GROUP-IB

THREAT HUNTING В ТЕХНОЛОГИЧЕСКИХ СЕТЯХ

Суслин Андрей Андреевич

Руководитель отдела по разработке решений для АСУ ТП

Threat Hunting. Что это?

Threat Hunting - процесс целевого поиска угроз, в котором многое строится вокруг гипотез того, как будет действовать атакующий.

Threat Hunting

Thread Hunting - процесс целевого поиска угроз, в котором многое строится вокруг гипотез того, как будет действовать атакующий.

Threat Hunting

Thread Hunting - процесс целевого поиска угроз, в котором многое строится вокруг гипотез того, как будет действовать атакующий.

Обнаружения недостаточно

Средство защиты информации обнаружило и/или заблокировало угрозы

РАБОТА ЗАКОНЧЕНА

- Есть события – решение работает.
- Сформируем отчет для руководства
- Отлично, потраченный бюджет оправдывает себя.

Обнаружения недостаточно

Средство защиты информации обнаружило и/или заблокировало угрозы

РАБОТА ЗАКОНЧЕНА

1. Злоумышленник продолжает анализировать Вашу инфраструктуру
2. Понимает технику обнаружения и анализирует неудавшуюся атаку
3. Находит техники обхода средств защиты
4. Сохраняет присутствие, перемещается по сети и успешно проводит атаку

Обнаружения недостаточно

Средство защиты информации обнаружило и/или заблокировало угрозы

РАБОТА ЗАКОНЧЕНА

1. Злоумышленник продолжает анализировать Вашу инфраструктуру
2. Понимает технику обнаружения и анализирует неудавшуюся атаку
3. Находит техники обхода средств защиты
4. Сохраняет присутствие, перемещается по сети и успешно проводит атаку

РАБОТА ТОЛЬКО НАЧИНАЕТСЯ

- Кто нацелился на наше предприятие?
- Какие были их задачи и конечная цель?
- Является ли это частью существующего инцидента или целевой атаки? Что мы можем сделать для обнаружения в будущем?
- Если они уже в вашей сети, как мы узнаем?

Целевые атаки касаются каждого

А правда ли вас могут атаковать?

Спойлер: да

Технологические сети – привлекательная мишень для всех

Спецслужбы

Мотивация: шпионаж и саботаж

Активность: 2005 – 2021

Особенность: обнаруживаются только после нанесения ущерба

Конкуренты

Мотивация: промышленный шпионаж

Активность: 2012 – 2021

Особенность: высокий уровень успеха, слабо детектируются

Криминал

Мотивация: финансовая и саботаж

Активность: 2019 – 2021

Особенность: партнёрские программы для привлечения разнородных экспертов


THIS IS FINE.

Проблемы индустрии

Разрозненные данные

Команда SOC получает тысячи несвязных предупреждений и уведомлений. Выстраивание цепочки инцидента отнимает драгоценное время.

8-12 тысяч

Каждую секунду компания среднего размера регистрирует около 8-12 тысяч событий информационной безопасности.

Нехватка ресурсов

Небольшим предприятиям сложно обеспечивать безопасность из-за отсутствия выделенной команды ИБ или недостаточного числа специалистов

68%

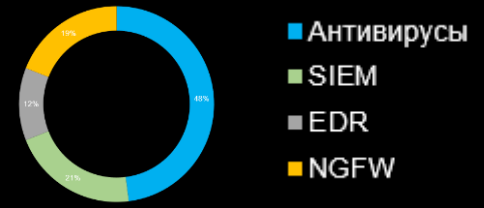
68% компаний не хватает персонала для реагирования на сложные угрозы

Найти ответственного

В отражении кибератак реального сектора экономики могут быть задействованы разные отделы: ИТ, ИБ, АСУ ТП. Их действия не всегда согласованы

«Зоопарк» решений

Отдельные инструменты безопасности, даже нового поколения, не позволяют понять другие элементы атаки. Нет видимости всей атаки



Актуальные угрозы

Секторы, наиболее затронутые раскрытием уязвимостей АСУ ТП во втором полугодии 2020

- ТЭК

- Водоснабжение и водоотведение

- Коммерческое производство

>70% обнаруженных уязвимостей АСУ ТП можно использовать удаленно

Около 45% выявленных уязвимостей затрагивают средний уровень АСУ ТП

78% выявленных уязвимостей АСУ ТП не требуют аутентификации для эксплуатации

Построение защиты предприятия. 1 этап

I

Сегментировать/
Изолировать сети

Сеть изолировали, что дальше?

Плюсы изоляции сегмента

1. Контроль и фильтрация всего трафика в ваш технологический сегмент
2. Блокировка попыток проникновения внешних нарушителей
3. Защита внутреннего периметра от корпоративных угроз

На что стоит обратить внимание

1. Правильная конфигурация
2. «Временный» доступ
3. Подрядчики и контрагенты

Построение защиты предприятия. 2 этап

I

Сегментировать корпоративные и технологические сети

II

- Использовать функций собственной безопасности компонентов АСУ
- Создать внутренние регламент

Бесплатные инструменты никто не отменял

Что можно сделать:

1. Установите политику паролей и придерживайтесь ей на всем программном и аппаратном обеспечении
2. Создайте регламенты по работы внутри технологического сегмента
3. Если невозможно отказаться от удаленного подключения в инфраструктуру, то используйте только защищенный канал связи
4. Если возможно, обновите ПО до новых версий

Построение защиты предприятия. 3 этап

I

Сегментировать корпоративные и технологические сети

II

- Использовать функций собственной безопасности компонентов АСУ
- Создать внутренние регламент

III

Выбрать средства защиты уровня сети и рабочих станций

Защита рабочих станций. Критерии выбора

КОНТРОЛЬ УСТРОЙСТВ И ПРИЛОЖЕНИЙ

Применение индивидуальных и групповых политик для контроля устройств и приложений в масштабах всего предприятия

ЦЕЛОСТНОСТЬ ПРОЕКТОВ НА АРМ

Целостность проектов на рабочих станциях оператора

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ НА ХОСТЕ

Высокопроизводительные классификаторы на серверах, обнаруживающие самые сложные атаки в режиме реального времени

ВОЗМОЖНОСТЬ РЕАГИРОВАНИЯ

Остановка атак в реальном времени путем изоляции хоста, автоматической блокировки вредоносного процесса и удалённого снятия триаж-копий.

Защита сети. Критерии выбора

КОНТРОЛЬ ОКРУЖЕНИЯ

Выявление изменений в топологии технологической сети и аномалий

ПОДДЕРЖКА ПРОТОКОЛОВ

Промышленные открытые и проприетарные протоколы

КОНТРОЛЬ УСТАВОК ТЕХ.ПРОЦЕССА

Контроль технологического процесса актуален в зрелой инфраструктуре

ПРОВЕРКА ЦЕЛОСТНОСТИ ПО ПЛК

Пассивный и активный контроль целостности программного обеспечения ПЛК

НАСТРАИВАЕМЫЕ ПОЛИТИКИ ОБНАРУЖЕНИЯ

Возможность настраивать политики обнаружения для формирования правил, соответствующих конкретным запросам клиента.

ЧАСТОТА ОБНОВЛЕНИЯ РЕШАЮЩИХ ПРАВИЛ

Частота обновлений базы решающих правил

Почему такой фокус на скорость обновления?

На что обратить внимание

1. Вам нужен хороший поставщик правил
2. Вам нужен тот, кто пишет сигнатуры
3. Сигнатуры не покрывают все CVE

3-тий этап пройден, достаточно ли этого?

Защита периметра

Мониторинг внутри ОТ сети

Защита рабочих станций

Все еще открытые вопросы:

- Кто нацелился на наше предприятие?
- Какие были их задачи и конечная цель?
- Является ли это частью существующего инцидента или целевой атаки? Что мы можем сделать для обнаружения в будущем?
- Если они уже в вашей сети, как мы узнаем?

Построение защиты предприятия. 4 этап

I

Сегментировать корпоративные и технологические сети

II

- Использовать функций собственной безопасности компонентов АСУ
- Создать внутренние регламент

III

Выбрать средства защиты сети и рабочих станций

IV

Threat Hunting

Готовы ли вы к реальной атаке?

«Мы пока что к этому не готовы»

Учитывайте сразу, что вам нужен threat hunting как процесс внутри компании

Threat Hunting

Защита периметра

Мониторинг внутри OT сети

Защита рабочих станций

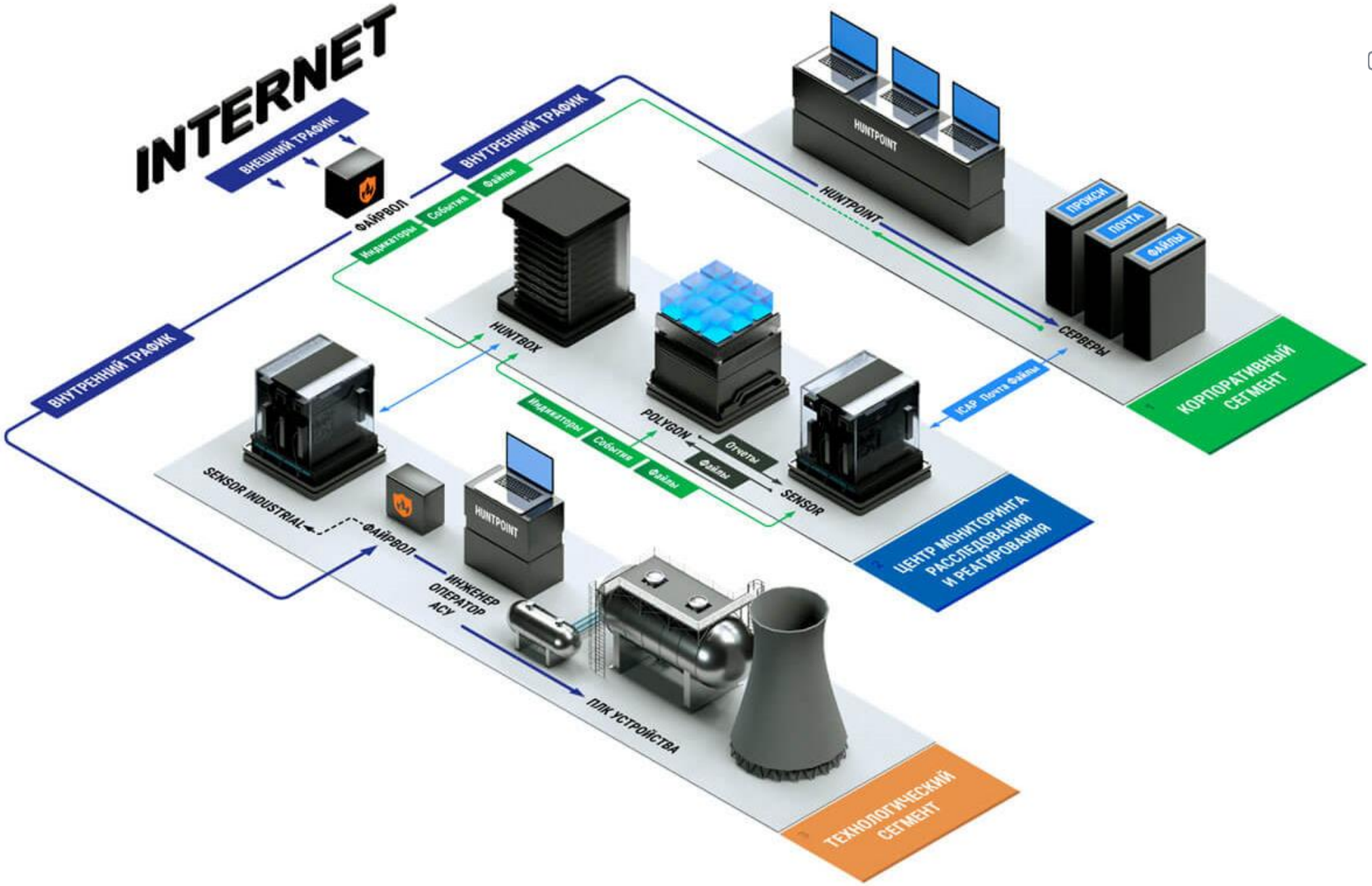
+

Threat Hunting

процесс целевого поиска угроз, в котором многое строится вокруг гипотез того, как будет действовать атакующий

Наш подход


Обнаружение
Хантинг
Расследование
Реагирование
GROUP-IB THREAT INTELLIGENCE & ATTRIBUTION
GROUP-IB THREAT HUNTING FRAMEWORK
Huntpoint
Анализ событий APM, выявление угроз и реагирование на хосте
Sensor Industrial
Анализ промышленных систем управления на уровне сети
Sensor
Анализ сетевого трафика, выявление аномалий и заражений
Polygon
Поведенческий анализ объектов в изолированной среде
Huntbox
Реагирование, хранение данных и корреляция событий
Decryptor
Расшифровка SSL-шифрованного трафика


INTERNET
ВНЕШНИЙ ТРАФИК
ФАЙРВОЛ
ВНУТРЕННИЙ ТРАФИК
Маркеторы
События
Файлы
HUNTPOINT
HUNTPOINT
ПРОКСИ
ПОЧТА
ФАЙЛЫ
СЕРВЕРЫ
КОРПОРАТИВНЫЙ СЕГМЕНТ
HUNTBOX
POLYGON
SENSOR
ICAP Почта Файлы
Индикаторы
События
Файлы
Отчеты
Файлы
ВНУТРЕННИЙ ТРАФИК
SENSOR INDUSTRIAL
ФАЙРВОЛ
HUNTPOINT
ИНЖЕНЕР
ОПЕРАТОР
АСУ
ПЛК УСТРОЙСТВА
ЦЕНТР МОНИТОРИНГА РАССЛЕДОВАНИЯ И РЕАГИРОВАНИЯ
ТЕХНОЛОГИЧЕСКИЙ СЕГМЕНТ

Единая система защиты от киберугроз

ЕДИНЫЙ ИНТЕРФЕЙС

Управление всеми модулями системы и их динамическая конфигурация

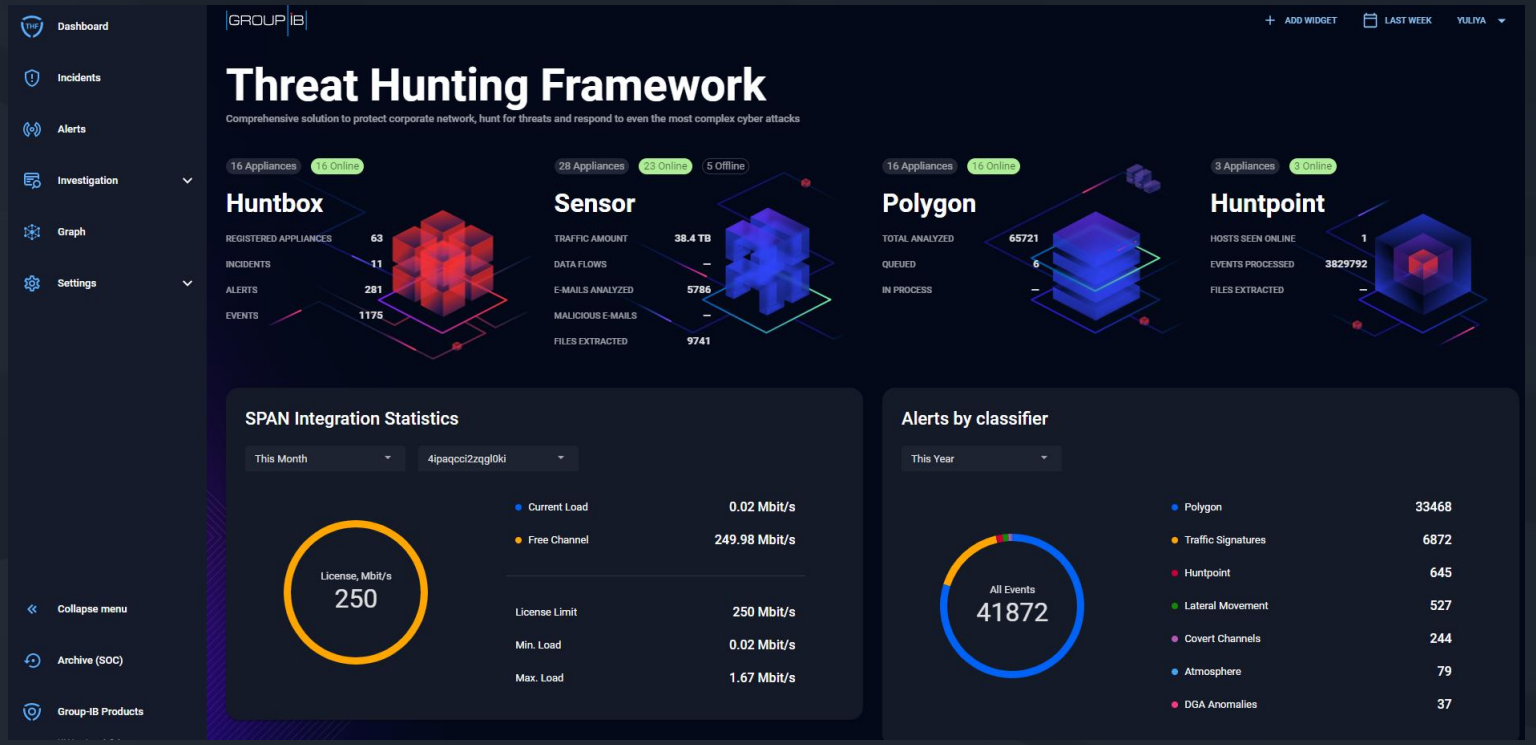
УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

Корреляция и группировка событий в инциденты, для сокращения времени их обработки

ГИБКИЕ ОПЦИИ ПОСТАВКИ

- Локальная установка для хранения всех данных внутри периметра
- Облачная инфраструктура с настраиваемыми службами безопасности

Полностью автоматизированный поиск внутренних и внешних угроз и оптимизированное реагирование



Три простых шага для Threat Hunting

GROUP IB

1

Форма

Напишите мне

2

Опросник

Заполните опросник, предоставленный нашей командой

3

THREAT HUNTING

Постройте процесс threat hunting совместно с Threat Hunting Framework

Предотвращаем и расследуем киберпреступления с 2003 года.

Суслин Андрей Андреевич

Руководитель отдела по разработке решений для АСУ ТП

www.group-ib.ru

info@group-ib.com

twitter.com/groupib

t.me/group_ib

group-ib.ru/blog

+7 495 984 33 64

facebook.com/groupib

instagram.com/group_ib