Kaspersky Threat Intelligence

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Наблюдать за эволюцией киберугроз, анализировать их, вовремя на них реагировать и сводить к минимуму их последствия – чрезвычайно трудоемкий процесс. Организации во всех отраслях сталкиваются с нехваткой достоверных и оперативно обновляемых данных об угрозах. Чтобы эффективно управлять рисками безопасности, необходимо регулярно получать такие данные.

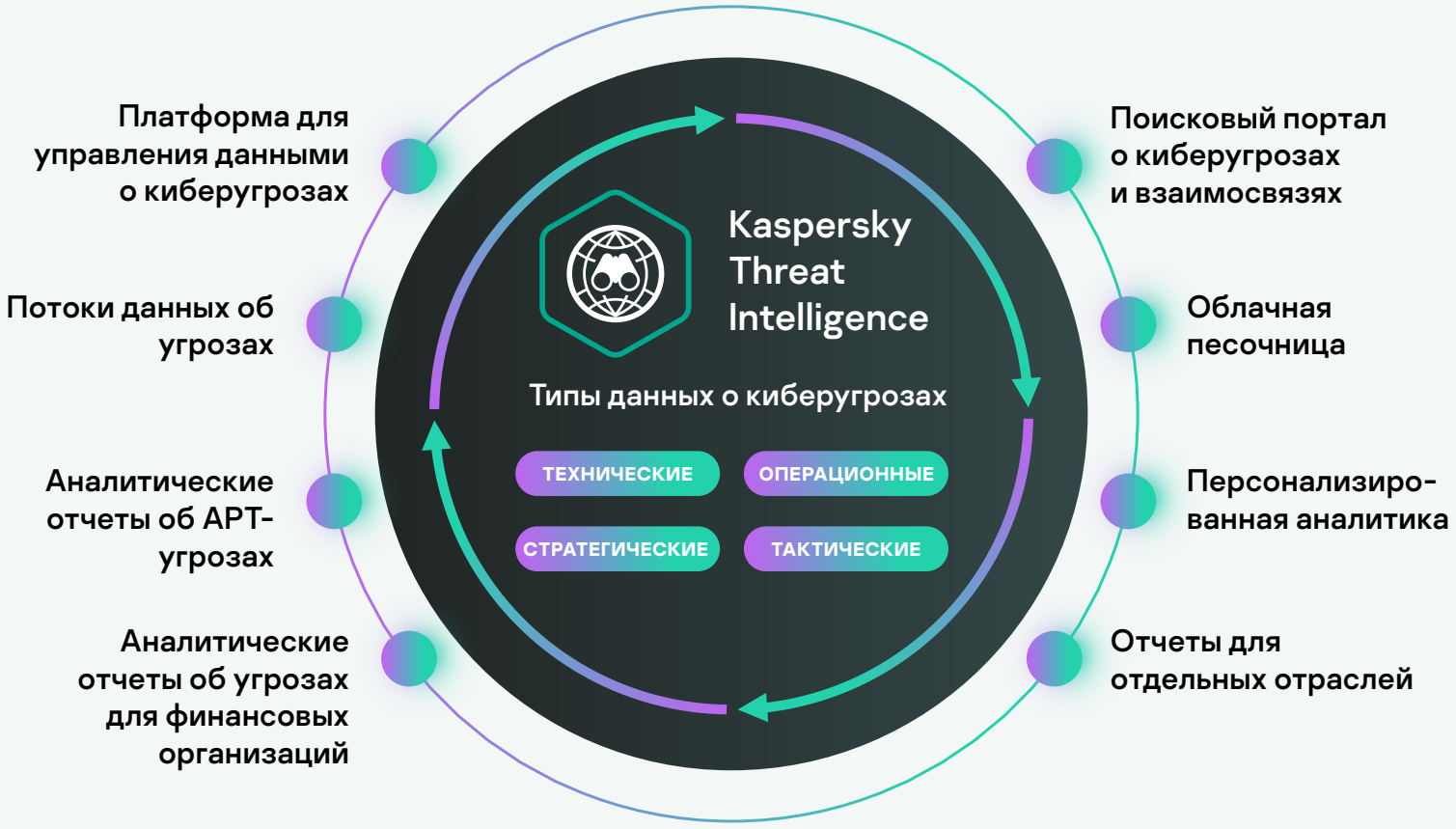
Kaspersky Threat Intelligence

«Лаборатория Касперского» предлагает сервисы информирования об угрозах, которые открывают доступ к различной информации, полученной нашими аналитиками и исследователями мирового класса. Эти данные помогут любой организации эффективно противостоять современным киберугрозам.

Наша компания обладает глубокими знаниями, богатым опытом исследования киберугроз и уникальными сведениями обо всех аспектах IT-безопасности. Благодаря этому «Лаборатория Касперского» стала доверенным партнером правоохранительных и государственных организаций по всему миру, в том числе Интерпола и различных подразделений CERT. Kaspersky Threat Intelligence предоставляет актуальные технические, тактические, операционные и стратегические данные об угрозах.

Kaspersky Threat Intelligence включает:

Kasperky CyberTrace, Kaspersky Threat Data Feeds, Kaspersky Threat Lookup, Kaspersky Cloud Sandbox и набор аналитических отчетов об угрозах.



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. В этой ситуации необходимы новые методы защиты, основанные на анализе угроз.

Благодаря интеграции потоков оперативных 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.

Контекстные данные

Каждая запись в каждом потоке содержит контекстные данные, позволяющие быстро подтвердить и приоритизировать угрозы (имена угроз, метки времени, географическое положение, установленные IP-адреса зараженных веб-ресурсов, хеши, популярность и прочее). Эти данные можно использовать, например чтобы составить общее представление о событии или провести дополнительные проверки. Они помогут найти ответы на вопросы «кто?», «что?», «где?» и «когда?» и выявить источники атак, чтобы принимать своевременные решения и защищать компанию от угроз любой сложности.

Преимущества

Сбор и обработка данных

Данные собираются из множества разнообразных надежных источников, включая сеть Kaspersky Security Network и наши собственные поисковые роботы, сервис мониторинга ботнет-угроз (круглосуточное слежение за ботнетами, их целями и действиями), ловушки для спама, данные исследовательских групп и партнеров.

Вся собранная информация тщательно проверяется и очищается в режиме реального времени при помощи различных методов предварительной обработки: статистических критериев, песочниц, средств эвристического анализа, инструментов для определения сходств, профилирования моделей поведения и проверки аналитиками.

Потоки данных генерируются автоматически в режиме реального времени на основе данных, собираемых по всему миру. Это обеспечивает точность и высокую скорость обнаружения.

Простота внедрения. Для эффективной интеграции предоставляется дополнительная документация, образцы, помощь службы технической поддержки «Лаборатории Касперского».

Простые форматы для распространения данных (JSON, CSV, OpenIoC, STIX) через HTTPS, TAXII и специализированные методы доставки позволяют с легкостью интегрировать потоки данных в ИБ-решения.

Потоки данных, содержащие много ложноположительных записей, практически бесполезны, поэтому проводятся скрупулезное тестирование и фильтрация данных, чтобы заказчикам предоставлялась только на 100% подтвержденная информация.

В подготовке потоков данных участвуют сотни специалистов, включая аналитиков безопасности со всего мира, экспертов из глобального центра исследования и анализа угроз (GReAT) и ведущие команды отдела исследований и разработки (R&D). Специалисты по безопасности получают критически важную информацию и уведомления, генерируемые на основе надежных данных, не тратя время и силы на обработку некритичных оповещений.

Все данные генерируются и отслеживаются мощной отказоустойчивой инфраструктурой, что обеспечивает постоянную доступность.

Ценность

Повышение эффективности решений для защиты сети, включая SIEM-системы, межсетевые экраны, системы обнаружения и предотвращения вторжений, прокси-серверы и другие защитные решения с помощью интеграции с постоянно обновляемыми списками. Эти списки содержат актуальные индикаторы компрометации с дополнительными контекстными данными, что позволяет вовремя обнаруживать угрозы и лучше понимать намерения злоумышленников.

Ускорение реагирования на инциденты и расширение возможностей криминалистического анализа за счет автоматизации процесса первоначальной сортировки. Аналитики по безопасности получают контекстные данные для немедленного выявления предупреждений, подлежащих расследованию или передаче группам реагирования на инциденты.

Поставщики управляемых услуг безопасности могут развивать свой бизнес, предлагая клиентам аналитику угроз мирового уровня как услугу премиум-класса. Группы экстренного реагирования на угрозы (CERT) могут расширить свои возможности и повысить качество обнаружения и идентификации угроз.

Kaspersky CyberTrace Платформа для управления данными о киберугрозах

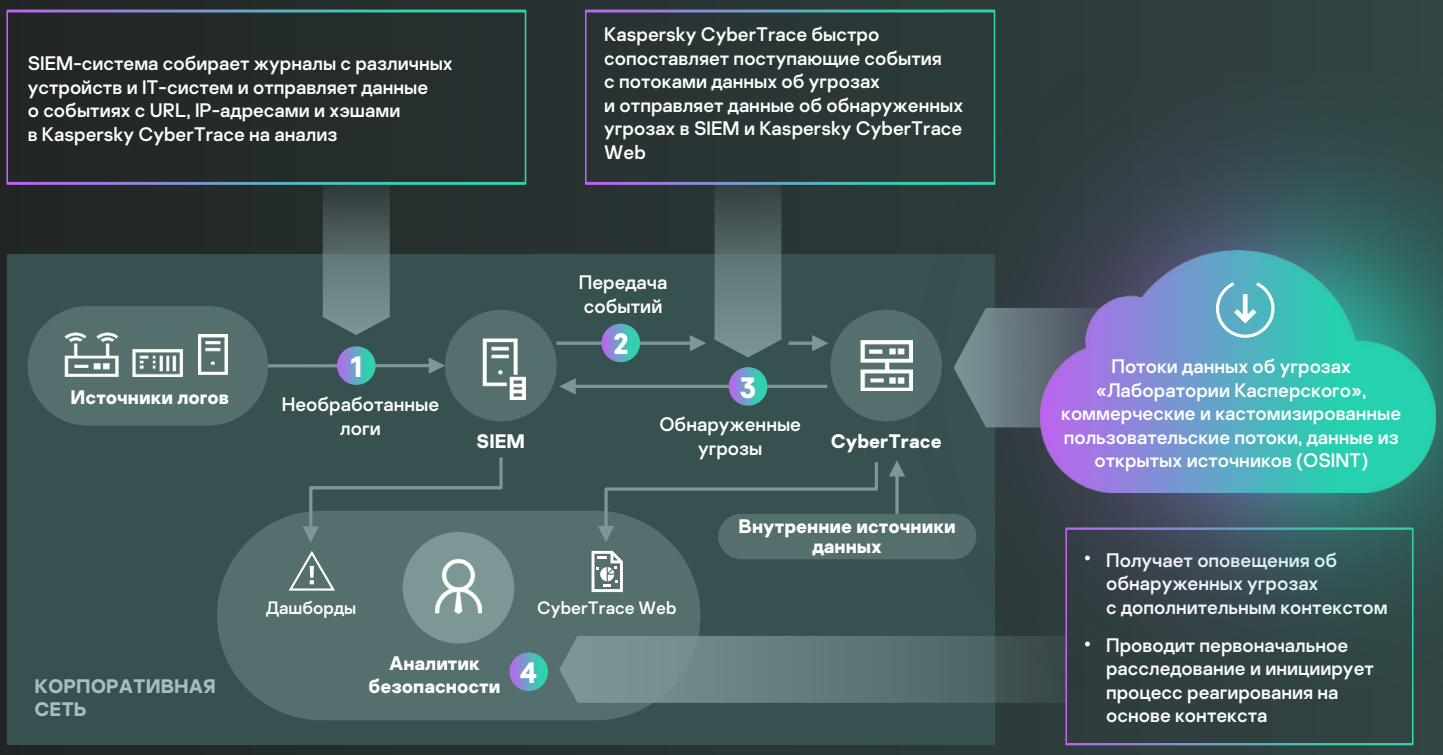
Интеграция актуальных машиночитаемых аналитических данных об угрозах в существующие средства управления безопасностью, такие как SIEM-системы, позволяет автоматизировать процесс первоначальной приоритизации и классификации. Но постоянный рост числа доступных для интеграции потоков данных об угрозах мешает определить источники информации, подходящие для конкретной организации. Аналитические данные предоставляются в различных форматах, 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.

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.
- 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.
- 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 наблюдаемые объекты в ранее проверенных событиях с использованием последних потоков данных для поиска не обнаруженных ранее угроз.
- 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.
- REST API позволяет выполнять поиск и управлять аналитическими данными об угрозах, а также интегрировать Kaspersky CyberTrace в сложные среды для автоматизации и управления.

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. На схеме ниже показана высокоуровневая архитектура решения.



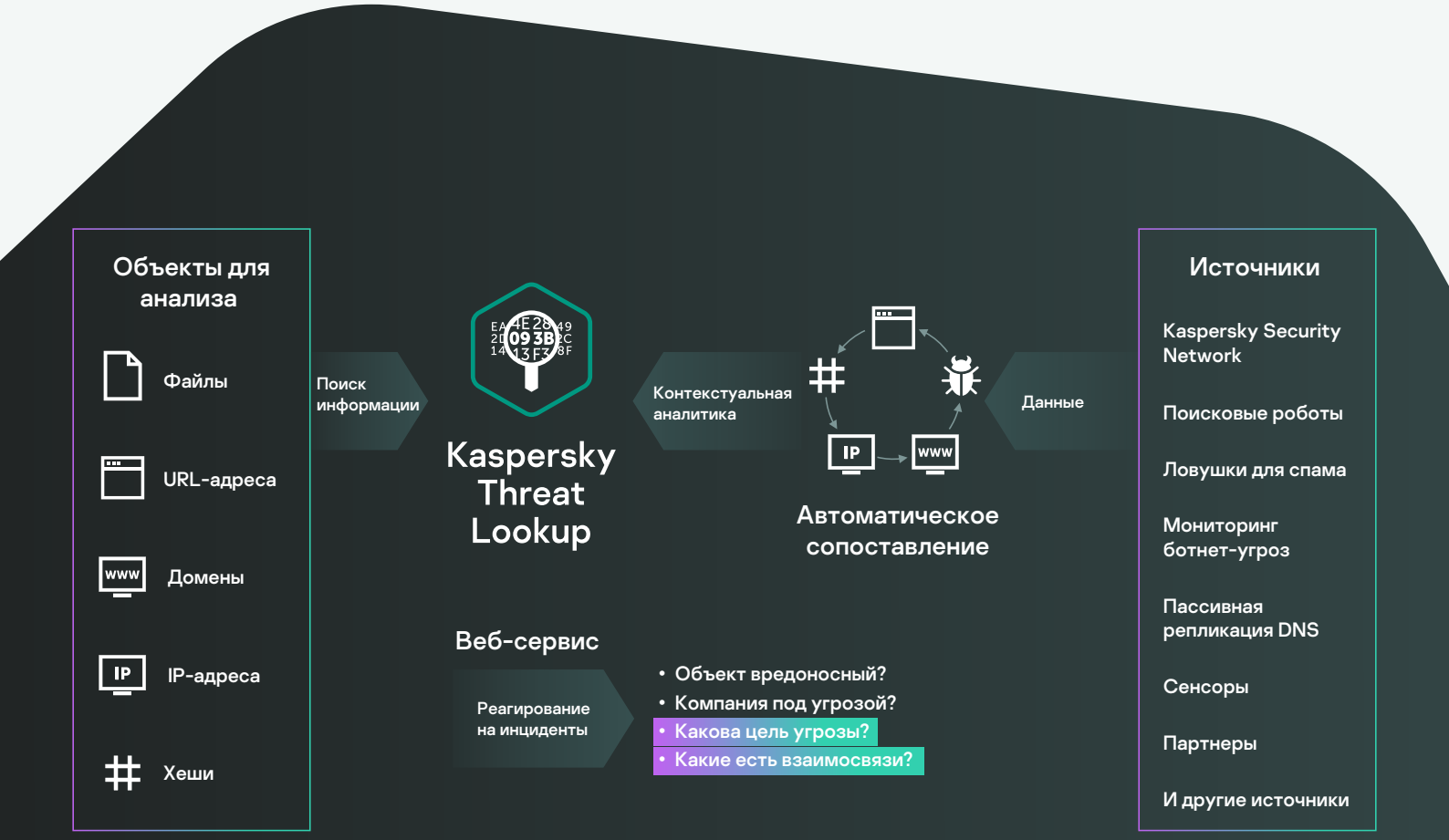
Kaspersky CyberTrace и потоки данных «Лаборатории Касперского» об угрозах позволяют аналитикам безопасности:

- эффективно фильтровать и приоритизировать огромное количество оповещений систем безопасности;
- оптимизировать и ускорять процессы классификации и сдерживания угроз;
- быстро определять наиболее критичные из оповещений и принимать более взвешенные решения об их дальнейшей передаче группам реагирования;
- создавать проактивную систему защиты на основе глобальных аналитических данных.

Kaspersky Threat Lookup
Поисковый портал о киберугрозах и 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 знаниям о киберугрозах и их взаимосвязях. Сервис предоставляет специалистам по безопасности максимум информации для предотвращения кибератак до того, как организации будет нанесен вред. Портал получает последние результаты анализа угроз, детализированные 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.



Плафторма поможет:

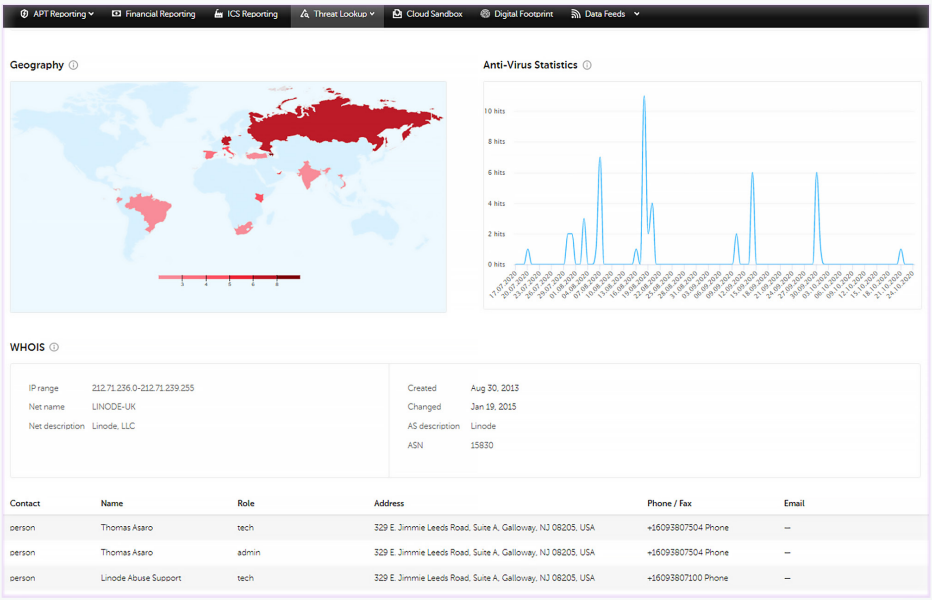
Найти информацию об индикаторах угроз с помощью веб-интерфейса или REST API.

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

Выяснить, является ли обнаруженный объект распространенным или уникальным.

Понять, почему объект считается вредоносным.

Интерфейс Kaspersky Threat Lookup



Аналитические данные об угрозах, предоставляемые сервисом Kaspersky Threat Lookup, генерируются и отслеживаются в режиме реального времени мощной отказоустойчивой инфраструктурой, которая обеспечивает постоянную доступность и бесперебойную работу сервиса. В подготовке аналитических данных участвуют сотни экспертов, включая аналитиков безопасности со всегомира, специалистов центра глобальных исследований и анализа угроз (GReAT) и ведущие научно-исследовательские коллективы.

Ценность

Глубокий поиск индикаторов угроз с проверенным контекстом, позволяющий приоритизировать атаки и сосредоточиться на устранении угроз, представляющих наибольший риск для бизнеса.

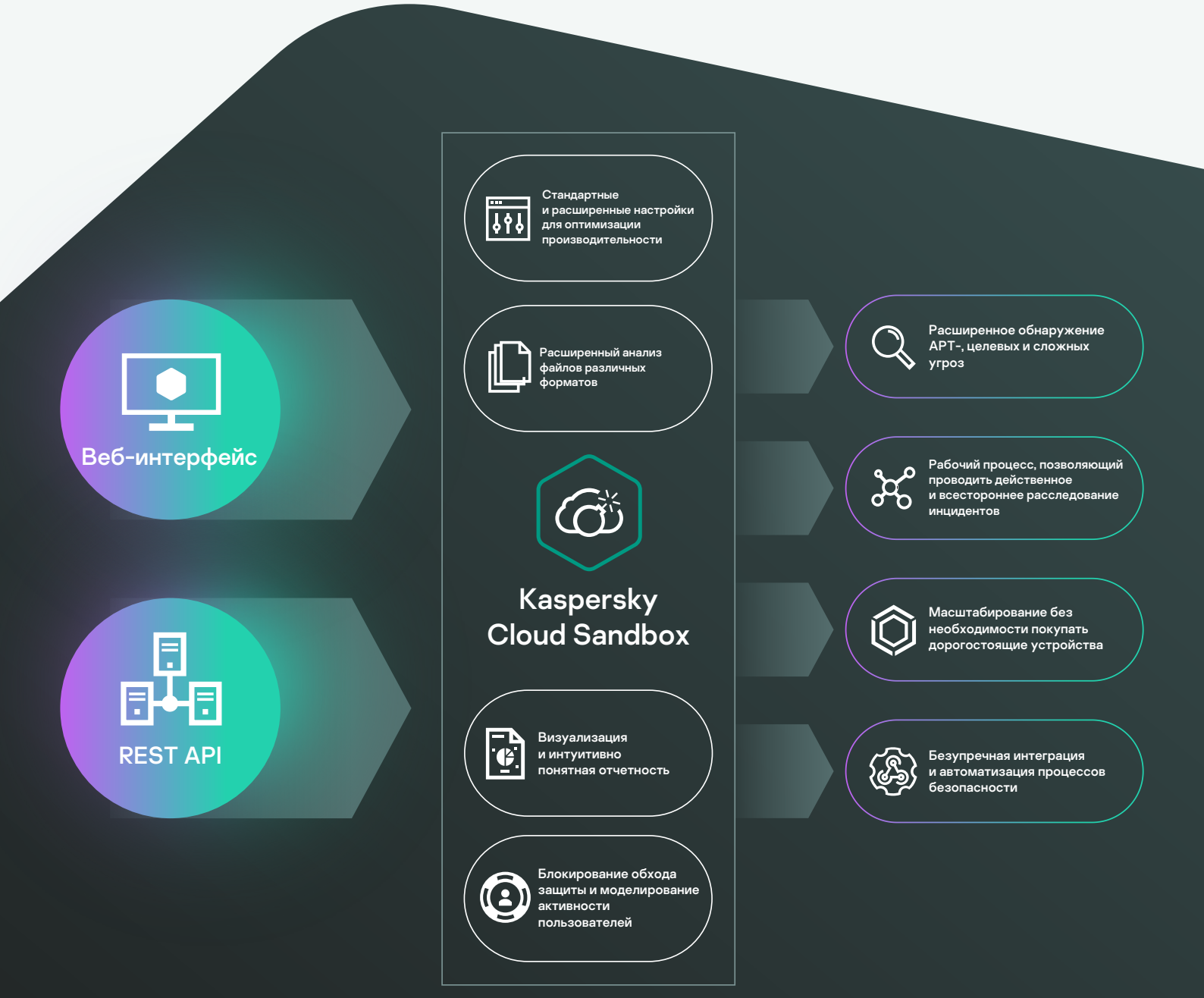
Эффективная и результативная диагностика и анализ инцидентов безопасности на узлах и в сети. Приоритизация сигналов о неизвестных угрозах от внутренних систем.

Улучшение процесса реагирования на инциденты и расширение возможностей поиска угроз, позволяющее прервать цепочку развития угрозы до момента компрометации критически важных систем и данных.

Kaspersky Cloud Sandbox
Облачная песочница

Современные целевые атаки невозможно предотвратить, используя только традиционные превентивные инструменты.

Принятие аналитического решения на основе поведения файла при одновременном анализе памяти процессов, сетевой активности и прочих показателей – это оптимальный подход к пониманию современных комплексных целевых и APT-угроз. В статистических данных часто не хватает информации о недавно измененных вредоносных программах, чего не скажешь о технологии песочницы – это мощный инструмент, который позволяет исследовать исходные образцы файлов, находить индикаторы компрометации на основании поведенческого анализа и обнаруживать вредоносные объекты, которые не встречались ранее.



Комплексная отчетность

- Загрузка и запуск библиотек DLL
- Внешнее соединение с доменными именами и IP-адресами
- Создание, изменение и удаление файлов
- Подробная информация об угрозах с рекомендациями для каждого выявленного индикатора компрометации
- Дампы памяти процессов и сетевого трафика (PCAP)
- Запросы и ответы HTTP и DNS
- Создание взаимных исключений (мьютексы)
- REST API
- Изменение и создание ключей реестра
- Создание процессов с помощью выполняемого файла
- Снимки экрана
- И многое другое

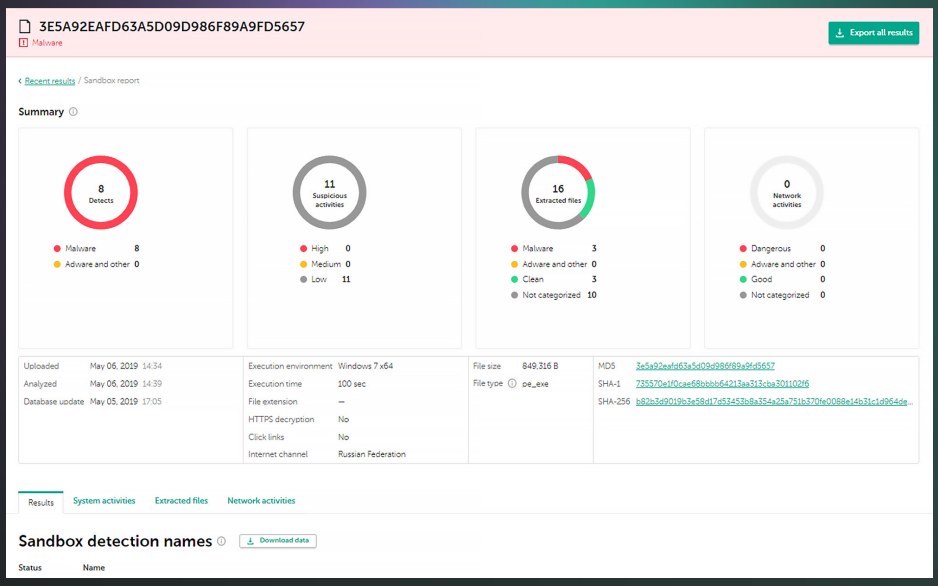
Проактивное выявление вредоносных программ

При выполнении вредоносных программ используются различные методы сокрытия от обнаружения. Если система жертвы не отвечает определенным критериям, вредоносная программа самоуничтожится, не оставив следов. Для выявления вредоносного кода песочница должна уметь точно имитировать поведение обычного пользователя.

В изолированной среде проводится поведенческий анализ и используются надежные методы блокировки обхода безопасности. Также песочница применяет технологии моделирования поведения человека, такие как автокликер, прокрутка документов и другие действия.

Облачная песочница от «Лаборатории Касперского» объединяет все знания о поведении вредоносных программ, полученные за более чем 20 лет непрерывного исследования угроз, что позволяет обнаруживать более 300 000 новых вредоносных объектов каждый день.

Kaspersky Cloud Sandbox является важным компонентом для анализа угроз. В рамках сервиса Kaspersky Threat Lookup собираются подробные актуальные сведения об угрозах: веб-адреса, домены, IP-адреса, хеши файлов, названия угроз, статистические и поведенческие данные, данные WHOIS/DNS и прочие. Облачная песочница для исследований позволяет связать эти данные с индикаторами компрометации, сгенерированными анализируемым образцом.



Благодаря Cloud Sandbox можно провести высокоэффективное сложное расследование инцидентов, сразу понять характер угрозы и объединить собранные в ходе расследования данные в общую картину, выявляя взаимосвязанные индикаторы угрозы.

Облачная песочница сокращает время реагирования на инциденты и повышает эффективность криминалистического расследования, обеспечивая масштабируемость при автоматической обработке файлов без необходимости покупать дорогостоящие устройства и беспокоиться о системных ресурсах.

Аналитические отчеты об APT-угрозах

Получатели аналитических отчетов об APT-угрозах имеют уникальный постоянный доступ к исследованиям и открытиям «Лаборатории Касперского», включая полные технические данные (в различных форматах) о каждой обнаруженной APT. Отчеты содержат ориентированную на руководство и легкую для понимания информацию, описывающую APT-угрозы, а также подробные технические данные об APT-угрозах с соответствующими индикаторами компрометации и правилами YARA, чтобы предоставить исследователям безопасности, аналитикам вредоносных программ, инженерам по безопасности и другим ИБ-аналитикам данные, позволяющие быстро и точно отреагировать на угрозу.

Специалисты «Лаборатории Касперского» также немедленно сообщают обо всех обнаруженных изменениях в тактиках киберпреступных групп. У вас также будет доступ к полной базе данных отчетов об APT-угрозах – еще одному мощному компоненту исследования и анализа.

Преимущества

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.

Информация о непубличных APT-угрозах

По разным причинам не все громкие угрозы становятся известны широкой публике. Но мы предоставляем такую информацию нашим клиентам.

Эксклюзивные данные

Доступ к техническим описаниям новейших угроз уже в ходе расследования, до публичного объявления.

Ретроспективный анализ

В течение срока действия подписки доступны все ранее выпущенные закрытые отчеты.

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.

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.

Непрерывный мониторинг APT-кампаний

Доступ к оперативной информации о распространении APT-угроз, во время расследования.

Поддержка RESTful API

Беспрепятственная интеграция и автоматизация процессов безопасности.

Kaspersky Digital Footprint Intelligence
Набор персонализированной аналитики угроз

Компаниям доступно множество защитных инструментов, однако некоторые задачи по-прежнему вызывают трудности, например отслеживание киберпреступных планов и схем на форумах даркнета. Чтобы аналитики по безопасности могли оценивать корпоративную среду с точки зрения злоумышленников, быстро выявлять возможные векторы атак и тут же адаптировать защиту, «Лаборатория Касперского» разработала сервис Kaspersky Digital Footprint Intelligence.

Как лучше всего организовать атаку на вашу организацию? Как провести ее с наименьшими затратами? Какие сведения доступны злоумышленнику, решившему атаковать вашу компанию? Возможно, ваша инфраструктура уже взломана без вашего ведома?

Kaspersky Digital Footprint Intelligence отвечает на эти и другие вопросы. Эксперты «Лаборатория Касперского» формируют полную картину текущей ситуации с угрозами, выявляют уязвимости в защите и признаки прошедших, текущих и даже планируемых атак.

На основе общедоступных источников информации (OSINT), автоматического и ручного анализа интернета, даркнета и глубокой сети, а также внутренней базы знаний «Лаборатории Касперского» составляются персонализированные отчеты. Они содержат **аналитические данные и рекомендации**, которые позволяют сократить количество потенциальных векторов атаки и цифровые риски для организации. Сервис Kaspersky Digital Footprint Intelligence включает следующие возможности:

- Инвентаризация периметра сети неинтрузивными методами, чтобы определить сетевые ресурсы и уязвимые сервисы клиента, которые могут служить точкой входа для атаки: случайно оставленные в периметре интерфейсы управления, неправильно сконфигурированные сервисы, интерфейсы устройств и т. д.
- Персонализированный анализ существующих уязвимостей с последующим ранжированием и комплексной оценкой рисков на основе системы CVSS, доступности публичных эксплойтов, результатов тестирования на проникновение и сведений о размещении сетевых ресурсов (хостинг/инфраструктура).
- Выявление, мониторинг и анализ любых активных или планируемых целевых атак, APT-кампаний, направленных на организацию, отрасль или регион.
- Выявление угроз, направленных на клиентов, партнеров и абонентов. Их зараженные системы могут быть использованы для атаки на компанию.
- Скрытое наблюдение за сайтами, публичными форумами, социальными сетями, каналами обмена мгновенными сообщениями, подпольными форумами и сообществами для выявления скомпрометированных учетных записей, утечки информации и обсуждения атак на организацию.

Инвентаризация

- Доступные сервисы
- Цифровые отпечатки в сервисах
- Выявление уязвимостей
- Анализ эксплойтов
- Оценка и анализ рисков

Интернет, даркнет и глубокая сеть

- Активность киберпреступников
- Утечки информации и учетных данных
- Инсайдеры
- Поведение сотрудников в социальных сетях
- Утечки метаданных

База знаний «Лаборатории Касперского»

- Анализ экземпляров вредоносных программ
- Отслеживание ботнетов и фишинга
- Sinkhole-серверы и серверы с вредоносным ПО
- Аналитические отчеты об APT-угрозах
- Потоки данных об киберугрозах

Неструктурированные данные:

- IP-адреса
- Домены компании
- Бренды
- Ключевые слова

Инвентаризация периметра сети

Интернет, даркнет и глубокая сеть

База знаний «Лаборатории Касперского»

Машиночитаемые форматы аналитики угроз

Аналитические отчеты

Мгновенные уведомления об угрозах

Отчеты об угрозах для АСУ ТП

В рамках отчетов об угрозах для АСУ ТП «Лаборатория Касперского» предоставляет подробные аналитические данные о вредоносных кампаниях, нацеленных на промышленные организации, и об уязвимостях, обнаруженных в наиболее популярных АСУ ТП и их технологиях.

Что входит в сервис?

Отчеты об APT-атаках. Отчеты о новых APT-атаках и масштабных кампаниях против промышленных организаций и обновленные данные об активных угрозах.

Обнаруженные уязвимости. Отчеты об уязвимостях, обнаруженных «Лабораторией Касперского» в наиболее популярных продуктах для АСУ ТП, промышленном интернете вещей и IT-инфраструктуре различных отраслей.

Ландшафт угроз. Отчеты о значительных изменениях в ландшафте угроз для АСУ ТП и новых критических факторах, которые влияют на уровень безопасности и уязвимости таких систем, с разделением по регионам, странам и отраслям.

Анализ и минимизация уязвимостей. Эксперты «Лаборатории Касперского» дают практические рекомендации по выявлению и минимизации уязвимостей в инфраструктуре предприятия.

Данные анализа угроз позволяют

Выявлять и предотвращать

угрозы для критически важных устройств, включая программное и аппаратное обеспечение, чтобы обеспечить безопасность и непрерывность производственного процесса.

Сопоставлять

вредоносную и подозрительную активность, обнаруженную в промышленной среде, с результатами исследований «Лаборатории Касперского», чтобы связать эту активность с вредоносными кампаниями, определить угрозы и оперативно отреагировать на них.

Оценивать

уязвимости производственной среды и устройств на основе точных сведений о масштабах и серьезности обнаруженных проблем и принять обоснованные решения по установке исправлений и другим рекомендованным профилактическим мерам.

Использовать

информацию о тактиках, техниках и процедурах атак, недавно обнаруженных уязвимостях и других важных изменениях ландшафта угроз.

Преимущества

Обеспечение глобальной видимости и своевременного обнаружения киберугроз, приоритизация предупреждений безопасности и эффективное реагирование на инциденты.

Предотвращение выгорания аналитиков и привлечение внимания сотрудников к реальным угрозам.

Понимание тактик, техник и процедур, используемых злоумышленниками в разных отраслях и регионах, для проактивной защиты от целевых и сложных угроз.

Сокращение время реагирования на атаки и минимизация возможного ущерба от них благодаря широким возможностям расследования и проактивного поиска угроз.

Заключение

Противодействие современным киберугрозам тесно связано с пониманием полной картины тактик, техник и процедур, используемых злоумышленниками. Получение этой информации и определение наиболее эффективных контрмер требует постоянной самоотдачи и высокого уровня знаний. Обладая петабайтами подробных данных об угрозах, «Лаборатории Касперского» предоставляет клиентам достоверные аналитические данные об угрозах со всего мира, помогая обеспечивать защиту даже от ранее неизвестных кибератак.

Узнать подробнее о сервисах Kaspersky Threat Intelligence

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования внешних сервисов анализа угроз (Forrester Wave: External Threat Intelligence Services, 2021)

Запросить тестовый доступ к сервисам Kaspersky Threat Intelligence

Отправить заявку

www.kaspersky.ru