GROUP-IB

GROUP-IB MANAGED XDR

Круглосуточный мониторинг, проактивный поиск недетектируемых угроз и своевременное реагирование на них

ОБЗОР ПРОДУКТА

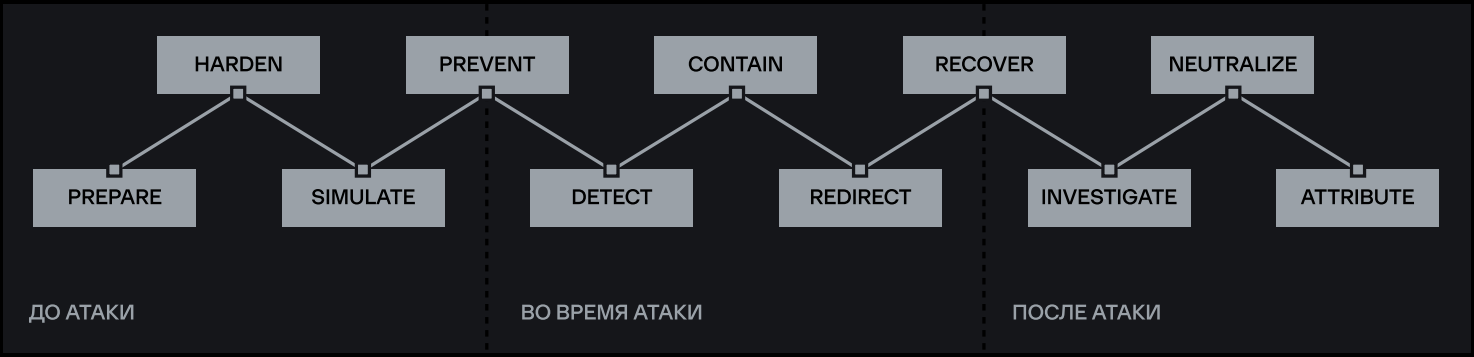
Новые цели ИБ

Cyber response chain

Отделам информационной безопасности становится всё сложнее предотвращать инциденты. При современном ландшафте киберугроз такая цель становится нереалистичной.

В текущих реалиях профессионализм специалистов ИБ оценивается по тому, насколько оперативно они могут обнаружить инцидент, ограничить масштаб ущерба и сократить среднее время восстановления.

Чтобы соответствовать актуальным требованиям, командам ИБ необходимо работать в соответствии со следующей последовательностью действий:



Время — ключевой фактор

Инциденты ИБ неизбежны, поэтому оперативное реагирование на них — задача первостепенной важности. Чем больше времени уходит на обнаружение инцидента и реагирование на него, тем дороже становится процедура полного восстановления.

13 дней

в среднем проходит с момента получения атакующими доступа в сеть жертвы до развертывания программы-вымогателя

1,25 млн$

в среднем затрачивается на инцидент при обнаружении спустя 200 или более дней с момента его начала (при среднем времени обнаружения и сдерживания 287 дней), согласно данным IBM

Managed XDR

Класс продуктов, увеличивающих скорость и эффективность реагирования

Managed XDR предоставляет исключительные возможности обнаружения угроз и реагирования на них за счет использования многочисленных источников телеметрии и передовых технологий машинного обучения.

Group-IB Managed XDR задействует мощности платформы детонации ВПО, данные киберразведки и модели машинного обучения для корреляции событий, тем самым защищая сети, конечные станции и облачные пространства.

Эффективность детектирования и реагирования значительно увеличивается благодаря сервисам Group-IB.

Managed XDR решает самые актуальные проблемы ИБ на сегодняшний день

Облегчает работу с событиями

Каждый час в системах ИБ генерируются тысячи событий. Group-IB XDR коррелирует данные и определяет те проблемы, которые требуют действий.

Расширяет возможности

Команды ИБ зачастую перегружены задачами и испытывают нехватку ресурсов. Group-IB XDR упрощает рабочие задачи благодаря оптимизации процессов обнаружения и реагирования.

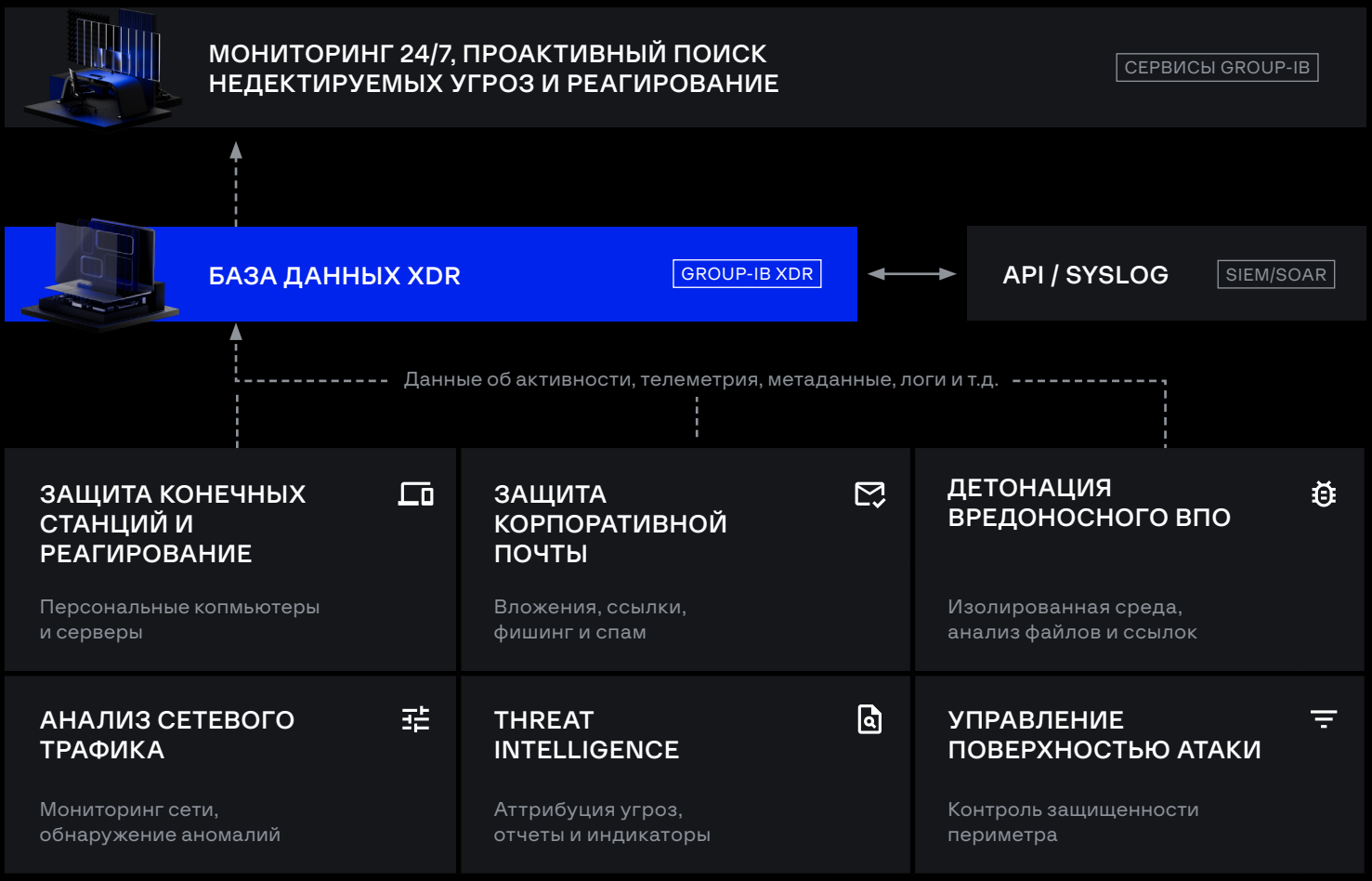
Объединяет отдельные решения

Управление портфелем ИБ-решений — это сложный и трудозатратный процесс. Компоненты Group-IB XDR работают как единое целое, повышая показатели ROI.

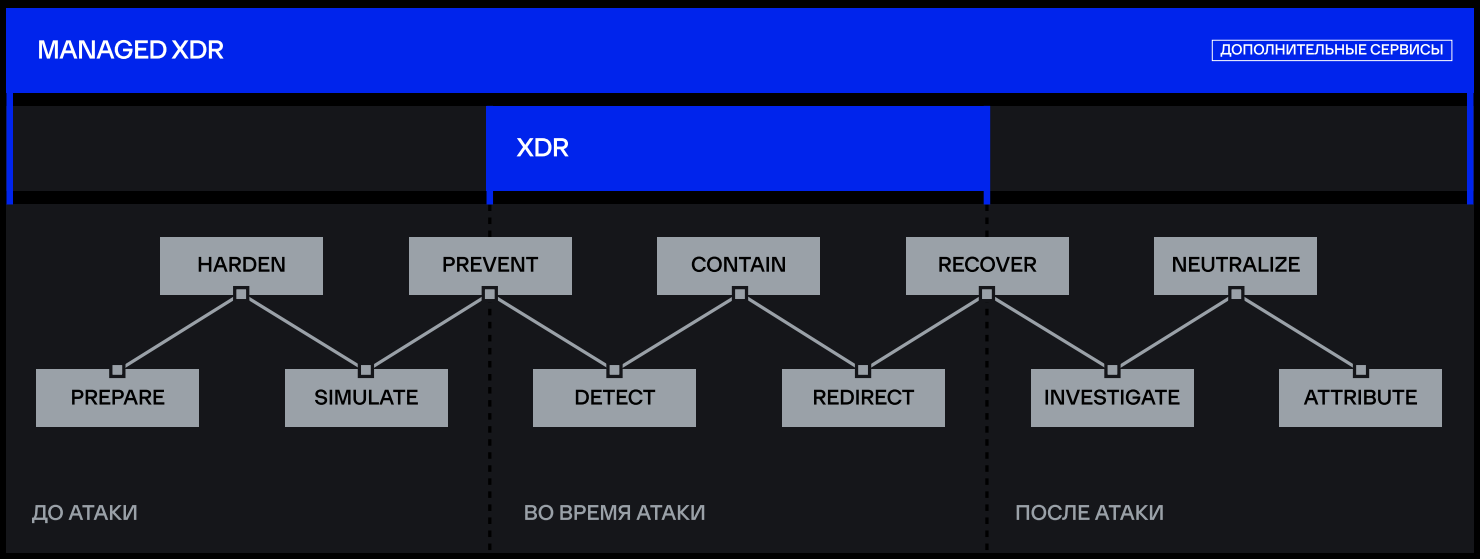
Отслеживает эволюцию угроз

Кибератаки постоянно усложняются. Данные киберразведки и продвинутые технологии позволяют выстраивать наиболее актуальную защиту.

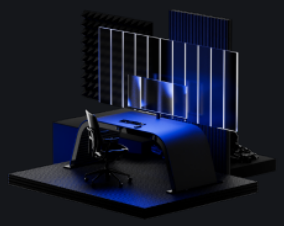
Общий обзор решения



Group-IB Managed XDR покрывает большинство задач цикла работы с инцидентами



Расширение возможностей команды ИБ

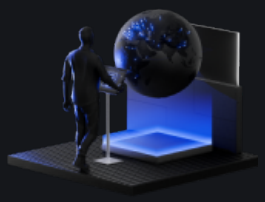


Мониторинг 24/7

Круглосуточный CERT-GIB поможет сконцентрировать усилия на важном и получать ключевые уведомления и нужные отчеты и рекомендации

Проактивный поиск недетектируемых угроз

Позвольте опытным специалистам проверить гипотезы на основе телеметрии XDR, чтобы обнаружить неизвестные, сложные и целевые угрозы



Реагирование на выявленные инциденты

Сокращайте ущерб от угроз и реагируйте на инциденты быстрее с помощью команды экспертов Group-IB, которые используют XDR для сбора данных и удаленного реагирования

Group-IB Managed XDR: Гибкость, которую можно измерить, скорость, которой нет равных

Беспрецедентная синергия продуктов

Специализированные решения Group-IB работают в связке и обеспечивают повышенную защиту сегментов инфраструктуры от разных видов атак с вариантами развертывания локально или в облаке.

Экономия времени благодаря инновационной автоматизации

Система обрабатывает сложные инциденты автоматически, избавляя клиента от ручного разбора сотен разрозненных событий, а команда экспертов Group-IB всегда помогает в реагировании на инцидент.

Умная приоритизация и рекомендации

Решение открывает доступ к базе знаний об актуальных угрозах по регионам и отраслям. Данные агрегируются в локальных центрах исследований и основаны на долгом опыте работы компании, ее лаборатории компьютерной криминалистики и исследованиях.

Обнаружение и реагирование в режиме реального времени

Реагирование проводится сразу же после выявления угроз в защищаемой инфраструктуре, и включает изоляцию хоста, сбор криминалистических данных и карантин файлов.

Преимущества Managed XDR от Group-IB в цифрах

272% ROI

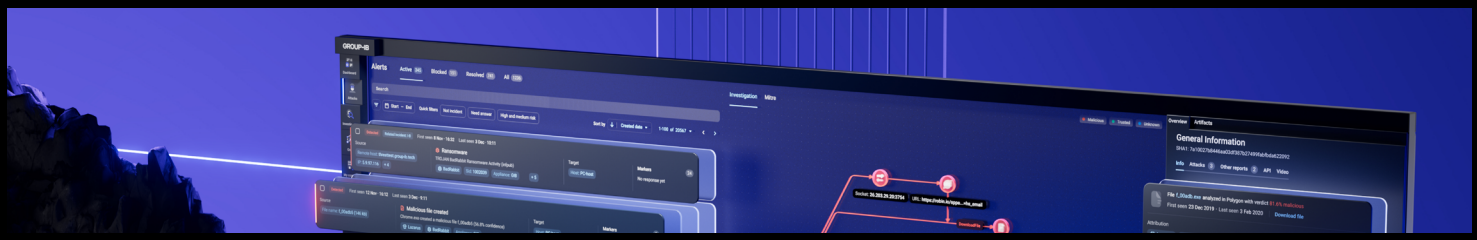
Возврат инвестиций по исследованию агентства Forrester

На 20% быстрее

Реагирование на выявленные инциденты

На 20% выше

Измеримая эффективность команд ИБ при использовании Managed XDR



Основные функции решения

Защита конечных станций и реагирование (EDR)

- Обнаружение угроз на хостах
- Классификаторы для поведенческого анализа на основе алгоритмов машинного обучения
- Эффективное реагирование
- Контроль запуска приложений
- Инвентаризация активов
- Обнаружение угроз UEFI
- Сбор криминалистических данных

Анализ сетевого трафика (NTA)

- Поддержка протоколов L2-L7
- Сбор сетевых логов и метаданных сетевых соединений
- Пользовательские сигнатуры
- Выявление скрытых каналов (DNS-, ICMP-туннелирование, DGA)
- Анализ зашифрованного трафика (ETA)
- Выявление C2 трафика
- Извлечение объектов для анализа

Детонация вредоносного ПО (MWD)

- Автоматическая настройка виртуальных машин
- Анализ объектов из разных источников
- Более 290 поддерживаемых форматов
- Анализ ссылок
- Ретроспективный анализ
- Технологии противодействия обходу средств обнаружения
- Подробные отчеты

Защита корпоративной почты (BEP)

- Локальное или облачное развертывание
- Фильтрация спама
- Антивирусный анализ
- Реалистичные виртуальные машины (морфинг образов)
- Туннелирование трафика
- Противодействие техникам обхода средств обнаружения
- Защита после доставки писем
- Выявление BEC-атак и фишинга

Сервисы MXDR

- Круглосуточный мониторинг событий
- Фильтрация ложноположительных срабатываний
- Прямое взаимодействие с аналитиками
- Тестирование гипотез
- Персонализированный ландшафт угроз
- Различные сценарии реагирования на выявленные инциденты
- Команда высококлассных экспертов

Group-IB — международная компания по кибербезопасности

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

Партнер и участник совместных расследований

Interpol

Europol

Решения Group-IB признаны мировыми агентствами

FORRESTER®

kuppingercole ANALYSTS

Gartner

IDC

FROST & SULLIVAN

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

- Цифровая криминалистика
- Исследование вредоносного кода
- Расследование высокотехнологичных преступлений

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

Предотвращение и исследование киберпреступлений с 2003 года

GROUP-IB.RU
INFO@GROUP-IB.COM
GROUP-IB.RU/BLOG
+7 495 984 33 64