DATASHEET

Group-IB Threat Hunting Framework / Huntpoint

Group-IB Threat Hunting Framework / Huntpoint

Threat Hunting Framework — комплексное решение, предназначенное для выявления сложных и целевых атак и неизвестных угроз, охоты за угрозами как внутри защищаемого периметра, так и за его пределами, реагирования на инциденты и их расследования.

Решаемые задачи:

- Защита корпоративной электронной почты от целевого фишинга и рассылок, содержащих ВПО
- Защита сетевого периметра, серверов и АРМ пользователей от шифровальщиков, троянов, червей, вирусов, кейлогеров и шпионского ПО, в том числе распространяемого в неконтролируемых сетевых потоках
- Защита инфраструктуры от наблюдения и управления злоумышленниками
- Защищенная передача файлов между файловыми хранилищами
- Аналитический инструмент по изучению ВПО
- Защита систем клиента от ВПО с помощью API
- Защита рабочих станций и серверов от потенциально нежелательных приложений и недоверенных устройств (Roadmap 2021)
- Обеспечение удаленного реагирования на инциденты специалистами CERT-GIB и криминалистической лаборатории Group-IB
- Проведение threat hunting в защищаемой инфраструктуре
- Выявление и исследование инфраструктуры злоумышленников
- Сбор криминалистически значимых данных и восстановление полной хронологии атаки – от сетевого соединения до вектора заражения
- Контроль передаваемых артефактов в зашифрованном трафике.
- Контроль зашифрованного трафика в сети
- Защита технологических сетей от нелегитимных устройств передачи данных
- Защита технологических сетей от неразрешенных модификаций ПЛК
- Защита технологических сетей от подмены функций технологических протоколов со стороны злоумышленников
- Защита технологических сетей от атак, приводящих к разрушению оборудования (и как следствие, к техногенным авариям)

Решение Threat Hunting Framework состоит из следующих модулей:

Huntbox

Платформа автоматизированного анализа и корреляции событий, а также обеспечения процесса охоты за угрозами и выявления действий атакующих группировок, направленных на клиента.

Sensor

Модуль, предназначенный для выявления угроз на сетевом уровне за счет глубокого анализа сетевого трафика. Используется для интеграции с IT-системами клиента.

Sensor Industrial

Модуль, предназначенный для защиты технологической сети от целевых атак и обеспечения контроля целостности программного обеспечения АСУ ТП за счет анализа промышленных протоколов и комплексной защиты корпоративной сети.

Polygon

Платформа для детонации ВПО. Модуль, предназначенный для детектирования угроз, за счет поведенческого анализа электронных писем, файлов и содержимого ссылок в изолированной среде.

Huntpoint

Модуль, предназначенный для защиты рабочих станций пользователей от угроз на основе методов фиксации полной хронологии событий на АРМ, обнаружения аномального поведения, блокировки вредоносного файла, изоляции хоста и сбора криминалистически значимых данных.

Decryptor

Модуль, предназначенный для расшифровки TLS/SSL-трафика в защищаемой инфраструктуре. Реализована поддержка российских протоколов шифрования по ГОСТ.

CERT-GIB

Услуги мониторинга событий и выявления инцидентов, исследования ВПО, локализации инцидентов и предоставления рекомендаций.

CERT-GIB является партнером IMPACT, аккредитован сообществами FIRST, Trusted Introducer, сертифицирован Университетом Карнеги-Меллона и обладает лицензией на использование товарного знака «CERT».

Huntpoint

Huntpoint – модуль продукта Group-IB Threat Hunting Framework, позволяющий контролировать и защищать АРМ пользователей от целевых атак, а также проводить сбор дополнительной контекстной информации для выявления вредоносной активности на хосте.

Технический подход

1. Постоянный сбор криминалистически значимых данных с АРМ пользователя
2. Автоматическая отправка файловых объектов на поведенческий анализ * (необходим Polygon)
3. YARA-правила для дополнительной тонкой кастомизации анализа файлов и ссылок *(необходим Polygon)
4. Автоматическая блокировка запуска ВПО
5. Автоматическое перемещение ВПО в карантин для дальнейшего анализа
6. Автоматическая блокировка запущенных вредоносных процессов
7. Доступ к общей базе вредоносных объектов Group-IB для проверки репутации объекта без необходимости поведенческого анализа
8. Блокировка возможностей сетевого взаимодействия АРМ по сигналу аналитика
9. Threat hunting по собираемым данным
10. Варианты поддерживаемых ОС:
    - Windows 7, 8/8.1, 10;
    - Windows Server 2008;
    - Windows Server 2012(r2);
    - Windows Server 2016;
    - Windows Server 2019.
11. Локальное хранение собираемых данных в случае потери связи с Huntbox
12. Централизованное управление из Huntbox с on-prem/cloud-вариантами развертывания

Централизованное управление

Huntbox предоставляет:

- графический интерфейс управления установленными модулями;
- данные о событиях и инцидентах за длительный период и осуществляет корреляцию по ним;
- атрибуцию событий к ВПО и атакующим группировкам;
- инструменты для поиска угроз (Threat Hunting) и удаленной форензики.

Архитектура Threat Hunting Framework

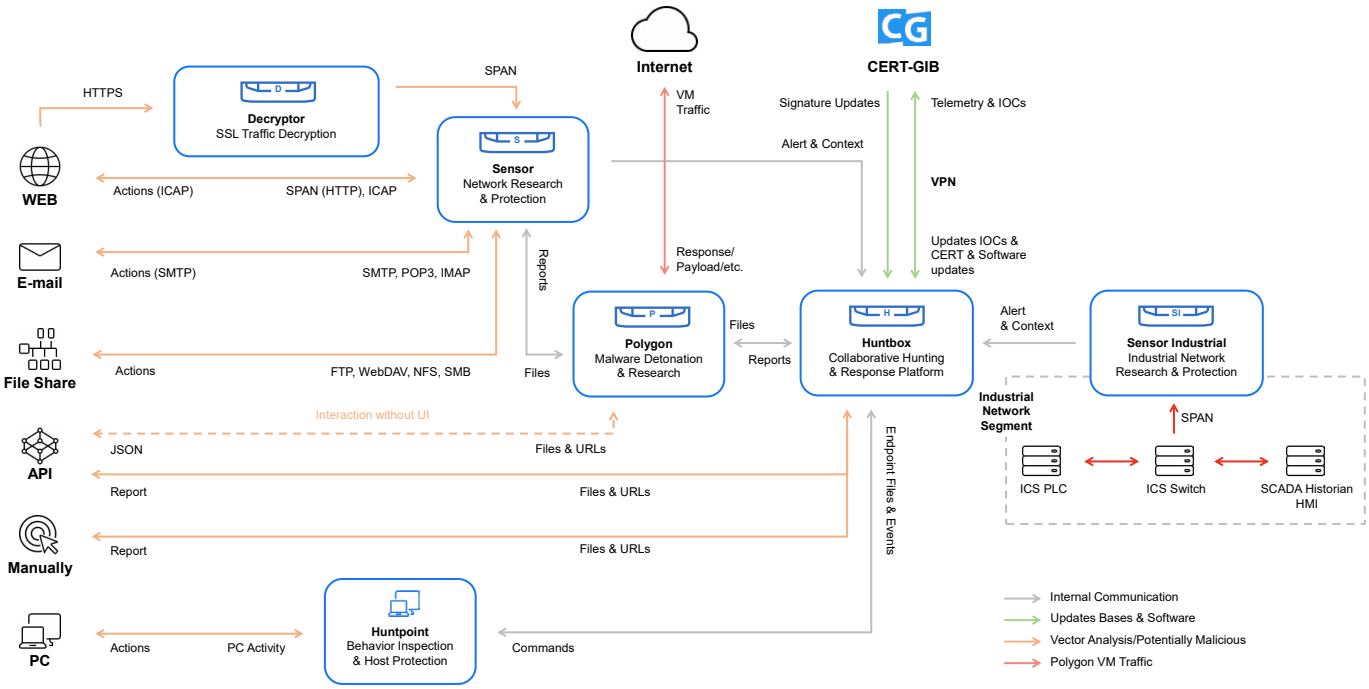
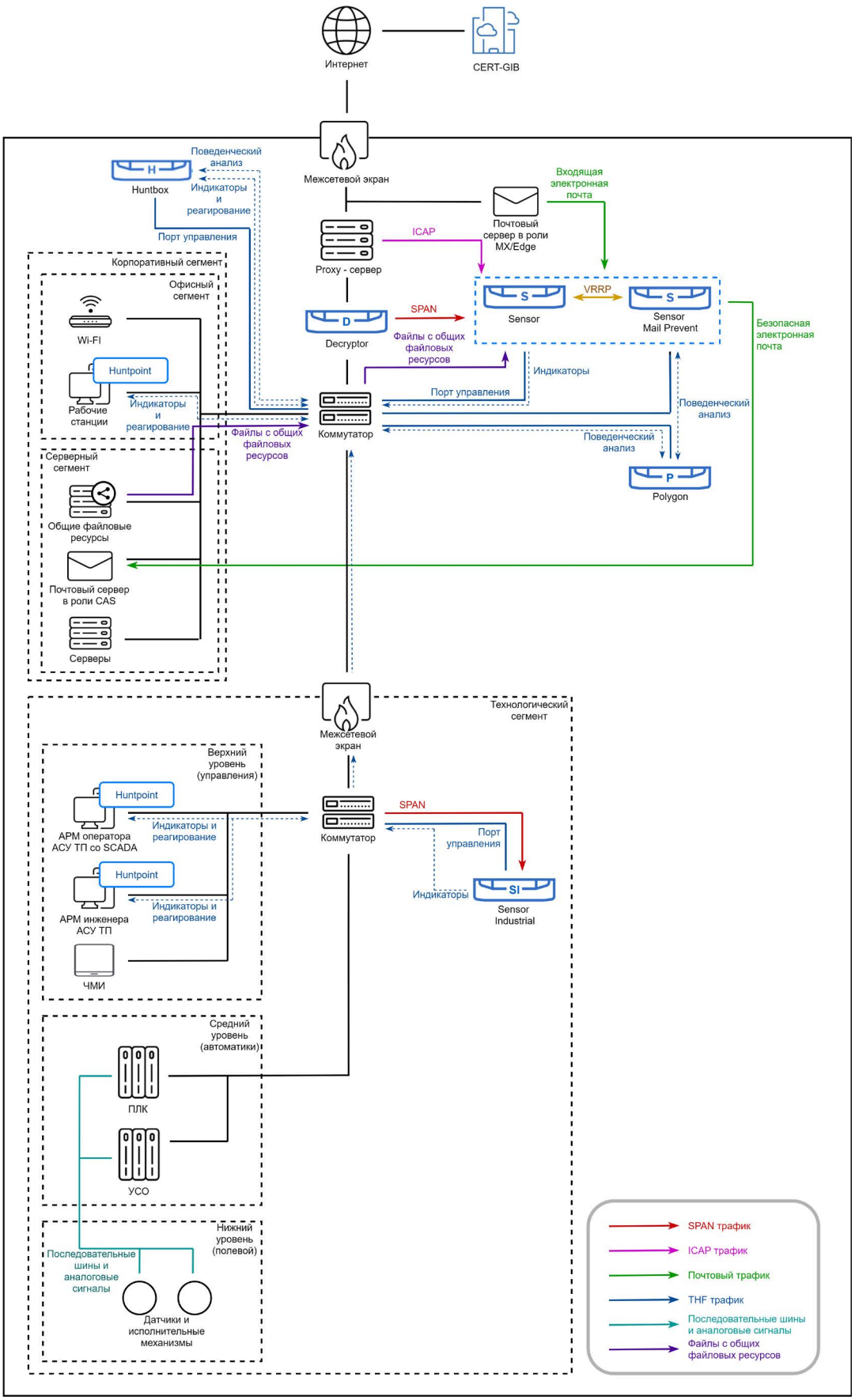


Схема интеграции



→

Свяжитесь с нами, чтобы провести тест-драйв Threat Hunting Framework

thf@group-ib.com

→

Познакомьтесь с Group–IB

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

→

Узнайте больше о возможностях Threat Hunting Framework