Комплексный подход к обеспечению защищенности от целевых атак в IT и OT сегментах цифрового предприяти

Фесенко Станилсав

Руководитель департамента системных решений

Что происходит вокруг

OT-сегмент – привлекательная мишень

Саботаж и аварии

Цель:
Физически вывести инфраструктуру из строя

Последствия:
От финансовых потерь, до человеческих жертв

Шпионаж

Цель:
Кража интеллектуальной собственности, ноу-хау

Последствия:
Потеря конкурентного преимущества, прямой финансовый ущерб

Целевые атаки

Цель:
Шифрование данных, требование выкупа

Последствия:
Простой тех. процесса, потеря данных, вплоть до закрытия предприятия

Стандартный подход к защите OT-сегмента

«Воздушный зазор» + Файрволл + стандартные средства защиты в корпоративном сегменте (AV, IDS, …)

Насколько он эффективен?

Атаки на OT-сегмент: встречаются чаще, становятся сложнее

GROUP-IB

2007-2015

Black Energy

Вредоносное ПО, которое обесточило целую область в Украине

2010-2012

Stuxnet

Сложное ВПО, вероятно уничтожившее критическую инфраструктуру в Иране

2014

Havex

ПО удаленного доступа в OT-сети, используемое для кампаний по шпионажу

2016

Industroyer

ВПО, нацеленное на электросети, способное привести к их отключению

2017

Triton

ВПО, отключившее системы безопасности на нефтехимическом заводе

2018

VPNFilter

Вредонос, нацеленный на подключенные устройства в АСУ ТП

2020

Unknown

Полная остановка крупного порта в Иране из-за кибератаки

2021

Unknown

Атака на АСУ ТП водоснабжения в США с изменением состава воды

Атаки на цепочку поставок

2018

Встраивание вредоносного кода в ASUS Live Update и распространение вредоносной версии с серверов ASUS

2018

Еще 3 неназванных компании были скомпрометированы и использованы для тех же целей

2019

Взлом компании с множеством продуктов для программистов на разных языках. Доступ получен к серверам компиляции программ

2020

Атака на SolarWinds, затронувшая тысячи организаций, которые устанавливали «легетимное» обновление скомпрометированного вендора

Атакующие и их инструменты

Спецслужбы, прогосударственные атакующие, обычный криминал

- Атаки на цепочки поставки
- Атаки на микрокод
- 0day уязвимости в ключевом ПО
- Физическая инфильтрация на объект
- Черный рынок доступов и услуг в андеграунде
- Приватные и публичные (доступные на рынке) вредоносные программы и эксплоиты
- Покупка «логов» и разведка чужими руками
- Кросс-чекинг аккаунтов
- Публичные инструменты: Metasploit, Cobalt Strike, PowerShell Empire, mimikatz, Gophish и т.д.
- Атака периметра, сбор OSINT
- Публичные уязвимости
- Социальная инженерия
- 0day уязвимости в оборудовании (исследования вендоров)

Угрозы для OT-сегмента в цифрах

Наибольшее количество уязвимостей АСУ ТП во втором полугодии 2020 раскрыто в секторах:

- ТЭК

- Водоснабжение и водоотведение

- Коммерческое производство

>70% обнаруженных уязвимостей АСУ ТП можно использовать удаленно

На 25% в год растет количество обнаруживаемых уязвимостей АСУ ТП

Около 45% выявленных уязвимостей затрагивают средний уровень АСУ ТП

70-80% уязвимостей АСУ ТП получают высокий уровень критичности при обнаружении

78% выявленных уязвимостей АСУ ТП не требуют аутентификации для эксплуатации

До 60% предприятий закрываются после успешной целевой атаки шифровальщика

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%

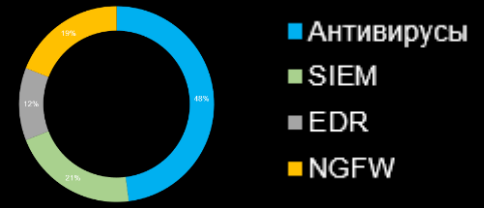
68% компаний не хватает персонала для реагирования на сложные угрозы

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



Обнаружения недостаточно

Стандартные средства защиты OT-сегмента останавливаются на обнаружении и блокировке, что приводит к плачевным последствиям

Решение обнаружило
и заблокировало угрозу

- Атакующий остается в инфраструктуре
- Делает выводы из неудавшейся атаки
- Подбирает тактику обхода средств защиты
- Перемещается по сети и достигает цели

Обнаружения недостаточно

Стандартные средства защиты OT-сегмента останавливаются на обнаружении и блокировке, что приводит к плачевным последствиям

Решение обнаружило и заблокировало угрозу

VS.

Решение активно охотится за угрозами, использует AI и ML

- Атакующий остается в инфраструктуре
- Делает выводы из неудавшейся атаки
- Подбирает тактику обхода средств защиты
- Перемещается по сети и достигает цели

- Выяснили, что алерт был частью сложного инцидента
- Нашли другие признаки атаки по аномалиям и с помощью машинного обучения
- Узнали конкретного атакующего, его цели, тактику и инструменты
- Убедились, что он не «затаился» в сети
- Подготовили стратегию и тактику защиты от подобных атак в будущем

Что делать?

Экосистема решений Group-IB

Threat Intelligence & Attribution

Новый класс решений для сбора данных об угрозах и атакующих, релевантных для конкретной организации, с целью проактивной охоты за злоумышленниками и защиты сетевой инфраструктуры, признанный Gartner, IDC, Forrester и Cyber Defense Magazine.

Проактивный хантинг и реагирование на киберугрозы

Threat Hunting Framework

Huntbox | Sensor | Polygon| Huntpoint | Sensor Industrial | Decryptor

Защита цифровой личности и предотвращение мошенничества

Fraud Hunting Platform

Processing Hub | Web Snippet | Mobile SDK | Preventive Proxy

Защита интеллектуальной собственности и товарных знаков

Digital Risk Protection

Антимошенничество | Антиконтрафакт | Антипиратство | Выявление утечек данных | Защита топ-менеджмента

Центр компетенций Group-IB

- Аудит & Red Team
- Команда кибербразведки
- 24/7 Центр реагирования CERT-GIB
- Лаборатория компьютерной криминалистики
- Департамент расследований высокотехнологичных преступлений
- Команда по киберобучению

Комплексный подход Group-IB

Возможности THF Sensor Industrial

Контроль топологии и карты соединений

- Детектирование новых устройств
- Непрерывная инвентаризация компонентов и процессов
- Обнаружение аномалий в трафике
- Отслеживание новых подключений
- Использование самоубучаемых моделей

Контроль целостности прошивок и ПУ

- Пассивное определение версий ПО и ПЛК
- Контроли изменений загруженных ПУ и firmware контроллеров
- Обнаружение не задокументированных возможностей промышленных протоколов и нестандартной активности в АСУ ТП

Поддержка протоколов и специфичных политик

- Поддержка ключевых проприетарных и открытых технологических протоколов
- Детектирование атак и поиск аномалий на основании клиенто-специфичных политик, настраиваемых в интерфейсе решения

Huntbox

ЕДИНЫЙ ИНТЕРФЕЙС

Управление всеми модулями системы и их динамическая конфигурация

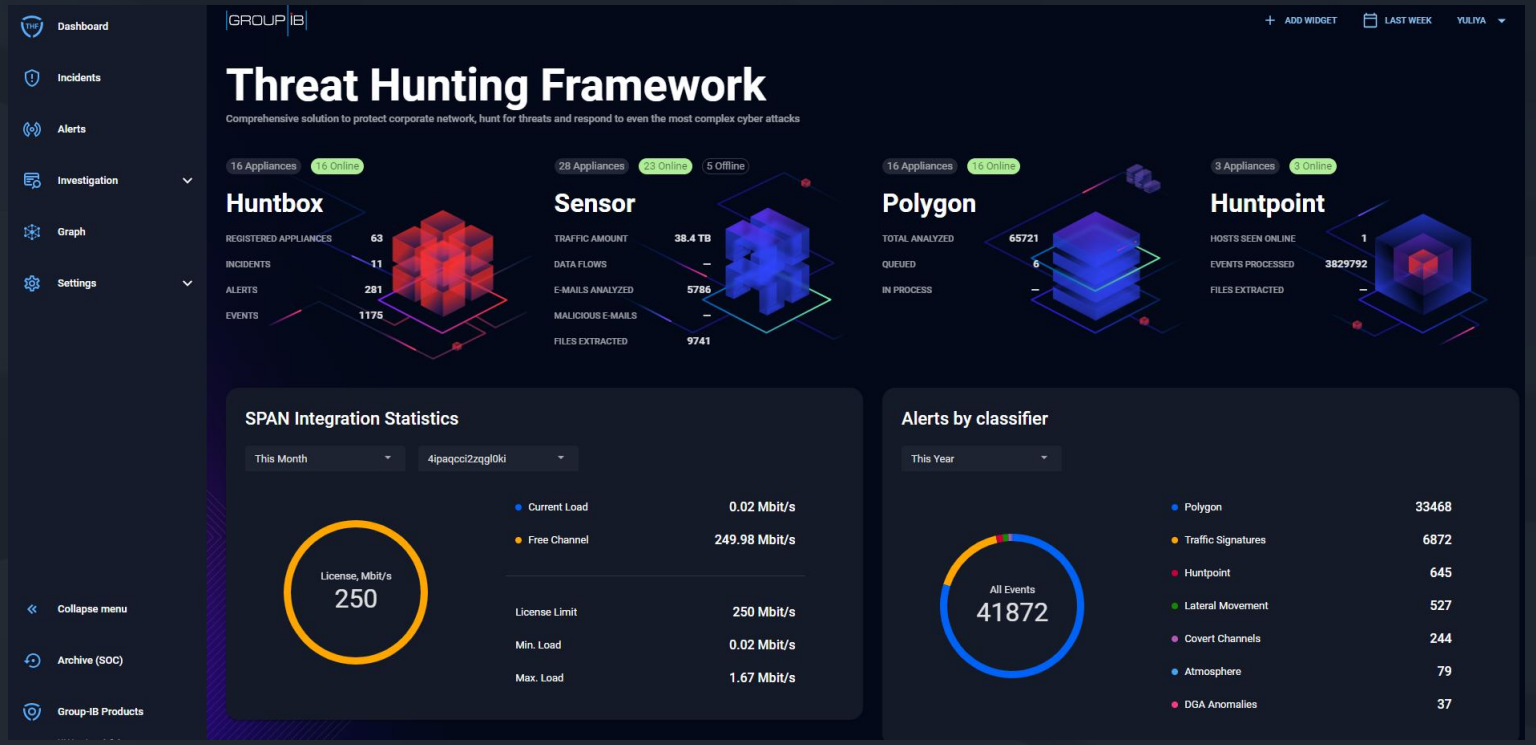
УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

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



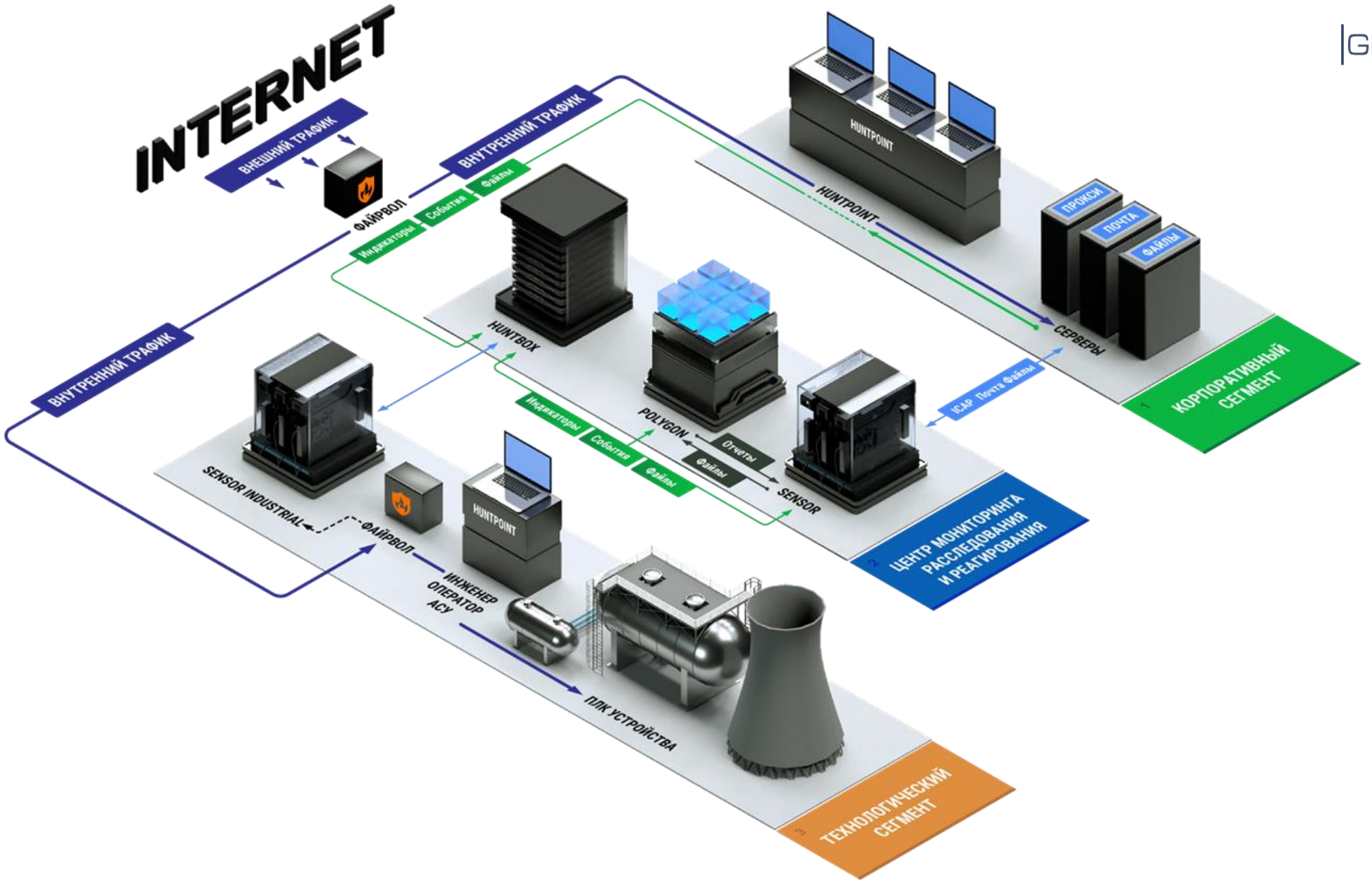
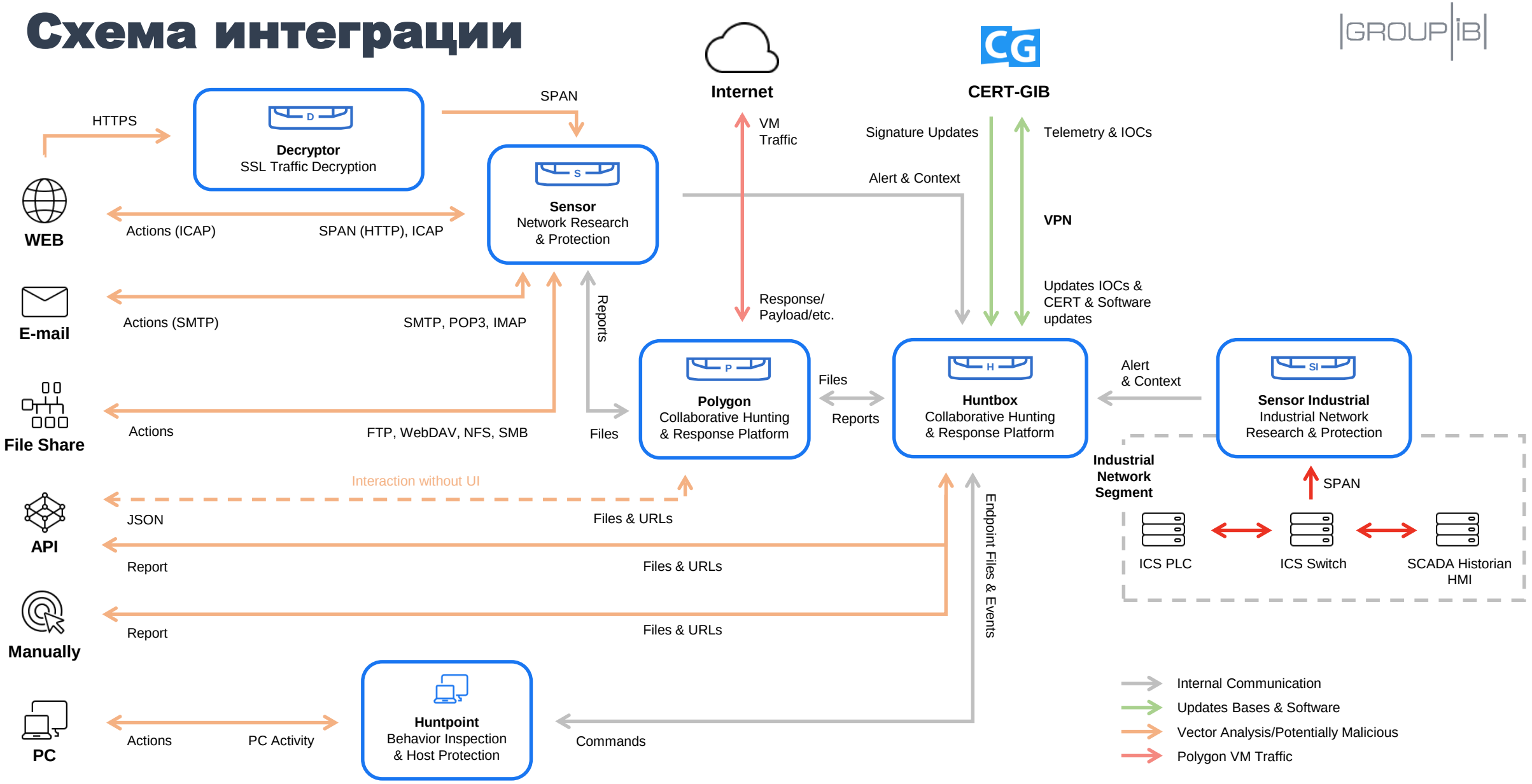

INTERNET
ВНЕШНИЙ ТРАФИК
ФАЙРВОЛ
ВНУТРЕННИЙ ТРАФИК
Индикаторы
События
Файлы
HUNTPOINT
HUNTPOINT
ПРОКСИ
ПОЧТА
ФАЙЛЫ
СЕРВЕРЫ
1 КОРПОРАТИВНЫЙ СЕГМЕНТ
ВНУТРЕННИЙ ТРАФИК
HUNTBOX
POLYGON
SENSOR
Отчеты
Файлы
ICAP Почта Файлы
Индикаторы
События
Файлы
SENSOR INDUSTRIAL
ФАЙРВОЛ
HUNTPOINT
ИНЖЕНЕР
ОПЕРАТОР
АСУ
ПЛК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

Схема интеграции



Выявление киберугроз OT-сегменту и целевых атак на всех этапах

Получение доступа

- Передача вредоносного ПО в технологическую сеть
- Горизонтальное перемещение злоумышленников между сегментами

Разведка и сбор данных

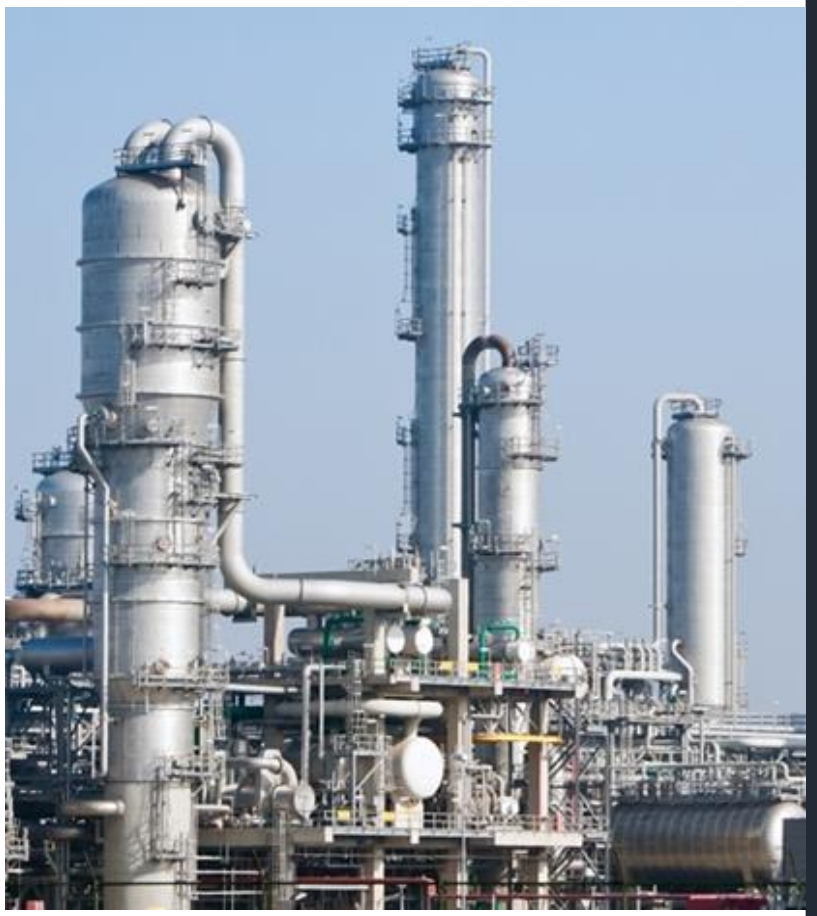
- Изучение топологии технологической сети атакующими
- Анализ устройств, подключенных к технологической сети

Закрепление в сети

- Эксплуатация уязвимостей и нарушение целостности прошивок на подключенных устройствах и сетевом оборудовании

Исполнение атаки

- Модификация алгоритмов работы программ
- Нарушение технологического процесса
- Вывод оборудования из строя



Почему Group-IB THF Industrial

Включенные услуги мониторинга 24/7

Прямой доступ к экспертам CERT-GIB с многолетним опытом. Помощь в мониторинге, реагировании, охоте за угрозами, расследовании инцидентов

Одно решение, работает как единое целое

Отдельные модули не требуют интеграционных работ, автоматизируют корреляцию событий между различными детектирующими компонентами и показывают общую картину

Доступ к уникальным данным системы киберразведки

Технологии сбора данных, доступ к закрытым источникам, данные «с поля боя» – с машин и серверов атакующих, поступающие в THF из системы киберразведки с мировым признанием

Собственные разработки и передовые технологии

Разработчики и изобретатели Group-IB – обладатели десятков патентов в разных странах мира на технологии по обнаружению и борьбе с неизвестными угрозами и целевыми атаками

GROUP IB

Предотвращаем и расследуем киберпреступления с 2003 года

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