



ATTACK SURFACE MANAGEMENT

Управление поверхностью атаки с помощью данных киберразведки

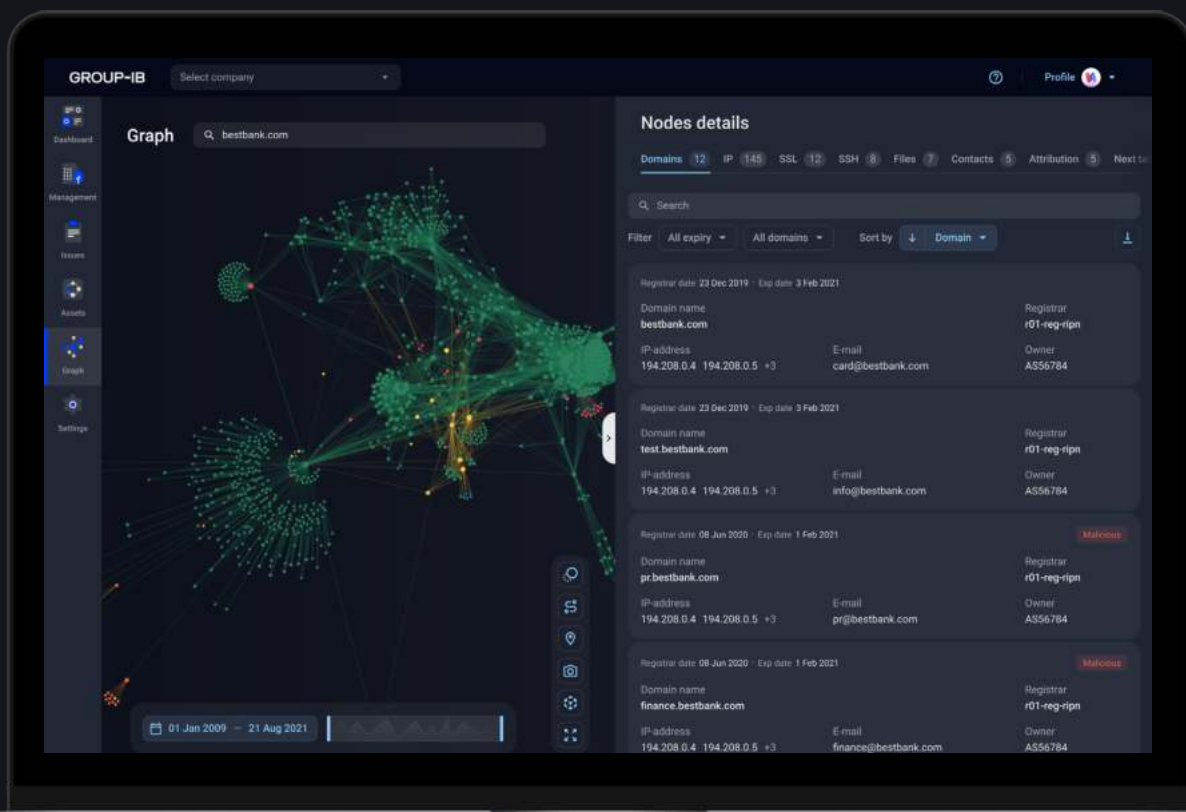
Полная картина внешней поверхности атаки

и уникальные данные для повышения уровня защищенности

Как правило, проникновения в корпоративные сети не связаны с эксплуатацией уязвимостей нулевого дня или использованием сложных инструментов.

Большинство взломов происходит из-за многочисленных неотслеживаемых уязвимостей периметра, таких как непропатченные серверы, некорректные конфигурации баз данных и неконтролируемые теневые ИТ.

Attack Surface Management – это комплексное и основанное на данных киберразведки SaaS-решение, позволяющее организациям оценивать поверхность атаки и управлять ею. Решение обеспечивает полную инвентаризацию всех интернет-ресурсов организации, выявляет уязвимости и приоритезирует критические риски для принятия должных мер.



Функционал и преимущества решения

Полная прозрачность

Не ограничиваясь сканированием пространства IPv4, Attack Surface Management выявляет и индексирует все ресурсы организации, включая теневые ИТ.

Максимальное покрытие

Attack Surface Management отслеживает все доступные извне ресурсы организации, включая локальные, облачные и гибридные решения.

Надёжная защита

Управление внешней поверхностью атаки позволяет предотвратить необязательные риски и повысить уровень защищённости организации.

Обогащение контекстом

Всем проиндексированным ресурсам присваивается уровень риска, позволяющий приоритезировать действия по устранению уязвимостей.

Данные из уникальных источников

Attack Surface Management – единственное решение для управления внешней поверхностью атаки, которое обогащается данными из бот-нетов, исследований вредоносных программ и дарквеба.

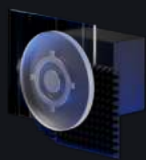
Быстрое начало работы

Attack Surface Management представляет собой безагентное облачное SaaS-решение, которое не требует установки ПО для начала работы.

Обнаружение критических рисков

в режиме реального времени для предотвращения угроз

ЕЖЕДНЕВНЫЙ
МОНИТОРИНГ ВСЕХ
ИЗМЕНЕНИЙ ВНЕШНЕЙ
ПОВЕРХНОСТИ АТАКИ



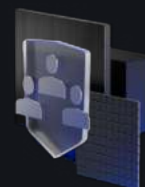
ВЫЯВЛЕНИЕ ТЕНЕВЫХ
ИТ И НЕКОРРЕКТНЫХ
КОНФИГУРАЦИЙ



ОЦЕНКА УРОВНЯ
ЗАЩИЩЕННОСТИ
С ПОМОЩЬЮ
УНИКАЛЬНОЙ
ИНФОРМАЦИИ
ИЗ ДАРКВЕБА



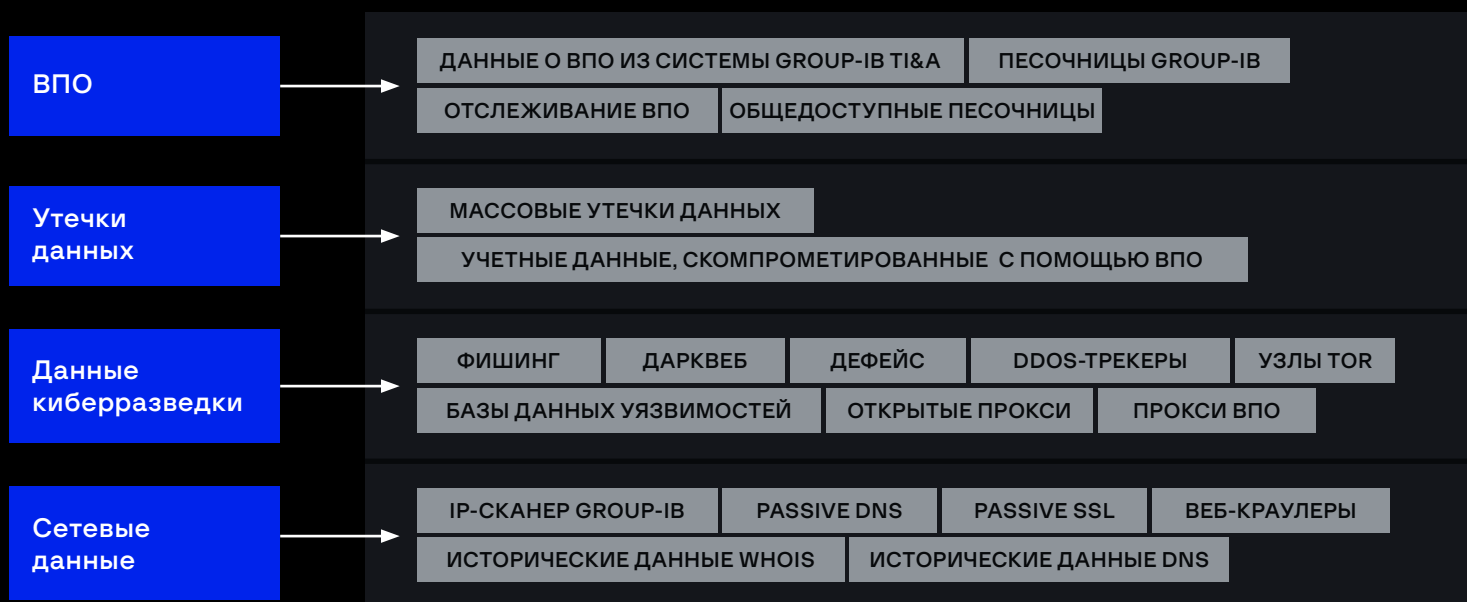
ПРОВЕРЕННЫЕ
АКТУАЛЬНЫЕ
ДААННЫЕ ДЛЯ
ПОВЫШЕНИЯ УРОВНЯ
ЗАЩИЩЕННОСТИ



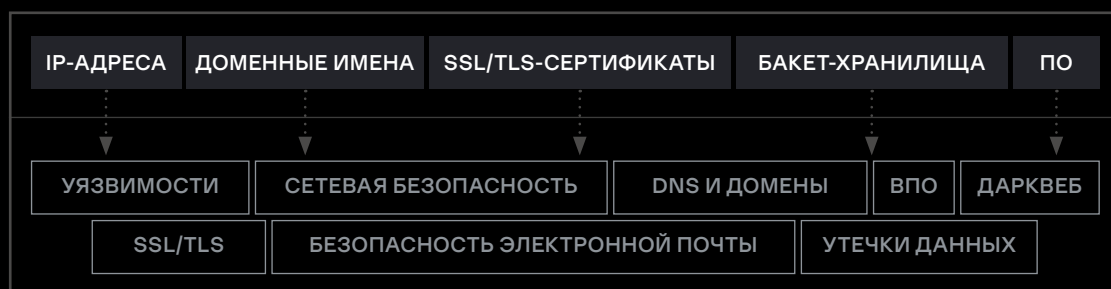
Attack Surface Management ВЫХОДИТ за рамки стандартных услуг и продуктов

Attack Surface Management превосходит существующие решения для управления внешней поверхностью атак благодаря запатентованным технологиям и данным киберразведки.

Непрерывное сканирование



Внешняя поверхность атаки



Обогащение контекстом

Уникальные данные из признанной международными агентствами системы Group-IB Threat Intelligence & Attribution, распределенные по 8 категориям

Значимая информация

Оповещения о потенциальных проблемах, отслеживание изменений и отчеты, позволяющие предпринять эффективные действия

Непрерывный мониторинг

Постоянно обновляемые данные дают полный контроль над поверхностью атаки и ее уязвимостями

Устранение слепых зон инфраструктуры

Индексация ресурсов

Комплексный подход к мониторингу ресурсов организации

Выявление угроз

Исчерпывающий список уязвимостей с разбивкой по категориям ресурсов и уровню риска







Управление рисками и устранение недостатков

Количественная оценка рисков для приоритизации задач по повышению защищенности



Уникальные возможности

Запатентованные технологии Group-IB, лежащие в основе Attack Surface Management

 Web & Internet snapshot generator	 Network graph analysis	 Malware config extractor	 Malware protocol emulator
 Phishing predictor	 Botnet data extractor	 Dark Web scraping engine	 Vulnerability detector engine

Group-IB — международная компания по кибербезопасности

<p>1 300+</p> <p>успешных расследований высокотехнологичных преступлений</p>	<p>600+</p> <p>сотрудников</p>	<p>450+</p> <p>корпоративных клиентов</p>	<p>60+</p> <p>стран по всему миру</p>
<p>11</p> <p>ключевых сервисов</p>	<p>6</p> <p>продуктов</p>	<p>120+</p> <p>патентов и заявок на патенты</p>	<p>4</p> <p>региона с Центрами исследований: Сингапур, Нидерланды, ОАЭ и Россия</p>

Партнер и участник совместных расследований

Решения Group-IB признаны мировыми агентствами



Услуги на основе данных киберразведки

Предотвращение

- Аудит безопасности
- Оценка соответствия
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Киберобразование

Реагирование

- Реагирование на инциденты
- Сервис по охоте за угрозами
- Сервис обнаружения и реагирования

Исследование

- Компьютерная криминалистика
- Исследование

Технологии и инновации

Кибербезопасность

- Threat Intelligence
- Управление поверхностью атаки
- Защита электронной почты
- Анализ сетевого трафика
- Детонация ВПО
- Защита конечных станций (EDR)
- XDR

Противодействие мошенничеству

- Противодействие мошенничеству client-side
- Адаптивная аутентификация
- Защита от ботов
- Выявление платежного мошенничества
- Поведенческий анализ

Защита бренда

- Антифишинг
- Антипиратство
- Антимошенничество
- Антиконтрафакт
- Выявление утечек данных
- Защита VIP-персон



GROUP-IB

FIGHT AGAINST CYBERCRIME

Предотвращение и исследование
киберпреступлений с 2003 года