Group-IB

THREAT INTELLIGENCE & ATTRIBUTION

Система исследования и атрибуции кибератак, проактивной охоты за угрозами и защиты сетевой инфраструктуры на основании данных о тактиках, инструментах и активности злоумышленников

Управление ландшафтом угроз

Высокотехнологичные инструменты анализа

Уникальные закрытые источники

GROUP IB

Возможности Group-IB Threat Intelligence & Attribution

Обнаруживать и предотвращать атаки

Предотвращение угроз, которые пропускают традиционные средства защиты

Понимать методы продвинутых атакующих

Оценка возможностей защищаемой инфраструктуры противостоять релевантным TTPs

Обнаруживать инсайдеров и утечки данных

Поиск скомпрометированных пользователей или клиентов для предотвращения ущерба

Выявлять и блокировать фишинг

Фишинг, нацеленный на компанию или клиентов, неправомерно использующий бренд

Анализировать и атрибутировать угрозы

Обогащение индикаторов, полученных из других систем, уникальной информацией

Усиливать, совершенствовать и обучать команды

Снижение издержек и привлечение экспертов для повышения эффективности команды на 30%

Ключевые особенности:

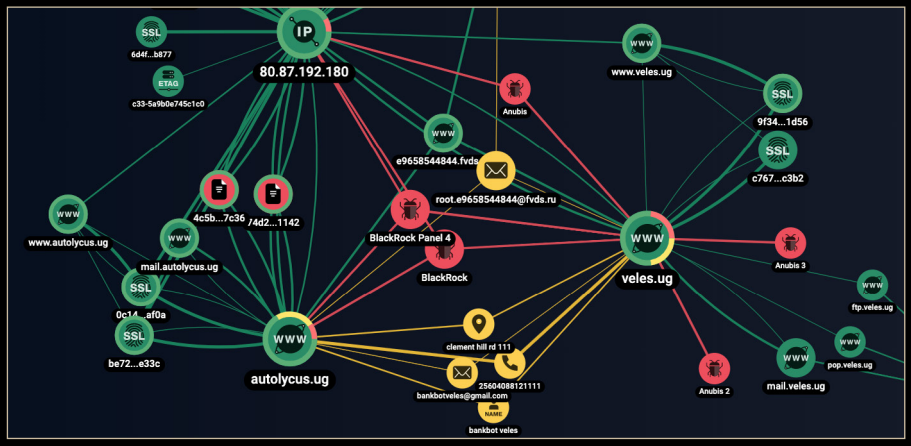
1. Возможность создавать ландшафт угроз и управлять им
2. Продвинутая модель профилирования киберпреступников и спецслужб
3. Доступ к уникальным данным и закрытым источникам
4. Максимальная релевантность и персонализация данных для компании и отрасли
5. Извлечение данных компании, утекших после фишинговой атаки или работы трояна
6. Готовая интеграция через API с SIEM, TIPs и другими системами

Доступ к уникальным аналитическим инструментам

Поиск по крупнейшей, собранной за годы коллекции данных из DarkWeb

Детонация и анализ вредоносного ПО в Malware Detonation Platform

Автоматизированный граф для корреляции и обогащения данных, атрибуции угроз



Источники данных

Human Intelligence

- Внедрение на подпольные форумы и сообщества в DarkWeb;
- Реагирование на инциденты, компьютерная криминалистика и совместные операции с международными правоохранительными органами;
- Реверс-инженеры, аналитики ВПО, аналитики TI с многолетним опытом;
- Обмен информацией в рамках сообщества, собственный сертифицированный CERT-GIB.

Malware Intelligence

- Сетевые сенсоры на уровне ISP;
- Group-IB Threat Hunting Framework
- Group-IB Fraud Hunting Platform (собственное антифрод-решение);
- Honeypot-сеть; SPAM-traps; Sinkholing;
- Эмуляторы вредоносного ПО;
- Система для глобальной охоты за угрозами, обнаружения инфраструктуры злоумышленников и получения данных об угрозах.

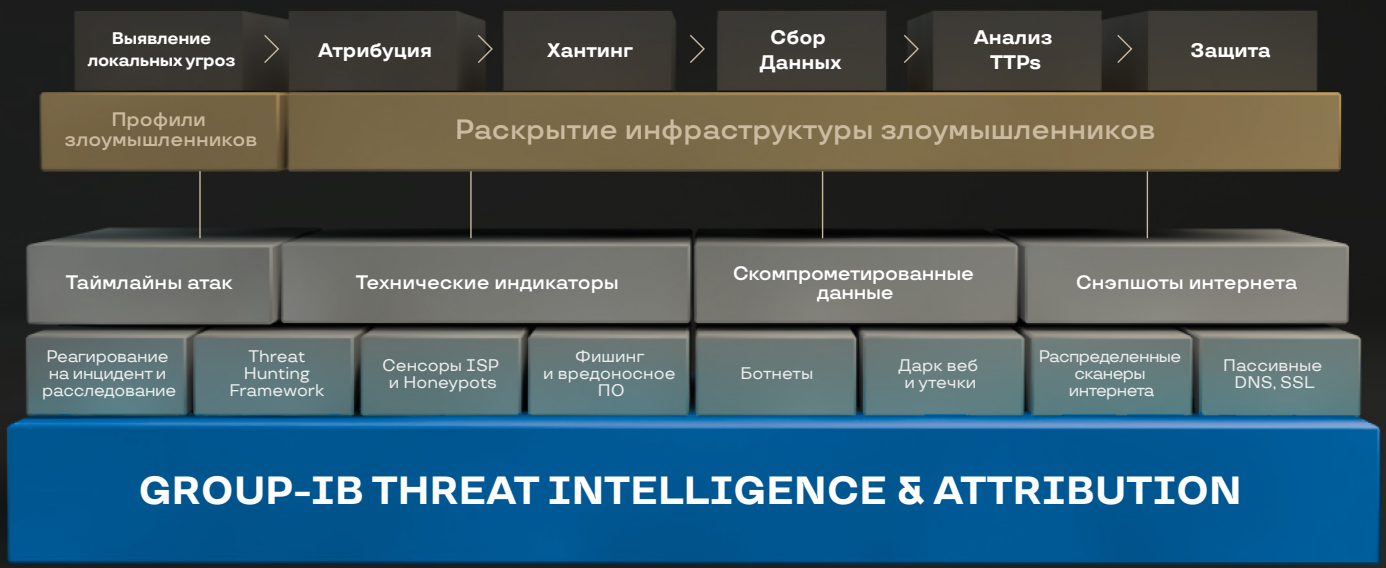
Data Intelligence

- Анализ командных серверов злоумышленников (botnet и фишинг);
- Анализ командных серверов JS-снифферов;
- Узлы сбора данных фишинговых страниц;
- Анализ конфигурации систем «автозалива»;
- Система проверки скомпрометированных данных.

Open Source Intelligence

- Хостинги контента (текстов и кода, например, Pastebin);
- Репозитории кода (Git);
- Telegram, социальные сети;
- Данные об уязвимостях и эксплойтах;
- Сервисы для продвижения и обмена ссылками.

Архитектура Group-IB Threat Intelligence & Attribution



Group-IB один из ведущих мировых разработчиков решений для детектирования и реагирования на кибератаки, предотвращения мошенничества и защиты интеллектуальной собственности в сети

Group-IB входит в число лучших мировых поставщиков решения класса Threat Intelligence по версии Gartner, IDC, Forrester, SC Media и Cyber Defenses Magazine.

Эксперты Group-IB проводят тренинги по кибербезопасности для специалистов Europol, INTERPOL, правоохранительных органов, корпоративных команд и преподавателей университетов в Европе и Азии.

INTERPOL EUROPOL

Официальный партнер

17 лет	65 000+	1 200+	500+
практического опыта	часов опыта реагирования	расследований по всему миру	специалистов и разработчиков

→

Узнайте больше о возможностях Threat Intelligence & Attribution

info@group-ib.com

→

Познакомьтесь с Group-IB

group-ib.ru
twitter.com/GroupIB_GIB

→

Узнайте больше о Threat Intelligence & Attribution

Сервисы Group-IB

Укрепите кибербезопасность с помощью специалистов с практическим опытом реагирования и расследования сложных атак, использующих одну из самых продвинутых в мире систем слежения за киберугрозами.

Аудит и оценка рисков

- Тестирование на проникновение
- Анализ исходного кода
- Выявление следов компрометации сети
- Киберобучения в формате Red Teaming
- Проверка готовности к реагированию на инциденты
- Оценка соответствия

Обучающие программы

- Реагирование на инциденты
- Анализ вредоносного кода
- Проактивный поиск угроз

Threat Hunting и реагирование

- 24/7 Центр реагирования CERT-GIB
- Охота за угрозами
- Выездное реагирование на сложные кибератаки
- Реагирование на инциденты «по подписке»

Криминалистика и расследования

- Компьютерная криминалистика
- Расследование финансовых и корпоративных киберпреступлений, атак на объекты КИИ