DATASHEET

Group-IB Threat Hunting Framework / Decryptor

Group-IB Threat Hunting Framework / Decryptor

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».

Decryptor

Decryptor – опциональный модуль продукта Group-IB Threat Hunting Framework, представляющий собой программно-аппаратный комплекс, предназначенный для вскрытия и анализа* содержимого шифрованных сессий, позволяющий повышать видимость и уровень контроля трафика защищаемой инфраструктуры, а также качество обнаружения целевых атак.

Технический подход

1. **Расшифрование SSL/TLS-сессий в любых приложениях «на лету» за счёт установки «в разрыв»**

2. **Автоматическое выявление шифрованного трафика вне зависимости от используемых сервисов**

3. **Передача копии расшифрованных сессий во внешние анализирующие системы, в том числе на Sensor**

4. **Поддерживаемые режимы работы:**
   - **Режим моста** — в этом режиме Decryptor функционирует на уровне L2 сетевой модели OSI.
   - **Режим шлюза** — в этом режиме Decryptor функционирует на уровне L3 сетевой модели OSI, являясь шлюзом для пользовательской сети.

5. **Формирование автоматических исключений при работе решения**

6. **Работа в режиме обратного прокси для контроля шифрованного трафика при обращении к корпоративным ресурсам**

7. **Поддержка современных стандартов и протоколов шифрования, в том числе:**
   - Все современные наборы Cipher Suites (RSA, DHE, ECDHE, ChaCha, Camilla и т.д.);
   - Поддержка ГОСТ шифрования (GOST2012-GOST8912-GOST8912, GOST2001-GOST89- GOST89);
   - Поддержка TLS 1.1 - 1.3 (включая RFC 8446) и механизмов SSL handshake.

Централизованное управление

Варианты поставки:

- **HW** – поставка готового ПАК от компании Group-IB
- **SW** – поставка образа для установки на серверном оборудовании клиента
- **Virtual** – поставка образа для установки на виртуальных мощностях клиента

Архитектура Threat Hunting Framework

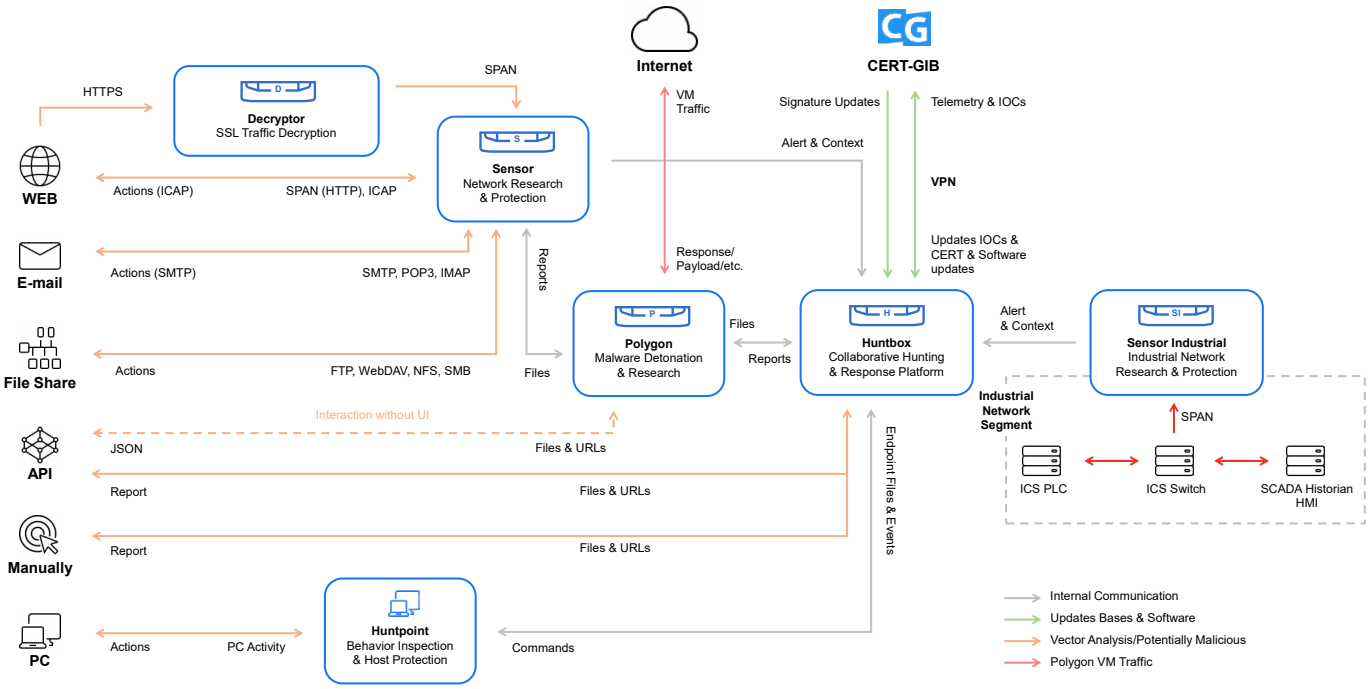
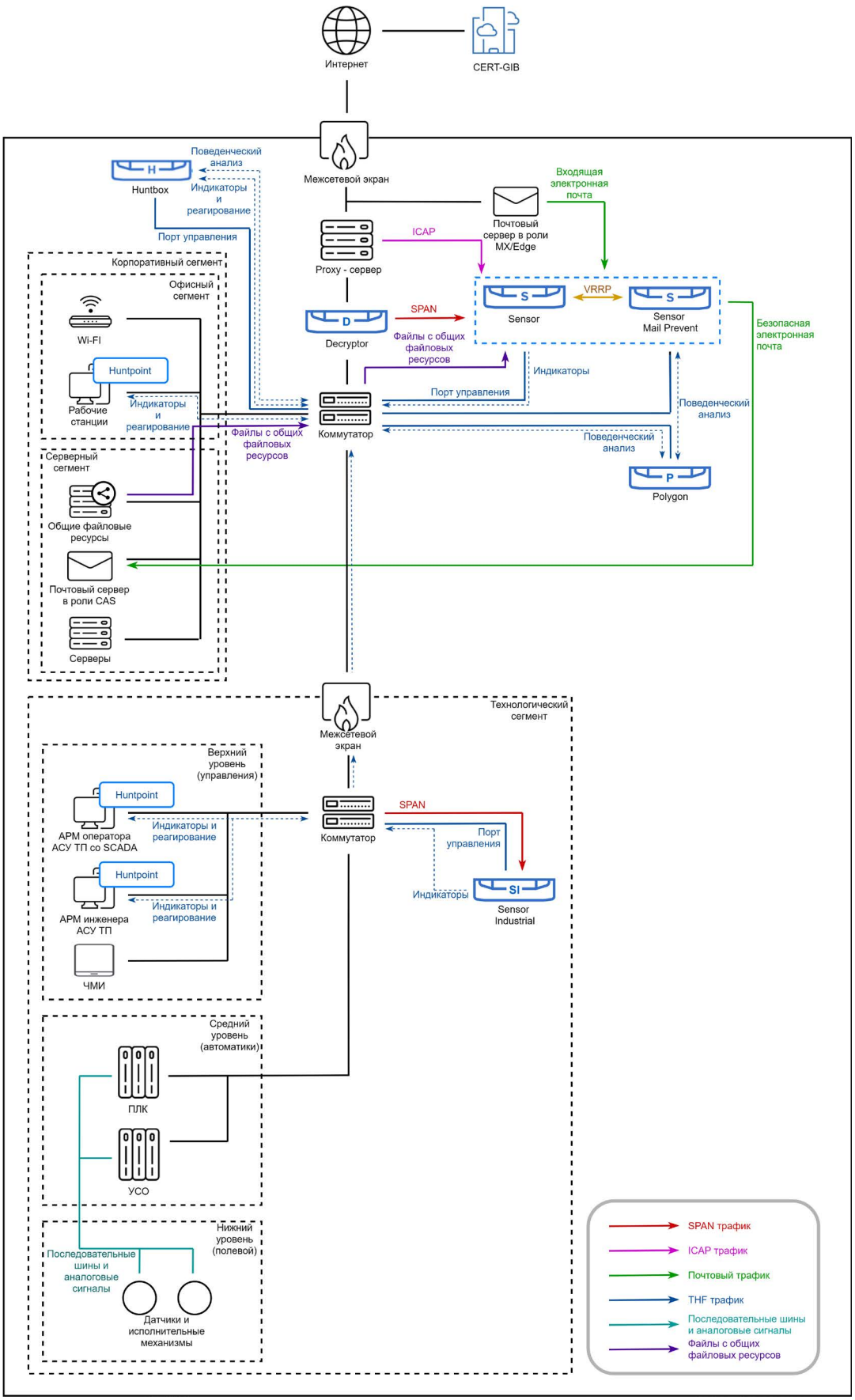


Схема интеграции



→

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