Kaspersky Threat Data Feeds

kaspersky АКТИВИРУЙ БУДУЩЕЕ

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 тактику и методы. 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.

Запрос пробного доступа к Kaspersky Threat Data Feeds

Подробнее

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

Потоки данных генерируются автоматически в режиме реального времени на основе данных, собираемых по всему миру (в сеть Kaspersky Security Network входят десятки миллионов конечных пользователей более чем из 213 стран, что позволяет отслеживать значительный объем интернет-трафика). Это обеспечивает точность и высокую скорость обнаружения.

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

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.

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.

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.

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

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

Ценность

Повышение эффективности решений для защиты сети, включая SIEM-системы, межсетевые экраны, системы обнаружения и предотвращения вторжений, прокси-серверы, решения для служб DNS и технологии противодействия APT-угрозам с помощью интеграции с постоянно обновляемыми потоками данных. Эти потоки данных содержат актуальные индикаторы компрометации с дополнительными контекстными данными, что позволяет вовремя обнаруживать кибератаки и лучше понимать намерения, возможности и цели злоумышленников. Поддерживаются ведущие SIEM-системы (HP ArcSight, IBM QRadar, Splunk и прочие) и платформы анализа угроз.

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.

Предотвращение утечки конфиденциальных данных и интеллектуальной собственности с зараженных устройств за пределы организации. Предотвращение утечки конфиденциальных данных и интеллектуальной собственности с зараженных устройств за пределы организации.

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

Kaspersky Threat Intelligence

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования внешних сервисов анализа угроз (Forrester Wave™: External Threat Intelligence Services, Q1 2021)

«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

Подробнее

www.kaspersky.ru