tds.group-ib.ru

THREAT DETECTION SYSTEM

Проактивное обнаружение и реагирование на киберугрозы, основанное на технологиях слежения за киберпреступниками.

Обнаружение сложных атак

Эффективное и быстрое реагирование

Покрытие всех векторов заражения

GLOBAL CYBER SECURITY COMPANY • GLOBAL CYBER SECURITY COMPANY • GIB

ЭВОЛЮЦИЯ МЕТОДОВ ЗАЩИТЫ ОТ СЛОЖНЫХ УГРОЗ

1990 –

Обнаружение с фокусом на известном вредоносном ПО

- Антивирусы
- Системы предотвращения вторжений

2010 –

Обнаружение с фокусом на неизвестном вредоносном ПО

- Песочницы
- Антивирусы нового поколения

2015 –

Обнаружение с фокусом на киберпреступнике

- Threat Intelligence
- Проактивный поиск угроз

УДАЧНАЯ ОХОТА С THREAT DETECTION SYSTEM

КОМПЛЕКСНОЕ РЕШЕНИЕ ДЛЯ ПРОАКТИВНОГО ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ НА КИБЕРУГРОЗЫ

ENDPOINT

Анализ активности, выявление угроз и реагирование на хосте

↓ События, индикаторы

SENSOR

Анализ сетевого трафика, выявление заражений

↓ События, индикаторы

POLYGON

Поведенческий анализ файлов в изолированной среде

↓ События, индикаторы

HUNTBOX

Автоматизированный поиск угроз и эффективное реагирование

- Разрозненные события объединяются в единое уведомление об угрозе
- Каждое уведомление содержит полный контекст, профиль атакующего, восстановленную хронологию атаки

Внутренний поиск угроз

Управление инцидентами, корреляция и обогащение индикаторов

Реконструкция хронологии атаки

Криминалистика и реагирование в корпоративной сети и на хосте

↓ Известные индикаторы

↑ Неизвестные индикаторы, контекст угрозы

Глобальный поиск угроз

Обогащение известных индикаторов

Атрибуция и профиль атакующего

Выявление инфраструктуры и инструментов для будущих атак

МАКСИМУМ УДОБСТВА С ГИБКИМИ ВАРИАНТАМИ УСТАНОВКИ

On-prem

Все данные остаются внутри периметра для соответствия требованиям регуляторов

Облако

Удобная интеграция с облаком, расположенным в стране клиента

Гибридное

Смешанная схема установки для решения индивидуальных задач клиента

ПОЛНОТА ДЕТЕКТИРОВАНИЯ И ЭФФЕКТИВНОЕ РЕАГИРОВАНИЕ

МОДУЛЬНОЕ РЕШЕНИЕ ДЛЯ МНОГОУРОВНЕВОЙ ЗАЩИТЫ ОТ СЛОЖНЫХ АТАК

Выявление угроз и реагирование на хосте

ENDPOINT

- Выявление вредоносного ПО, зараженных документов и эксплойтов для браузера, скриптов и инструментов сбора учетных данных
- Эффективное реагирование
- Управление приложениями и устройствами

Анализ трафика и выявление аномалий

SENSOR

- Глубокий анализ трафика с помощью искусственного интеллекта
- Обнаружение скрытых каналов коммуникации с командными серверами злоумышленников
- Обновление правил в режиме реального времени на основе уникальных данных Threat Intelligence

Анализ в песочнице и блокировка угроз

POLYGON

- Противодействие техникам обхода песочниц
- Сложные алгоритмы извлечения объектов для качественной работы с зашифрованными файлами, архивами, паролями, ссылками
- Передовые технологии поведенческого анализа

Вся информация об обнаруженных инцидентах доступна в удобном интерфейсе в режиме реального времени. Оповещения включают подробный анализ угрозы и контекст для дальнейшего расследования.

24 Круглосуточная поддержка

Рекомендации опытных экспертов по реагированию на инциденты

HUNTBOX

TDS Huntbox - передовое решение для эффективного управления инцидентами, автоматизации проактивного поиска угроз (threat hunting) внутри сети и обогащения внутренних индикаторов глобальными данными об активности киберпреступников

Huntbox выводит технологии информационной безопасности на новый уровень благодаря уникальным возможностям...

Полный контекст атаки, атрибуция угрозы, профиль атакующего

Понимание уникальных признаков поведения и инфраструктуры киберпреступников

Выявление инфраструктуры на этапе подготовки новой атаки для проактивного реагирования

...на основе данных киберразведки из закрытых источников и запатентованных технологий от экспертов с 15-летним опытом анализа угроз и расследования инцидентов

Threat Intelligence

Проверенная и значимая информация об угрозах, нацеленных на вашу компанию

Описание инструментов и тактики атак в формате MITRE's ATT&CK

Глубинные исследования сложных целевых угроз и группировок киберпреступников

Group-IB входит в рейтинг лучших мировых поставщиков Threat Intelligence по версии Gartner, IDC, Forrester, Cyber Defense Magazine и SC Media

100 000+
профайлов злоумышленников в базе Threat Intelligence

Выявление инфраструктуры атакующих

Правила выявления инфраструктуры для будущих атак, основанные на уникальных поведенческих характеристиках атакующих

4,2 МЛРД
IP-адресов

650 МЛН
доменов

689 МЛН
SSL-сертификатов

145 МЛН
ключей SSH

Group-IB – один из ведущих мировых разработчиков решений для детектирования и предотвращения кибератак, выявления фрода и защиты интеллектуальной собственности в сети

15 лет
ПРАКТИЧЕСКОГО ОПЫТА

55 000+
ЧАСОВ РЕАГИРОВАНИЯ

1 000+
РАССЛЕДОВАНИЙ ПО ВСЕМУ МИРУ

300+
СПЕЦИАЛИСТОВ И РАЗРАБОТЧИКОВ

Официальный партнер

INTERPOL EUROPOL

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

Эксперты Group-IB проводили тренинги профессионального развития для специалистов Europol, INTERPOL, правоохранительных органов, корпоративных команд безопасности и преподавателей университетов в Великобритании, Германии, Нидерландах, Бельгии, Франции, Таиланде, Бахрейне и Ливане.

УЗНАТЬ БОЛЬШЕ

о возможностях Threat Detection System

tds.group-ib.ru

СВЯЖИТЕСЬ С НАМИ

Чтобы провести тест-драйв TDS

tds@group-ib.ru

ПОЗНАКОМЬТЕСЬ С GROUP-IB

group-ib.ru

facebook.com/GroupIB

СЕРВИСЫ GROUP-IB

Укрепите кибербезопасность с помощью опытных специалистов, погруженных в реагирование и расследование актуальных атак и имеющих доступ к одной из самых современных систем слежения за киберугрозами в мире.

АУДИТ И ОЦЕНКА РИСКОВ

- Тестирование на проникновение
- Исследование уязвимостей
- Анализ исходного кода
- Compromise Assessment
- Red Teaming
- Pre-IR Assessment
- Оценка соответствия

THREAT HUNTING И РЕАГИРОВАНИЕ

- Managed Threat Hunting
- APT-мониторинг
- Криминалистическое реагирование (целевые атаки, утечки и др.)
- Оперативное реагирование (фишинг, DDoS, нарушение прав на интеллектуальную собственность и др.)
- Реагирование «по подписке»

КРИМИНАЛИСТИКА

- Сбор цифровых доказательств
- Криминалистический анализ
- Анализ вредоносного кода

РАССЛЕДОВАНИЯ

- Целевые атаки
- Инциденты информационной безопасности
- Финансовые и корпоративные преступления