Потоки данных об угрозах

Kaspersky Threat Data Feeds

kaspersky активируй будущее

Kaspersky Threat Data Feeds

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.

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.

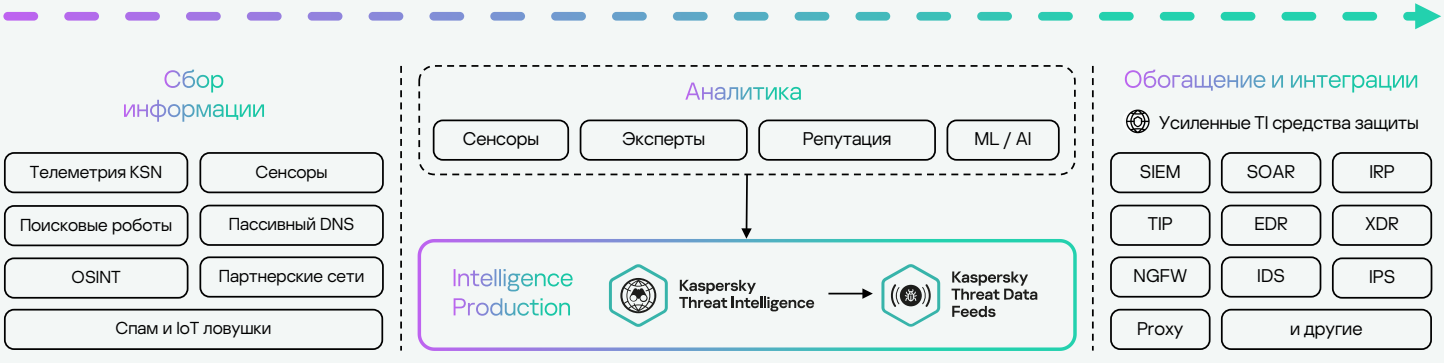
Потоки данных об угрозах — это сервис «Лаборатории Касперского», предоставляющий компаниям информацию об угрозах для защиты их инфраструктуры. В рамках данного сервиса предоставляется информация об известных вредоносных программах, фишинговых веб-сайтах, последних уязвимостях и эксплойтах, а также других 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 Threat Data Feeds

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее