



Всесторонняя защита ваших
активов от цифровых рисков

Kaspersky Digital Footprint Intelligence

Вопросы для экспертов

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 «Лаборатории Касперского» формируют полную картину текущей обстановки с угрозами предприятию, выявляют уязвимости в защите и признаки прошедших, текущих и даже планируемых атак.

Kaspersky Digital Footprint Intelligence

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).



Защита бренда

Мониторинг и блокировка несанкционированного использования бренда компании в сети. Выявление поддельных учетных записей и приложений в социальных сетях, фишинговых веб-сайтов и других мошеннических действий, которые могут нанести ущерб репутации компании или обмануть ее клиентов.



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, АРТ-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).

Принцип работы



Конфигурация

Инвентаризация всех цифровых активов компании

Сбор данных

Автоматизированный сбор данных из глубокого Интернета, даркнета и темного веба, а также из базы знаний «Лаборатории Касперского»

Фильтрация

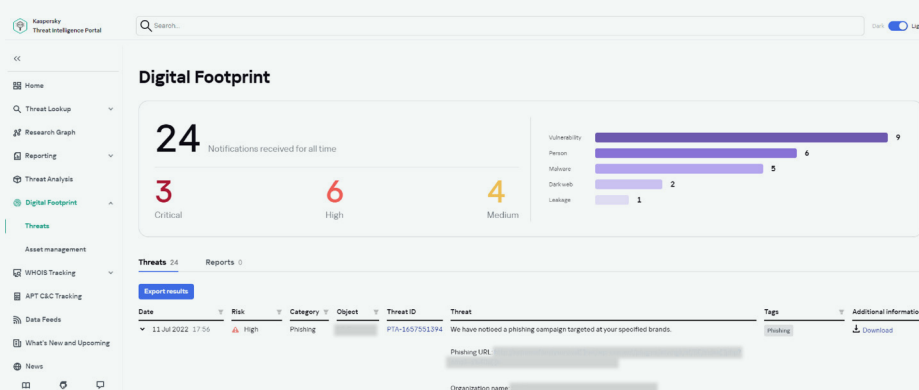
Обнаружение угроз, их анализ и приоритезация под управлением аналитиков

Реакция

Предоставление уведомлений, отчетов и вариантов реагирования на угрозы

Вы получите

- Оповещения об угрозах на портале Threat Intelligence Portal
- Аналитические отчеты, подготовленные нашими экспертами
- Машиночитаемые данные
- Запросы на поиск информации в даркнете
- Запросы на поиск информации в социальных сетях
- Запросы на блокирование вредоносных и мошеннических ресурсов
- Презентации и сессии вопросов и ответов с экспертами



Типы угроз

Kaspersky Digital Footprint Intelligence позволяет организациям быстро и эффективно реагировать на потенциальные угрозы с помощью уведомлений в режиме реального времени и возможностей устранения. Это снижает вероятность нанесения ущерба репутации бренда, потери доверия клиентов и остановки бизнес-операций в целом.

Угрозы, связанные с сетевым периметром

- Неправильно настроенные сетевые службы
- Незакрытые уязвимости
- Поврежденные или скомпрометированные ресурсы

Угрозы, связанные с даркнетом

- Схемы мошенничества и планы киберпреступников
- Украденные кредитные карты и взломанные аккаунты
- Инсайдерская деятельность

Угрозы, связанные с вредоносным ПО

- Фишинговые атаки
- Деятельность ботнетов
- Целевые атаки
- АРТ-кампании

Утечки данных

- Открытый доступ к корпоративным документам
- Активность сотрудников в социальных сетях
- Скомпрометированные учетные данные

Неправомерное использование бренда

- Поддельные веб-сайты
- Поддельные мобильные приложения (в Google Play и AppStore)

Источники

Крайне важно, чтобы вы имели полное представление о потенциальных угрозах для вашей компании. Для предоставления этих сведений аналитики безопасности «Лаборатории Касперского» собирают и обобщают информацию из следующих источников.

Неструктурированные данные

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

Инвентаризация сетевого периметра

Публичные источники и ресурсы даркнета

База знаний «Лаборатории Касперского»

Аналитические отчеты
Мгновенные уведомления об угрозах в Threat Intelligence Portal

10 запросов на устранение в год
Запросы на поиск по базе знаний «Лаборатории Касперского», тематическим ресурсам и ресурсам даркнета и темного веба

Бизнес-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.



Оптимизация затрат

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



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.



Вскрытие замыслов злоумышленников

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



Дополнительная экспертиза

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

Чтобы узнать больше о сервисе и вариантах подписки, свяжитесь с нашей командой:

Связаться



Kaspersky Digital Footprint Intelligence

[Подробнее](#)

www.kaspersky.ru

© 2023 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки
обслуживания являются собственностью
их правообладателей.

[#kaspersky](#)
[#активируйбудущее](#)