Аналитические отчеты
об угрозах для организации

Kaspersky Digital Footprint Intelligence

kaspersky активируй будущее

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 Intelligence Reporting

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее