GROUP-IB

THREAT INTELLIGENCE

Преимущества Group-IB

Уникальные источники данных

Максимально полное представление о ландшафте угроз за счет самого обширного набора источников данных кибербразведки на рынке, непрерывно собираемых системой Unified Risk Platform от Group-IB.

Широкий спектр возможностей

Возможность получить максимально полную информацию, вооружив команду безопасности решением с самым обширным набором исследовательских инструментов и команд аналитиков на рынке.

Доверие партнеров по сектору

Group-IB – единственная компания в сфере кибербезопасности, у которой заключены соглашения о сотрудничестве с Interpol, Europol и правоохранительными органами по всему миру, направленные на противодействие злоумышленникам и установление их личностей.

Неограниченный доступ

Снижение издержек и устранение потенциальных узких мест системы безопасности благодаря отсутствию ограничений на количество пользователей и использований API. Команда Group-IB всегда готова оказать клиентам поддержку.

Комплексный пакет решений

Для обеспечения всесторонней защиты Unified Risk Platform также предоставляет функционал решений Attack Surface Management, Digital Risk Protection и Managed XDR.

Инфраструктура организации не должна быть первым рубежом на пути атакующих. Усовершенствуйте свою систему безопасности и проактивно предотвращайте атаки до того, как они произойдут, благодаря знаниям о злоумышленниках, их методах и намерениях.

Решение Threat Intelligence от Group-IB предоставляет уникальные сведения по всем атакующим, нацеленным на вашу компанию. Интеграция данных кибербразведки позволяет добиться максимальной эффективности каждого из компонентов экосистемы безопасности. Предоставив в распоряжение вашей команды безопасности уникальные стратегические, операционные и тактические данные кибербразведки от Group-IB, вы тем самым оптимизируете рабочие процессы и повысите эффективность системы ИБ.

Стратегические данные

- Новый уровень управления рисками благодаря персонализированным отчетам об угрозах, которые составляются аналитиками по запросу, ежемесячно или ежеквартально специально для презентации бизнес-кейсов высшему руководству компании
- Обеспечение роста компании с помощью значимых данных кибербразведки по регионам и отраслям. Данные об угрозах позволяют снизить риски в случае расширения деятельности в новых регионах, открытия нового направления бизнеса или проведения цифровой трансформации
- Снижение затрат на обеспечение безопасности за счет отказа от необязательных закупок и переноса усовершенствований на более поздние сроки благодаря максимизации эффективности уже имеющихся решений

Оперативные данные

- Трансформация системы безопасности и максимально быстрая адаптация к изменениям. Использование аналитической информации позволяет блокировать вредоносную активность в сетях и на хостах сразу после того, как она была зафиксирована где-либо в мире
- Выявление и устранение уязвимостей еще до того, как их удалось использовать злоумышленникам, за счет обогащения знаний вашей Red Teaming-команды подробной информацией о тактиках, техниках и процедурах атакующих
- Автоматизация рабочих процессов и повышение эффективности вашей команды за счет обогащения SIEM-, SOAR- и EDR-систем и платформ по управлению уязвимостями готовыми API-интеграциями с поддержкой TAXII и STIX

Тактические данные

- Приоритизация устранения уязвимостей для всего стека технологий за счет автоматизации оповещений, которые отправляются в момент обнаружения уязвимости или ее эксплуатации злоумышленниками, атакующими предприятия вашей отрасли
- Фильтрация ложноположительных срабатываний и возможность сфокусироваться на событиях с критическим уровнем риска благодаря подробной и постоянно обновляющейся информации об индикаторах компрометации по киберпреступникам, относящимся к вашему ландшафту угроз
- Сокращение времени реагирования и быстрое устранение атакующих из вашей сети благодаря данным об используемых злоумышленниками методах атаки (Cyber Kill Chain), представленных в формате матрицы MITRE ATT&CK®

Ключевые функции

Инструмент графового анализа

Исследование угроз при помощи интуитивно понятного интерфейса. Система графового анализа позволяет моментально проследить связи между злоумышленниками, их инфраструктурой и инструментами, а также одним кликом получить доступ к детализированной информации.

Детектирование скомпрометированных данных

Обнаружение скомпрометированных учетных данных (включая личные аккаунты VIP-персон, банковские карты, утекшие базы данных) до того, атакующие используют их для проведения атак или нанесения финансового ущерба. Создание оповещений об обнаружении релевантных для организации скомпрометированных данных при помощи системы Threat Intelligence.

Данные из Darkweb

Использование самой обширной базы данных Darkweb среди всех компаний в области кибербезопасности за счет Unified Risk Platform. Доступ к данным киберразведки, обнаружение нелегальной активности в сети и отслеживание упоминаний организации в андеграунде благодаря решению Threat Intelligence. Создание правил для получения оповещений об опубликованных сообщениях на интересующие темы.

Обнаружение фишинга и реагирование

Автоматическое обнаружение и блокировка вредоносных сайтов для защиты брендов и клиентов организации за счет настройки Unified Risk Platform через Group-IB Threat Intelligence. Рекордно быстрая блокировка фишинговых сайтов и сведение к минимуму причиненного организации ущерба благодаря отлаженным рабочим процессам центра реагирования на инциденты Group-IB (CERT-GIB).

Атрибуция злоумышленников

Возможность быстро составить представление о поведении злоумышленников, узнать, какие методы и какую инфраструктуру они используют в своих атаках, а также получить информацию об их активности в формате матрицы MITRE ATT&CK. Unified Risk Platform отслеживает и фиксирует действия атакующих в реальном времени, а Group-IB Threat Intelligence предоставляет пользователям быстрый и удобный доступ к этим данным.

Исследование вредоносного ПО и уязвимостей

Детонация подозрительных файлов через Unified Risk Platform или передача их команде Group-IB по реверс-инжинирингу для исследования при помощи Threat Intelligence. Просмотр на дашборде результатов углубленного анализа тех уязвимостей, которые стали мишенью определенных ВПО и злоумышленников, для выделения приоритетных задач по устранению слабых звеньев в системе защиты.

Персонализированный ландшафт угроз

Простое и удобное отслеживание действий злоумышленников в виде матрицы – «Ландшафта угроз». Мониторинг информации о тех, кто атакует компанию, партнеров и клиентов, отрасль или чья активность представляет интерес.

Широкие возможности интеграции

Повышение эффективности существующей экосистемы информационной безопасности за счет готовых интеграций Unified Risk Platform с популярными SIEM-, SOAR- и TIP- решениями, а также передача данных в любые элементы экосистемы через API с поддержкой STIX и TAXII.

Unified Risk Platform собирает данные кибер-разведки из широкого спектра источников

Open-source intelligence

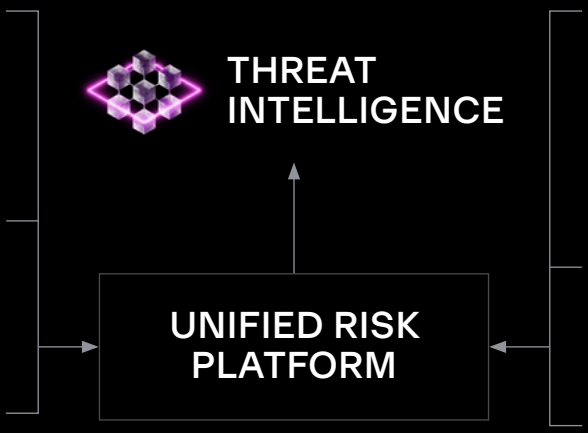
- Paste-сайты
- Репозитории исходного кода
- Данные об уязвимостях и эксплойтах
- Обсуждения в социальных сетях
- Сервисы для обмена ссылками и их продвижения

Malware intelligence

- Платформа детонации ВПО
- Эмуляторы ВПО
- Извлечение конфигурационных файлов ВПО
- Общедоступные песочницы

Sensor intelligence

- Сетевые сенсоры на уровне ISP
- Honeypot-сеть
- Сканеры IP-адресов
- Веб-краулеры



Human intelligence

- Реверс-инжиниринг ВПО
- Внедрение на подпольные форумы и сообщества в Darkweb
- Сервисы компьютерной криминалистики и аудита
- Совместные операции с правоохранительными органами
- Региональные специалисты

Vulnerability intelligence

- Список CVE
- Репозиторий эксплойтов
- Обсуждения на даркнет-форумах
- Использование в текущих

Data intelligence

- Анализ C&C-серверов злоумышленников
- Darkweb форумы
- Darkweb маркетплейсы
- Мониторинг мессенджеров
- Фишинг-киты и ВПО
- Анализаторы скомпрометированных данных
- Точки сбора данных с фишинговых страниц

Совместные операции с органами правопорядка

Благодаря сотрудничеству с органами правопорядка по всему миру, включая Interpol и Europol, специалисты Group-IB расширили свою экспертизу и овладели лучшими практиками, а также получили доступ к данным, которые никогда не находились в общем доступе.