Group-IB

THREAT HUNTING FRAMEWORK

Система для защиты от сложных целевых атак и проактивной охоты за угрозами внутри и за пределами периметра.

Основана на запатентованных передовых технологиях.

Управление сложными инцидентами

Работа с лучшими экспертами в единой среде

Гибкая автоматизация исследования угроз и реагирования

GROUP-IB

Threat Hunting Framework

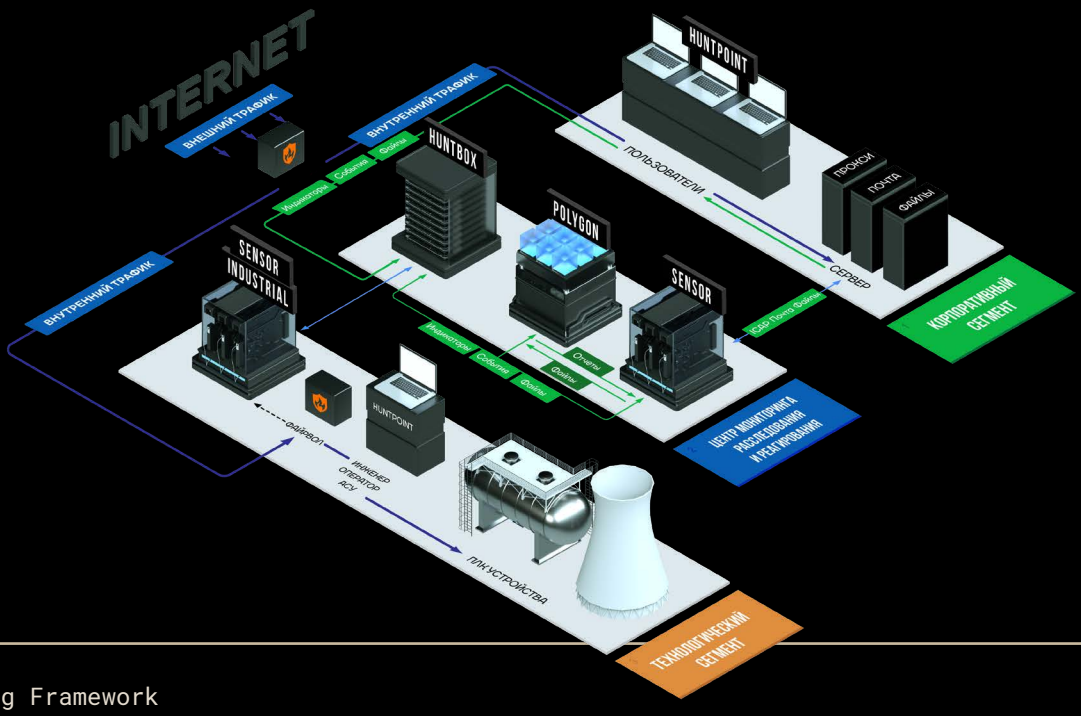
«Видит» больше остальных

В прошлом десятилетии		Group-IB Threat Hunting Framework
Детектирование известных угроз постфактум, пассивный подход к защите	→	Поиск ранее неизвестных угроз за счет данных киберразведки, обнаружения аномалий, скрытых тоннелей, коммуникации с C&C-серверами
Много систем, ручная работа с событиями, потеря массы времени на их обработку и корреляцию	→	Автоматическая корреляция событий и алертов в инциденты и их последующая атрибуция до семейств ВПО или атакующих групп
Охота за угрозами (threat hunting) ограничена локальными сетями	→	Глобальный поиск угроз: раскрытие внешней инфраструктуры, планов атакующих
Отсутствие мощных аналитических инструментов	→	Свой сетевой граф, открывающий доступ к обогащению, корреляции и анализу
Не до конца понятны связи между происходящими событиями	→	Определение полной хронологии атаки, полное описание инцидента до Mutex/Pipes/Registry/Files

Удобен. С гибкими вариантами установки

On-prem	Облачный	Гибридный
Данные хранятся внутри периметра для соблюдения необходимых требований	Простая интеграция с облаком, расположенным в вашей стране для удобства и доступности сервисов	Решение индивидуальных задач с использованием смешанной схемы установки

Становится вашим локальным центром обнаружения



Возможности Threat Hunting Framework

Управление сложными инцидентами

Обнаружение аномалий, скрытых каналов в трафике, анализ поведения программ и пользователей и корреляция событий

Детонация и анализ вредоносного ПО

Запатентованная система динамического исследования ВПО, имитирующая реальные машины и действия пользователей

Совместная работа с экспертами

Единая среда, удаленное реагирование и компьютерная криминалистика, доступ к аналитикам и сообществу

Проактивная охота за угрозами

На хостах и в сетевом трафике, внутри инфраструктуры и за ее пределами (анализ инфраструктуры атакующих)

Доступ к данным систем киберразведки

Возможность атрибутировать разрозненные события одной атаки до конкретного ВПО или злоумышленника и остановить ее развитие

Единое решение для корпоративной и технологической сетей

Комплекс всех нужных инструментов для адаптивной автоматизации исследования, хантинга и реагирования

Ключевые преимущества

- Комплексная защита технологической и корпоративной сетей
- Одно решение покрывает все каналы распространения угроз: почта, сетевой трафик, рабочие станции и съемные носители
- Круглосуточный мониторинг и поддержка центра реагирования
- Простота установки и настройки модулей под решение конкретных задач
- Непрерывность процессов и минимум ложных срабатываний
- Автоматизация и глубина отчетности
- Гибкие настройки политики обновлений под цели компании
- В стоимость включена страховка от ведущих агентств на случай инцидента

Архитектура Threat Hunting Framework

Соответствие требованиям 187-ФЗ “О безопасности КИИ”

Сертификат соответствия ФСТЭК

Единый реестр отечественного ПО

group-ib.ru ↗

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 проводили 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	специалистови разработчиков

→

Узнайте больше о возможностях Threat Hunting Framework

thf@group-ib.com

→

Познакомьтесь с Group-IB

group-ib.com
info@group-ib.com
twitter.com/GroupIB_GIB

→

Узнай больше об Threat Hunting Framework

Сервисы Group–IB

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

Аудит и оценка рисков

- Тестирование на проникновение
- Анализ исходного кода
- Выявление следов компрометации сети
- Киберучения 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
- Проактивный хантинг угроз
- Выездное реагирование на сложные кибератаки
- Реагирование на инциденты «по подписке»

Криминалистика и расследования

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