DATASHEET

Group-IB Threat Hunting Framework / CERT-GIB

Group-IB Threat Hunting Framework / CERT-GIB

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».

CERT-GIB

CERT-GIB — Центр круглосуточного реагирования на инциденты информационной безопасности

Технический подход

1	**Как работает CERT-GIB**	• Круглосуточный мониторинг • Звонок в Group-IB по номеру **+7 (495) 984-33-64** • Получение запроса на email **response@cert-gib.com**	• Получение оповещения об инциденте через форму на сайте
2	**Анализ и классификация полученных данных**	• Определение источника угрозы • Оценка уровня опасности инцидента	• Получение сведений об угрозе из системы Threat Intelligence
3	**Первая помощь в рамках реагирования**	• Предоставление четких инструкций по локализации инцидента • Блокировка фишинговых и других опасных ресурсов	• Проактивный мониторинг угроз для предотвращения повторных инцидентов
4	**Реагирование и проведение расследования**	• Локализация масштабных инцидентов • Сбор и анализ цифровых доказательств	• Идентификация злоумышленника, поддержка заказчика в дальнейшем расследовании

Эффективная работа с Huntbox

- Huntbox предоставляет единый интерфейс для управления детектирующей инфраструктурой заказчиков, автоматизированного анализа, хранения всех событий и алертов и проведения ретроспективного анализа инцидентов.
- Использование Huntbox в работе CERT-GIB позволяет эффективнее управлять инцидентами, дает доступ аналитикам к обширной базе событий и сокращает время на обработку инцидентов благодаря их автоматической группировке и корреляции в системе.

Архитектура Threat Hunting Framework

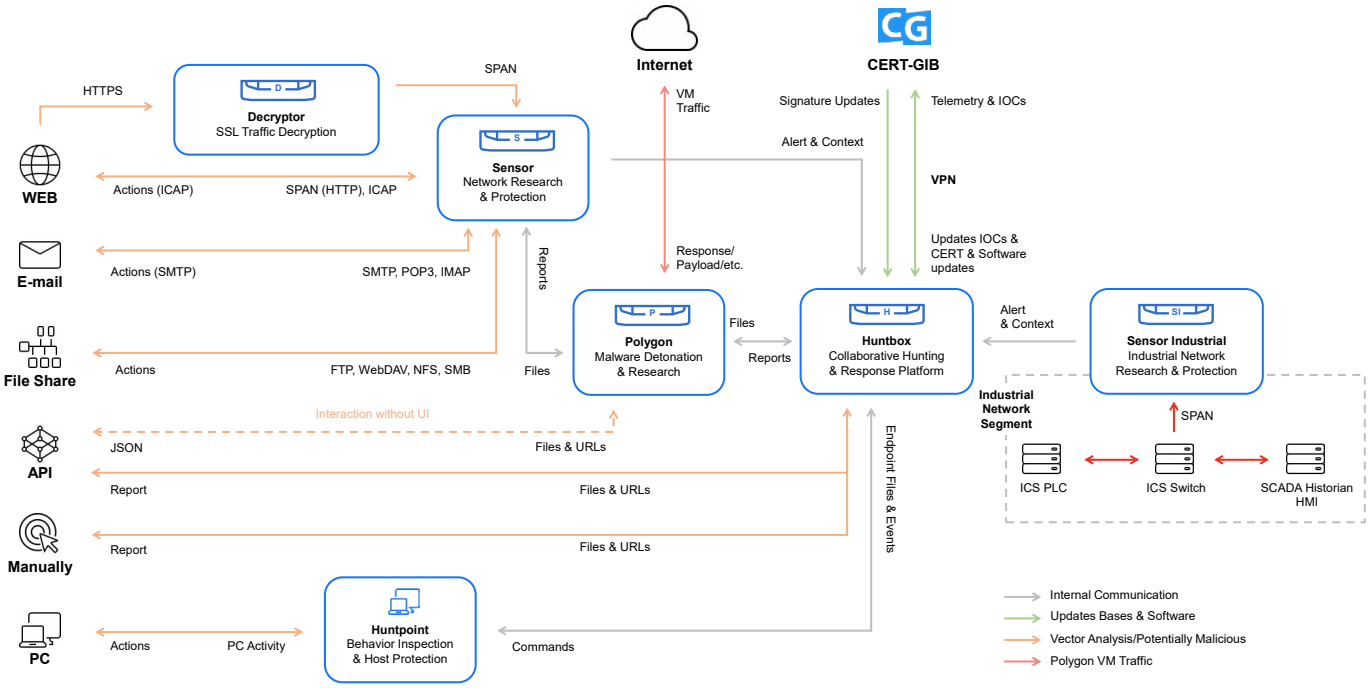
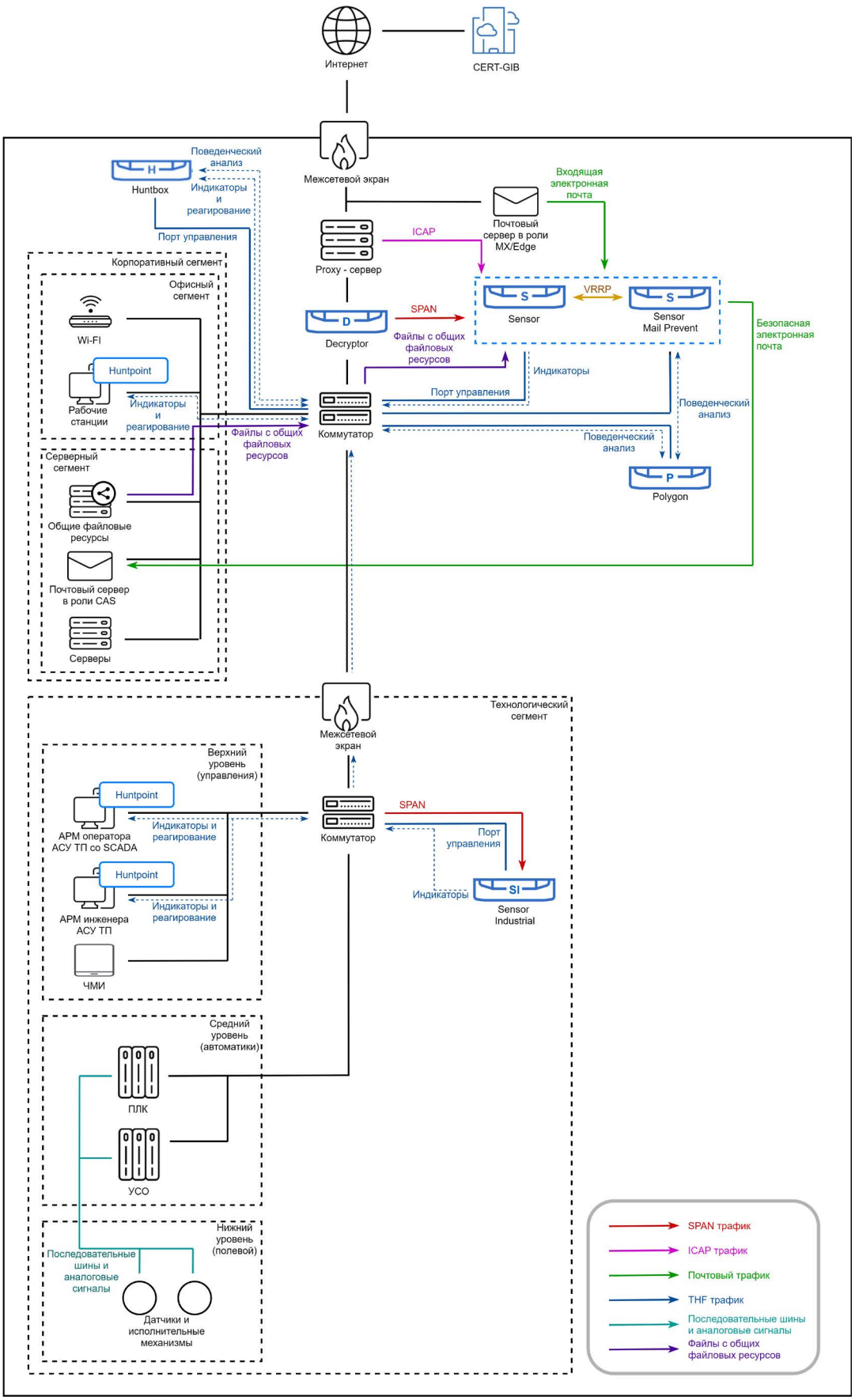


Схема интеграции



→

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