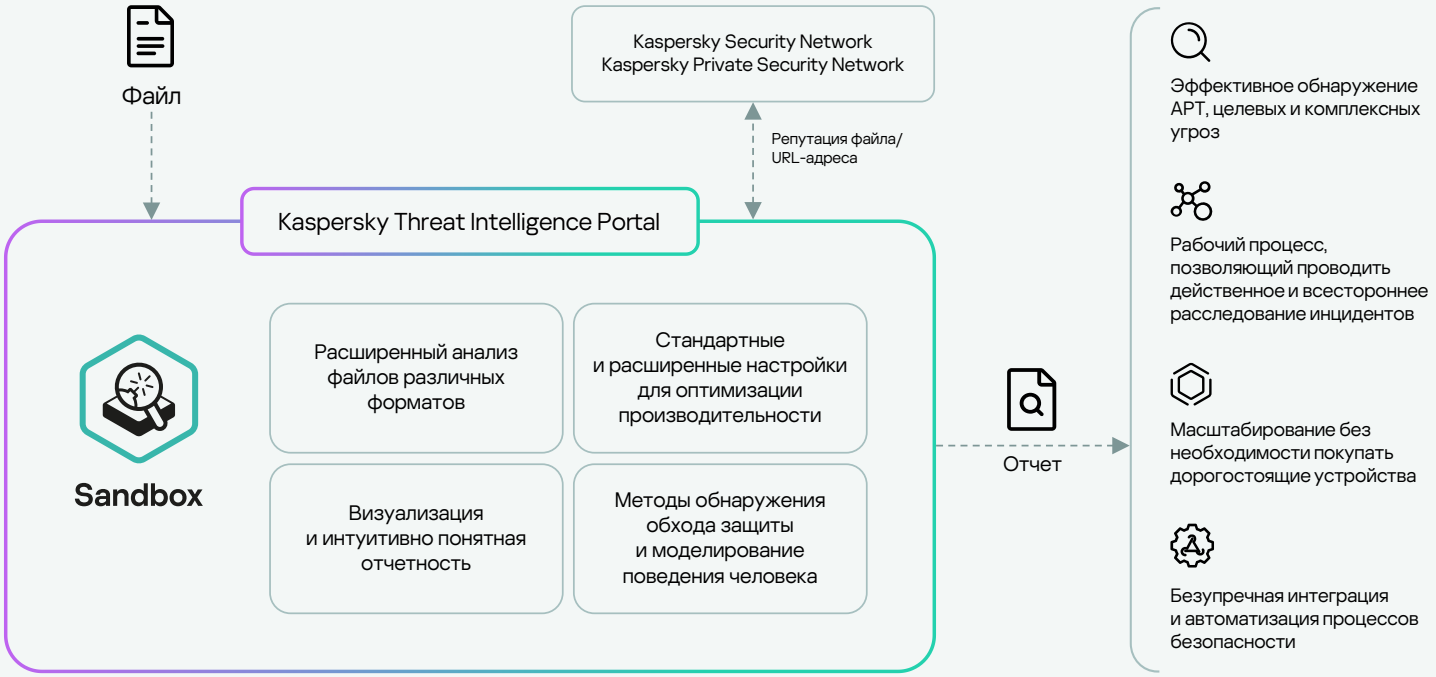
Возможность проверять сетевой трафик, генерируемый при выполнении файла, с помощью преднастроенных Suricata правил

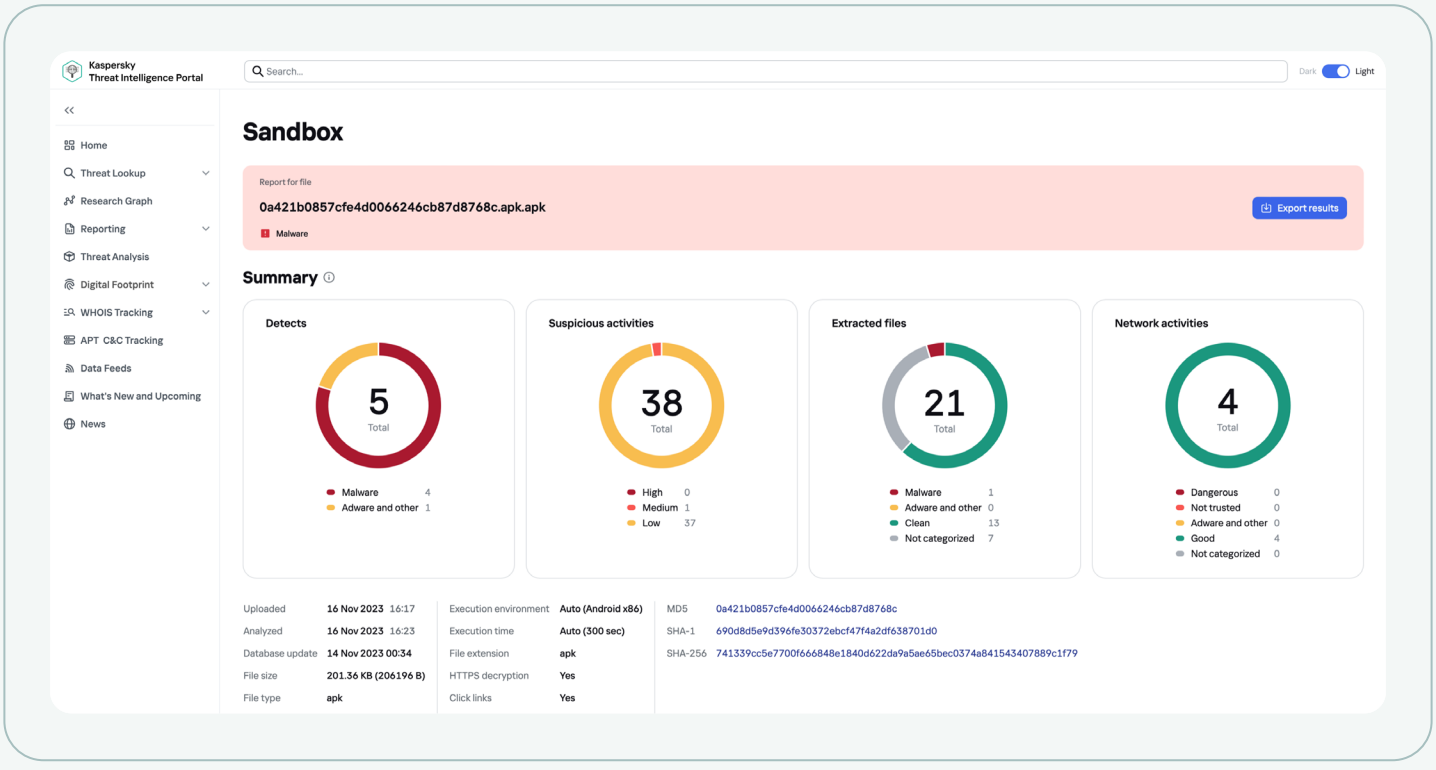
Отправка файлов на анализ вручную и посредством API

В основе Sandbox лежит запатентованная технология «Лаборатории Касперского» (№ патента US10339301). Песочница воссоздает условия для запуска вредоносного кода, позволяя исследователям анализировать подозрительный файл или URL-адрес.

Чтобы избежать разоблачения, вредоносный файл в процессе выполнения может пытаться определить, находится ли он в виртуальной среде, или оставаться неактивным в течение некоторого времени, пока песочница предположительно не завершит процесс анализа его выполнения. Запатентованная технология ускоряет течение времени на виртуальной машине, что позволяет инициировать выполнение вредоносного кода, не дожидаясь истечения запрограммированного в нем времени ожидания.

Схема работы Sandbox





Подробные аналитические отчеты

По завершении анализа Sandbox предоставляет подробный отчет о поведении анализируемого файла, позволяющий реализовать подходящие меры противодействия. Отчет содержит следующие сведения:

Краткие сведения	Общая информация о результатах выполнения файла или проверки URL адреса
Обнаруженные угрозы	Список угроз, выявленных в процессе выполнения файла стандартным антивирусом и технологиями поведенческого анализа
Сработавшие сетевые правила	Список сетевых Suricata-правил, сработавших во время анализа трафика от запущенного объекта
Карта выполнения файла	Графически представленные действия объекта и взаимосвязи между ними
Подозрительная активность	Список зарегистрированных подозрительных действий
Скриншоты	Набор скриншотов, сделанных во время выполнения файла или проверки URL-адреса
Загруженные PE-образы	Список загруженных PE-образов, обнаруженных во время выполнения файла или проверки URL-адреса
Файловые операции	Список файловых операций, которые были зарегистрированы во время выполнения файла или проверки URL-адреса
Операции с реестром	Список операций с реестром ОС, обнаруженных во время выполнения файла или проверки URL-адреса.
Операции с процессами	Список взаимодействий файла с различными процессами, которые были зарегистрированы во время выполнения файла.
Операции синхронизации	Список операций созданных объектов синхронизации (мьютекс, событие, семафор), которые были зарегистрированы во время выполнения файла или проверки URL-адреса
Загруженные файлы	Список файлов, извлеченных из сетевого трафика во время выполнения файла или проверки URL-адреса
Сохраненные файлы	Список файлов, которые были сохранены (созданы или изменены) выполняемым файлом
HTTPS/HTTP/DNS/IP/TCP/UDP и др.	Сведения о сетевых сеансах/запросах, зарегистрированных во время выполнения файла или проверки URL-адреса.
Дамп сетевого трафика (PCAP)	Сетевая активность, которая может быть экспортирована в формат PCAP
Матрица MITRE ATT&CK	Вся активность процессов, зафиксированная в ходе эмуляции, представлена в виде матрицы MITRE ATT&CK

Kaspersky Threat Analysis

Attribution

Аналитический инструмент, помогающий определить возможных авторов и источник вредоносного ПО.

Технология основана на уникальном методе сравнения анализируемых экземпляров подозрительных файлов с целью выявления степени сходства с вредоносными образцами из коллекции «Лаборатории Касперского», обеспечивая практически нулевой процент ложноположительных срабатываний. Система атрибуции «Лаборатории Касперского» позволяет сопоставить новые потенциальные угрозы с известными хакерскими группировками.

Attribution

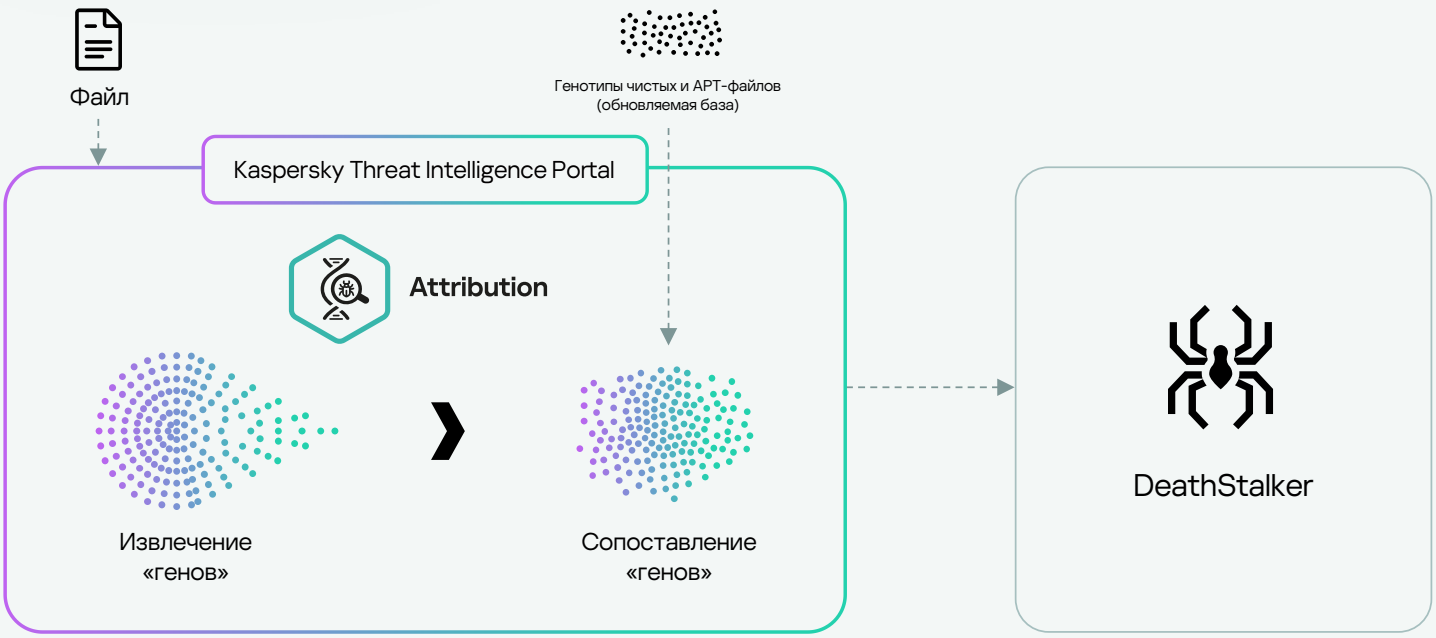
Как правило вредоносные программы, написанные одним и тем же автором, имеют общие паттерны. Сэмплы, оставленные злоумышленниками, тщательно анализируются. На основе уникального кода, обнаруженного во вредоносном файле можно найти похожие на него объекты. Эксперты «Лаборатории Касперского», обнаружившие десятки атак глобального масштаба за годы работы, постоянно изучают новые угрозы и проводят скрупулезные исследования APT-атак. Эти обширные знания легли в основу технологии Attribution, которая позволяет атрибутировать новую угрозу к ранее исследованному вредоносному ПО и APT-группировке.

«Лаборатория Касперского» отслеживает более 1100 угроз и кампаний и выпускает 200+ отчетов об угрозах ежегодно. Исследования экспертов непрерывно пополняют коллекцию APT-файлов, содержащую уже более 80 000 образцов, что в сочетании с использованием автоматизированных инструментов позволяет добиться исключительной точности атрибуции.

Какую проблему решает?

Атрибуция файла к определенной хакерской группировке наряду с информацией о том, как именно атакуют эти киберпреступники, дает возможность определить место и назначение данного файла в общей цепочке атаки. В свою очередь, это дает возможность предположить, где необходимо искать другие IoC/IoA, чтобы, заблокировав отдельный вредоносный файл, не пропустить основную атаку. Все это позволяет оперативно проводить анализ и принимать эффективные меры по защите от целевых атак.

Схема работы Attribution



Особенности продукта

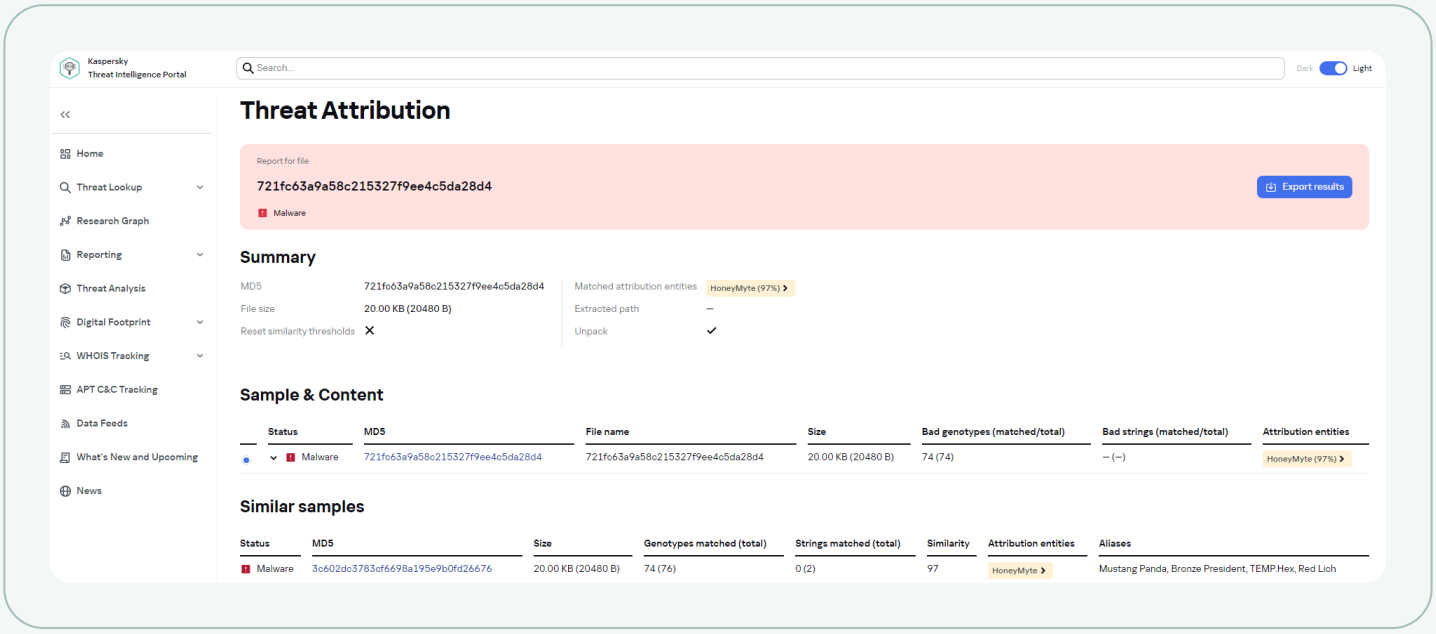
Мгновенный доступ к хранилищу, где содержатся коллекции данных о сотнях APT-компаний и множестве экземпляров вредоносного ПО

Экспорт YARA-правил для дальнейшего автоматизированного поиска похожих файлов в инфраструктуре

Загрузка экземпляров файлов через веб-интерфейс, а также по API (для интеграции с автоматизированными процессами)

Функциональность распаковки защищенных паролем архивов

Экспорт в формат STIX 2.1 (также поддерживаются форматы TXT и JSON) для дальнейшего автоматизированного анализа журналов безопасности и для интеграции со сторонними решениями и средствами безопасности



Метод поиска сходства

Чтобы выявить связь подозрительных файлов с хакерскими группировками, Attribution использует уникальный запатентованный метод поиска сходства «генетического кода» файлов. Этот метод включает в себя:

Анализ генетики образца

путем извлечения из его кода следующих элементов:

- Генотипы — характерные фрагменты двоичного кода
- Строки — характерные строки символов

Автоматический поиск в анализируемых файлах

генотипов и строк, схожих с генотипами и строками образцов, встречавшихся в ранее расследованных APT-атаках или связанных с конкретными хакерскими группировками

На основе найденных схожих данных

формируется отчет о файлах, связанных с анализируемым образцом, и используемых конкретными хакерскими группировками

Kaspersky Threat Analysis

Similarity

Инструмент для выявления файлов со схожей функциональностью, позволяющий защититься от неизвестных и скрытых угроз.

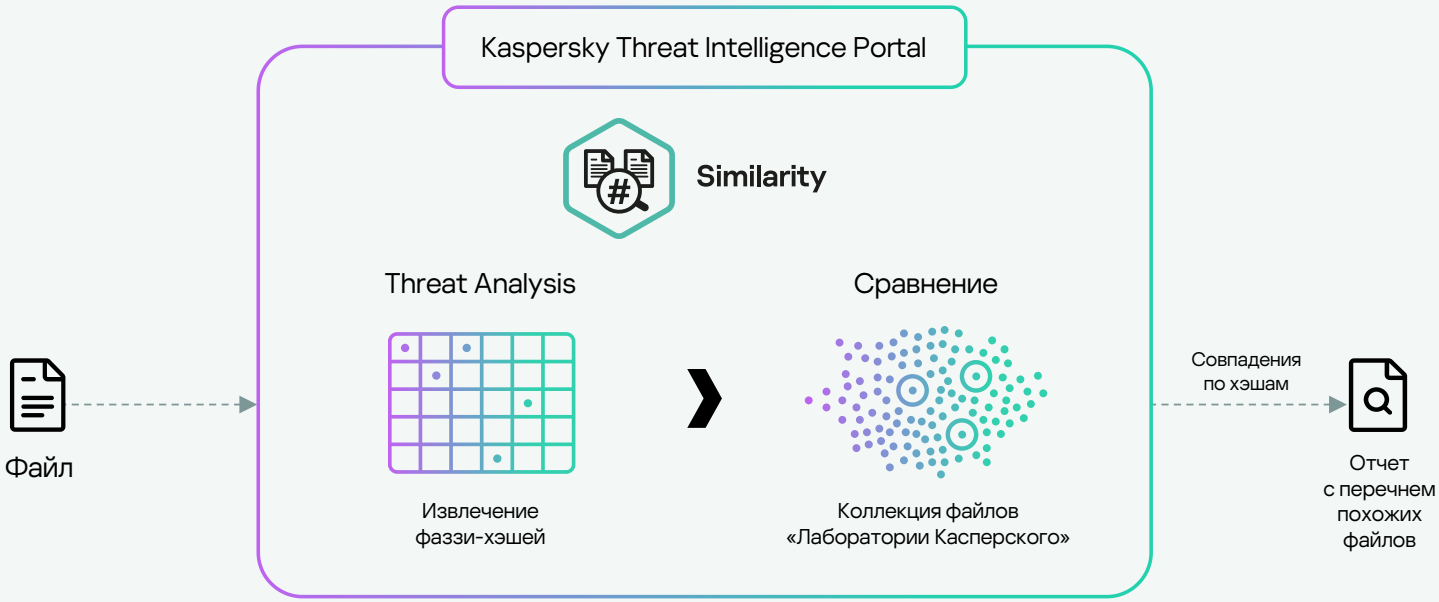
Similarity

Для выстраивания надежной линии обороны не обязательно знать врага в лицо. Similarity — удобный инструмент для выявления файлов, которые функционируют схожим образом, созданный на основе новейшей технологии, разработанной ведущими экспертами «Лабораторией Касперского». Для определения схожести используется более 50 уникальных типов специальных хэшей, а также база данных образцов вредоносного ПО, накопленная «Лабораторией Касперского» более, чем за 25 лет, и содержащая миллионы вредоносных файлов, что позволяет обеспечить высочайшую точность и достоверность результатов.

Какую проблему решает?

Технология позволяет находить в инфраструктуре файлы, похожие по своему поведению на уже известное «Лаборатории Касперского» вредоносное ПО (в том числе уклоняющееся от средств защиты). Благодаря уникальному методу определения схожести можно выявить даже те вредоносные файлы, которые не удалось связать с известными хакерскими группировками. Это дает уверенность в том, что любое изменение злоумышленником вредоносного файла с целью уклонения от обнаружения останется в поле вашего зрения.

Схема работы Similarity



Отчеты

Каждый файл имеет определенный формат, содержит специфические строки, секции, таблицы импорта, может использовать определенный набор программ-упаковщиков. Эксперты «Лаборатории Касперского» создали набор хэшей для определения схожести между файлами по данным признакам. При загрузке исследуемого файла на анализ в Similarity, система извлекает из него фаззи-хэши и сравнивает их с аналогичными хэшами вредоносных файлов, накопленных за более чем 25 лет в библиотеке образцов вредоносного ПО «Лаборатории Касперского». В случае обнаружения совпадений формируется список хэшей наиболее похожих на данный образец известных вредоносных файлов, отсортированных по степени схожести. В отчете содержится дополнительный контекст с метаданными для каждого похожего файла:

- Достоверность схожести
- Статус файла (вредоносное или рекламное ПО)
- Название угрозы (вердикт антивируса)
- Временные метки первого и последнего обнаружения
- Количество совпадений (обнаружений)
- Хэш файла
- Тип файла
- Размер файла

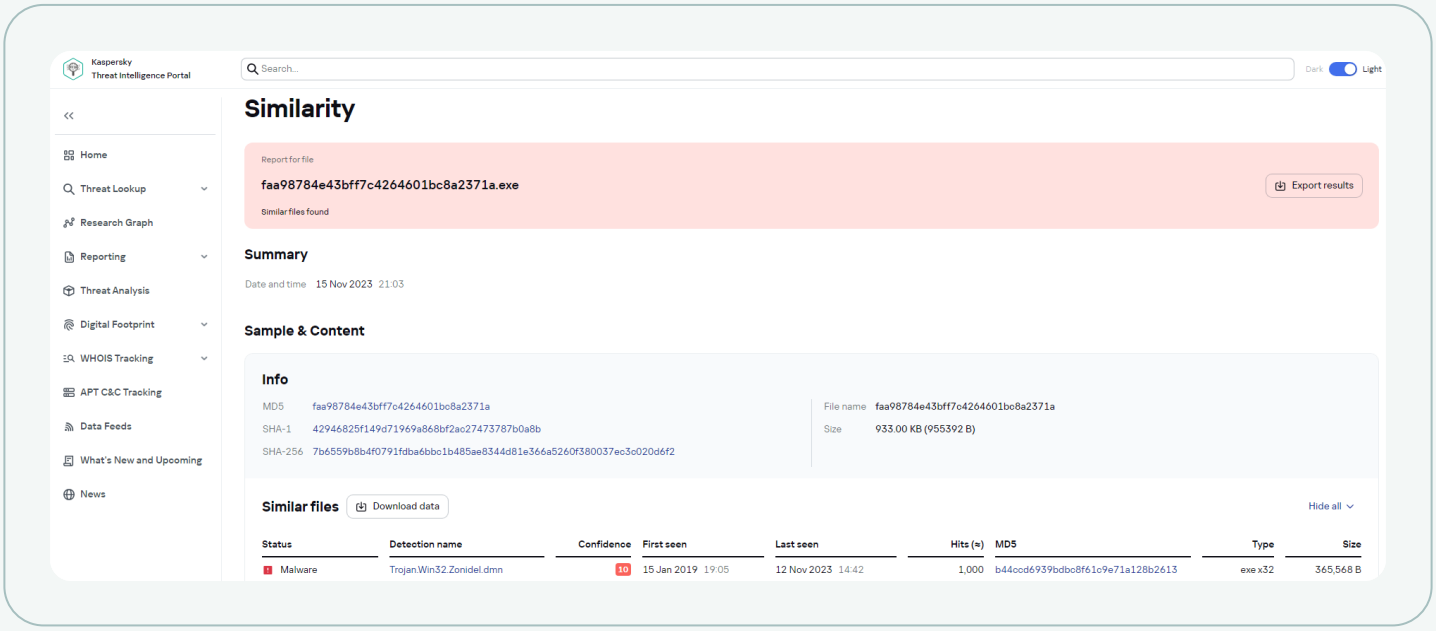
Особенности продукта

Для сравнения используется одна из самых крупнейших в отрасли коллекция данных вредоносных и чистых файлов — миллионы образцов, собранных ведущими экспертами «Лаборатории Касперского» более чем за 25 лет

Загрузка экземпляров файлов через веб-интерфейс и с использованием API (для интеграции с автоматизированными процессами)

Функциональность активно используется в том числе и экспертами «Лаборатории Касперского» для изучения новых угроз, с целью обеспечения максимального уровня защиты в наших продуктах, что регулярно подтверждается высокими оценками по результатам независимых тестов и обзоров

Подробнее



Сценарии использования Kaspersky Threat Analysis

Kaspersky Threat Analysis предоставляет собой полноценный набор инструментов для обнаружения киберугроз. Данные инструменты могут применяться в следующих сценариях:

Реагирование на инциденты

Обнаружение угроз, уклоняющихся от обнаружения средствами защиты

Статический/динамический анализ подозрительных файлов

Выявление связи нового вредоноса с определенной группировкой для понимания возможных дальнейших этапов атаки

Threat Hunting (активный поиск угроз)

Сканирование инфраструктуры на наличие IoCs, содержащихся в отчете

Поиск потенциально вредоносных модификаций популярных чистых файлов

Выявление общих IoCs между неизвестными и известными вредоносными файлами

Анализ вредоносного ПО

Анализ неизвестных угроз

Поиск и анализ схожих вредоносных файлов для определения функциональности исходных обфусцированных файлов

Kaspersky Threat Analysis — это гибкий и мощный инструментарий, состоящий из взаимосвязанных компонент, позволяющих проводить комплексный и многоуровневый анализ подозрительных файлов для выявления и классификации современных киберугроз. Данный инструментарий помогает командам SOC, исследователям безопасности и аналитикам вредоносного ПО оставаться в курсе существующих и возникающих угроз, позволяя быстро расставлять приоритеты и фокусироваться в первую очередь на устранении наиболее критических проблем безопасности.

Kaspersky Intelligence Reporting

Подробнее

Аналитические отчеты об угрозах

Для эффективного противодействия современным киберугрозам требуется всестороннее понимание тактик, техник и процедур, используемых киберпреступниками. Несмотря на то, что командные серверы и инструменты, применяемые для проведения атак, часто меняются, злоумышленникам достаточно сложно изменить свое поведение и методы, применяемые в ходе атаки.

Понимание этих признаков позволяет заранее развернуть эффективные защитные механизмы и таким образом обезоружить киберпреступников, нарушив их планы.

Подписка на аналитические отчеты об угрозах обеспечивает постоянный эксклюзивный доступ к исследованиям «Лаборатории Касперского», предоставляя актуальные сведения о наиболее опасных угрозах.

Наши эксперты непрерывно отслеживают действия кибергруппировок, выявляя наиболее сложные и опасные целевые атаки, кампании кибершпионажа, образцы вредоносного ПО и шифровальщиков, а также новейшие тенденции в сфере киберпреступности по всему миру. Лишь небольшой процент наших расследований доступен широкой публике, в то время как постоянные клиенты «Лаборатории Касперского» всегда имеют доступ к самым актуальным сведениям о новейших угрозах. Это помогает организациям проактивно применять эффективную стратегию для своевременного обнаружения атак, а также нейтрализации и минимизации ущерба от аналогичных угроз.

200+
приватных отчетов в год

300+
профилей кибергруппировок

500+
кампаний

2500+
YARA-правил

17 000+
индикаторов компрометации

В состав аналитических отчетов входят:

Профили злоумышленников

Сопоставление с матрицей MITRE ATT&CK

Бизнес-ориентированная информация для топ-менеджмента

Глубокий технический анализ

- Методы атаки
- Использованные эксплойты
- Описание ВПО
- Описание инфраструктуры атакующих (командные центры и протоколы злоумышленников)
- Анализ эксфильтрации данных
- Атрибуция

Индикаторы компрометации (IOCs) и YARA / Sigma / Suricata-правила

Заключения и рекомендации экспертов «Лаборатории Касперского»

Преимущества

Привилегированный доступ

Не все громкие угрозы становятся известны широкой публике. Но мы предоставляем такую эксклюзивную информацию нашим клиентам еще в ходе расследования, до публичного объявления

Доступ к техническим данным

Технические данные включают расширенный список индикаторов компрометации, доступный в стандартных форматах, таких как openIOC и STIX, а также доступ к правилам YARA / Sigma / Suricata

Профили злоумышленников

Профили злоумышленников включают предполагаемую страну происхождения, основной вид деятельности, используемые семейства вредоносных программ, целевые отрасли и географические регионы, а также описания всех используемых тактик и техник и их сопоставление с MITRE ATT&CK

MITRE ATT&CK

Все тактики и техники злоумышленников, описанные в отчетах, сопоставляются с базой данных MITRE ATT&CK. Это позволяет улучшить качество обнаружения и реагирования на соответствующие тактики и техники злоумышленников

Ретроспективный анализ

В течение срока действия подписки доступны все ранее выпущенные закрытые отчеты

Поддержка RESTful API

Беспрепятственная интеграция и автоматизация процессов безопасности

В зависимости от специфики деятельности вашей организации предлагаем несколько типов коммерческих отчетов

Kaspersky APT Intelligence Reporting

APT Intelligence Reporting

В аналитических отчетах об APT-угрозах содержится информация о самых сложных целевых атаках, авторами которых обычно являются хорошо организованные и финансируемые кибер-группировки. В нем содержится информация о различных APT-группах по всему миру, их тактиках, техниках и процедурах (TTPs), а также о секторах экономики и регионах, на которые они направлены. В данном типе отчета основное внимание уделяется шпионской деятельности — от атак на цепочки поставок до активистских и деструктивных действий.

Эти отчеты наиболее ориентированы на крупные корпорации, государственные учреждения и организации, связанные с критической инфраструктурой, хранящие конфиденциальные данные, представляющие интерес для государственных субъектов.

Kaspersky Crimeware Intelligence Reporting

Crimeware Intelligence Reporting

Отчеты об угрозах, связанные с финансово мотивированными группировками посвящены последним тенденциям в киберпреступности, включая утечки данных, продаваемых в дарквебе, финансовое мошенничество, программы-вымогатели и вредоносное ПО, ориентированное на банкоматы и платежные терминалы. В данном отчете основное внимание уделяется кампаниям, атакам, и инструментам, основной целью которых является получение финансовой выгоды.

Этот тип отчетов особенно актуален для организаций, ведущих значительный объем бизнеса через интернет или хранящих конфиденциальные данные о клиентах, например для финансовых и платежных организаций, банков, платформ электронной коммерции.

Kaspersky Intelligence Reporting

ICS Threat Intelligence Reporting

В рамках Kaspersky ICS Threat Intelligence Reporting «Лаборатория Касперского» предоставляет подробную аналитику вредоносных кампаний, нацеленных на промышленные организации, аналитику уязвимостей, обнаруженных в наиболее популярных АСУ ТП и технологиях, используемых в инфраструктурах промышленных компаний, а также предоставляет ранние предупреждения об угрозах и свежих найденных уязвимостях. Материалы создаются выделенной командой Kaspersky ICS CERT, в которой работает 20+ высококвалифицированных специалистов по исследованию угроз и уязвимостей АСУ ТП, реагированию на инциденты и анализу безопасности.

Сервис позволяет снизить время реакции на инцидент, отреагировать на инцидент оптимальным образом с меньшими потерями, снизить риски остановки работы и сократить время возможного простоя предприятия.

Другие сервисы, предоставляемые командой Kaspersky ICS CERT:

ICS Malishious Hash Data Feed

Регулярно обновляемый поток машиночитаемых данных об актуальных угрозах кибербезопасности для АСУ ТП, позволяющий упростить и автоматизировать своевременное обнаружение и расследование кибератак

ICS Vulnerability Data Feed

Регулярно обновляемый поток проверенных и уточненных данных об уязвимостях в ПО и оборудовании АСУ ТП и других решениях, широко применяемых в промышленных средах, в унифицированном машиночитаемом формате

ICS Vulnerability Data Feed в формате OVAL

Регулярно обновляемый поток OVAL-определений для автоматического обнаружения известных уязвимостей в SCADA системах и другом промышленном программном обеспечении

Kaspersky Digital Footprint Intelligence

Подробнее

Kaspersky Digital Footprint Intelligence

Аналитические отчеты об угрозах для организации

По мере развития компании ее IT-инфраструктура становится все более сложной, поэтому появляется важная задача — защитить распределенные цифровые ресурсы без прямого контроля над ними. Динамические и взаимосвязанные среды дают организациям множество преимуществ. Однако постоянный рост взаимосвязей расширяет поверхность атаки, а злоумышленники действуют все более изощренно. Поэтому важно не только иметь точное представление об онлайн-присутствии предприятия, но также отслеживать изменения и реагировать на актуальные данные об уязвимых цифровых активах.

Компаниям доступно множество защитных инструментов, но некоторые задачи по-прежнему вызывают у них трудности, к примеру отслеживание киберпреступных планов и мошеннических схем на форумах даркнета. Чтобы аналитики по безопасности могли оценивать угрозы со стороны внешних атакующих, быстро выявлять возможные векторы атак и принимать стратегические решения по защите от них, «Лаборатория Касперского» разработала сервис Kaspersky Digital Footprint Intelligence.

Основные возможности

Kaspersky Digital Footprint Intelligence предоставляет комплексную защиту от цифровых рисков, которая помогает компаниям отслеживать свои цифровые активы и обнаруживать угрозы в даркнет-ресурсах (deep web, darknet и dark web).

Мониторинг даркнета

Постоянный мониторинг десятков даркнет-ресурсов (форумы, блоги вымогателей, мессенджеры, тор-сайты и т. д.), выявляющий любые упоминания и угрозы, касающиеся вашей компании, клиентов и партнеров. Анализ активных целевых или планируемых атак, APT-кампаний, направленных на вашу компанию, отрасль и регионы присутствия.

Обнаружение утечек данных

Обнаружение скомпрометированных учетных данных сотрудников, партнеров и клиентов, банковских карт, номеров телефонов и другой конфиденциальной информации, которая может быть использована для проведения атаки или создания репутационных рисков для вашей компании.

Анализ сетевого периметра

Идентификация сетевых ресурсов и открытых сервисов компании, которые являются потенциальной точкой входа злоумышленников для атаки. Индивидуальный анализ существующих уязвимостей с дальнейшим подсчетом баллов и всесторонней оценкой рисков на основе системы Common Vulnerability Scoring System (CVSS), наличия общедоступных эксплойтов, опыта тестирования на проникновение и местоположения сетевого ресурса (хостинга/инфраструктуры).

Обнаружение угроз

Мониторинг вредоносной активности, которая может нанести ущерб репутации компании и/или привести к атакам на ее клиентов.

Принцип работы

Конфигурация

Инвентаризация всех цифровых активов компании

Сбор данных

Автоматизированный сбор данных из Даркнета (DarkWeb) и видимой часть сети Интернет (Surface Web), а также из базы знаний «Лаборатории Касперского»

Фильтрация

Обнаружение угроз, их анализ и приоритезация под управлением аналитиков

Оповещение

Предоставление оперативных уведомлений об угрозах на Kaspersky Threat Intelligence Portal или по API

Преимущества

Защита бренда

Выявление потенциальных угроз в режиме реального времени для защиты репутации вашего бренда, сохранения доверия клиентов, снижения риска финансовых потерь и ущерба бизнес-операциям

Вскрытие замыслов злоумышленников

Предупрежден — значит вооружен. Узнайте, что киберпреступники обсуждают в даркнете о вашей компании и планируют ли атаки

Быстрое реагирование

Дополнительный контекст для мгновенных уведомлений улучшает реагирование на инциденты и сокращает среднее время реагирования (MTTR)

Сокращение векторов атаки

Аналитические данные и рекомендации позволяют сократить количество потенциальных векторов атаки и риски информационной безопасности для организации

Оптимизация затрат

Помощь лицам, принимающим решения, в приоритезации расходов на кибербезопасность за счет выявления пробелов в текущей защите и связанных с ними рисков

Дополнительная экспертиза

Усиление ваших внутренних команд безопасности дополнительными возможностями для противостояния кибератакам и выявления угроз

Kaspersky Takedown Service

Подробнее

Kaspersky Takedown Service

Сервис по удалению вредоносных и фишинговых доменов

Киберпреступники создают вредоносные и фишинговые домены для атак на организации и их бренды. Такие угрозы требуют немедленного реагирования, поскольку могут причинить финансовый ущерб, повредить репутации, привести к потере клиентов, утечке данных и другим неприятным последствиям. Однако блокирование доменов — комплексный процесс, которым должны заниматься эксперты.

За день «Лаборатория Касперского» блокирует более 15 000 фишинговых и мошеннических адресов и предотвращает более миллиона попыток перехода по таким ссылкам. Kaspersky Takedown также позволяет защититься от поддельных аккаунтов в социальных сетях и приложений, публикуемых на маркетплейсах, до того, как они нанесут вред бренду и бизнесу.

За годы нашей работы мы проанализировали большое количество вредоносных и фишинговых доменов и знаем, как собирать доказательства их вредоносности. Мы возьмем на себя управление всем процессом блокировки и примем оперативные меры для снижения цифровых рисков для вашей компании, а вы сможете заняться другими приоритетными задачами.

«Лаборатория Касперского» предлагает своим клиентам эффективные решения для защиты онлайн-сервисов и репутации. Мы сотрудничаем с международными организациями, государственными и региональными правоохранительными органами полицейского управления Нидерландов и полицией Лондона), а также с группами экстренного реагирования на инциденты (CERT) по всему миру.

Принцип работы

1

Отправьте запрос через свою корпоративную учетную запись на нашем портале поддержки корпоративных клиентов.

Подробнее

2

Мы подготовим всю необходимую документацию и направим запрос на блокирование в компетентный местный или региональный орган (CERT, регистратор и т. д.), уполномоченный на исполнение такого запроса.

3

Вы будете получать уведомления на каждом этапе работы с вашим запросом – до тех пор, пока домен не будет заблокирован.

Преимущества

Полная прозрачность

Вы будете получать уведомления на каждом этапе процесса — от регистрации вашего запроса на блокирование до его исполнения

Экономия ваших ресурсов

Мы позаботимся обо всем процессе блокирования — ваше участие в нем будет минимальным

Глобальный охват

Где бы ни был зарегистрирован домен вредоносного или фишингового сайта, мы направим запрос на блокирование такого домена в организацию с необходимыми полномочиями в регионе

Интеграция с Digital Footprint Intelligence

Kaspersky Takedown и Kaspersky Digital Footprint Intelligence можно приобрести отдельно. Но еще лучше они работают вместе, так как они полностью интегрированы и дополняют друг друга. Kaspersky Digital Footprint Intelligence в режиме реального времени уведомляет о фишинговых и вредоносных доменах, и эти данные могут быть немедленно переданы в Kaspersky Takedown, чтобы заблокировать такие домены

Kaspersky Ask the Analyst

Подробнее

Kaspersky Ask the Analyst

Сервис по взаимодействию с экспертами

Ландшафт угроз непрерывно меняется, их количество быстро растет, а у злоумышленников появляются все более изощренные методы и техники для проведения атак. Все чаще происходят сложные киберинциденты, вызванные атаками без использования вредоносных программ, бесфайловыми атаками, атаками с использованием легитимных инструментов, эксплойтами «нулевого дня», а также встречаются различные комбинации этих сценариев, которые применяются для проведения сложных, целевых и APT-атак. Кибератаки могут разрушить бизнес, поэтому профессионалы в области кибербезопасности важны как никогда. Но найти и удержать их бывает непросто. Даже если у вас есть компетентная ИБ-команда, ваши эксперты не всегда могут противостоять изощренным угрозам самостоятельно — иногда им требуется обратиться к сторонним специалистам за помощью. Привлекая внешних экспертов, вы сможете выявить наиболее вероятные векторы сложных и целевых атак и получить практические рекомендации по эффективной борьбе с ними.

Kaspersky Ask the Analyst дополняет наш комплекс сервисов Kaspersky Threat Intelligence. С помощью этого сервиса вы можете обращаться к экспертам за поддержкой и полезной информацией по конкретным угрозам, с которыми вы сталкиваетесь или которые вас интересуют. Сервис персонализирует мощные инструменты аналитики угроз и проведения исследований «Лаборатории Касперского» под ваши потребности. Используя эти данные, вы сможете усовершенствовать систему защиты против угроз, нацеленных на вашу организацию.

Преимущества

Заручитесь поддержкой профессионалов

Вы сможете при необходимости обращаться к отраслевым экспертам: вам больше не понадобится искать людей и нанимать в штат узких специалистов

Ускорьте расследование

Эффективно оценивайте инциденты безопасности и назначайте им приоритеты на основании персонализированной и подробной контекстной информации

Реагируйте быстро и точно

Оперативно реагируйте на угрозы и уязвимости, блокируя известные векторы атак с помощью инструкций наших экспертов

Доступ к экспертным знаниям и ресурсам

Kaspersky Ask the Analyst предоставляет доступ к команде исследователей «Лаборатории Касперского». Мы готовы делиться знаниями и ресурсами, которые дополнят ваши возможности в области анализа угроз и реагирования на инциденты

Основные возможности

Запросы, связанные с АСУ ТП

- Дополнительная информация об опубликованных отчетах
- Информация об уязвимостях АСУ ТП
- Статистика угроз АСУ ТП и новые тенденции по регионам и отраслям
- Анализ вредоносных программ, нацеленных на АСУ ТП
- Информация, касающаяся нормативных требований и стандартов

Информация об APT-атаках и Crimeware-угрозах

Дополнительная информация об опубликованных ранее отчетах и текущих исследованиях; в дополнение к отчетам об APT-атаках и атаках с использованием специального ПО, разработанного для совершения преступлений (Crimeware*)

Анализ угроз в даркнете**

- Исследование даркнета на предмет конкретных артефактов, IP-адресов, доменных имен, имен файлов, адресов электронной почты, ссылок или изображений
- Поиск и анализ информации

Анализ вредоносного ПО

- Анализ образцов вредоносного ПО
- Рекомендации по противодействию и устранению последствий

Описание угроз, уязвимостей и связанных с ними индикаторов компрометации

- Общее описание конкретных семейств вредоносного ПО
- Дополнительный контекст для индикаторов компрометации (связанные хеши, URL, командные серверы и т. д.)
- Информация о конкретных уязвимостях (насколько они критичны, какие механизмы продуктов «Лаборатории Касперского» защищают от них)

Принцип работы

Подписку на сервис Kaspersky Ask the Analyst можно приобрести отдельно или в дополнение к любому другому нашему сервису Kaspersky Threat Intelligence. Запросы в рамках сервиса можно отправлять через свою корпоративную учетную запись на нашем портале поддержки корпоративных клиентов. Мы направим ответ по электронной почте, но в случае необходимости и по согласованию с вами мы можем также организовать конференц-связь и (или) звонок с совместным доступом к экрану. После принятия вашего запроса мы сообщим вам предварительные сроки его обработки.

* Доступно только клиентам, которые подписались на отчеты об APT-атаках и (или) атаках с использованием Crimeware

** Уже включено в подписку Kaspersky Digital Footprint Intelligence

Сценарии использования:

1. Уточнение информации из ранее опубликованных отчетов об угрозах
2. Получение дополнительной информации по уже обнаруженным индикаторам компрометации
3. Получение подробного описания уязвимостей и рекомендации по защите от их эксплуатации
4. Получение сведений об интересующей вас активности на ресурсах даркнета
5. Получение общего отчета по семейству вредоносного ПО, включая его поведение, возможные последствия атаки и подробное описание любой связанной активности, известной «Лаборатории Касперского»
6. Эффективная приоритизация оповещений об угрозах и (или) инцидентах с помощью подробной контекстной информации и категоризации связанных индикаторов компрометации
7. Помощь в определении природы подозрительной активности (APT-угроза или атака с использованием Crimeware)
8. Отправка вредоносных файлов на комплексный анализ, чтобы понять поведение и функциональность предоставленных образцов

Kaspersky Threat Intelligence

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее