DATASHEET

Group-IB Threat Hunting Framework / Huntbox

Group-IB Threat Hunting Framework / Huntbox

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».

Huntbox

Huntbox — это платформа, включающая в себя набор инструментов, необходимых для процессов мониторинга, реагирования на инциденты, а также поиска угроз в защищаемой инфраструктуре и в сети Интернет.

Технический подход

1. **Автоматическая атрибуция событий, алертов и инцидентов к применяемым в атаке ВПО, техниками, а также к атакующим группировкам**

2. **Графовый анализ – технология наблюдения за инфраструктурой злоумышленников**

3. **Threat hunting – поиск и проверка предположений о компрометации сети по сырым данным из трафика и АРМ * (необходим Huntpoint и/или Sensor)**

4. **Управление модулями Threat Hunting Framework**

5. **Блокировка ВПО и активности АРМ в автоматическом или в ручном режиме * (необходим Huntpoint)**

6. **Инструменты мониторинга инцидентов ИБ:**
   - Аккумулирование и хранение всех событий ИБ, выявленных модулями
   - Корреляция множества событий в единую запись по цели атакующего
   - Корреляция многоцелевой и многовекторной атаки в единый инцидент

7. **Настраиваемые оповещения аналитиков THF по состояниям работы решения**

8. **Интеграция с аналитическими системами:**
   - SysLog-интеграция с SIEM системами
   - SNMP-интеграция с системами мониторинга состояния

9. **Интеграция с системами оркестрации событий ИБ и платформами управления инцидентами по API для предоставления отчётов детонации ВПО * (необходим Polygon)**

10. **Интеграция с системами сбора и корреляции событий ИБ из различных источников через API для передачи полного контекста выявленных инцидентов.**

Централизованное управление

Четыре режима работы комплекса

- Полная изоляция без обновлений ПО и решающих правил;
- Одностороннее обновление ПО, сигнатур и IoCs, инициируемое Huntbox;
- Двустороннее соединение с инфраструктурой Group-IB. Функциональность выявления скрытой инфраструктуры атакующего. Обновление инициируется Group-IB. Мониторинг состояния оборудования - со стороны Group-IB.
- Сервис мониторинга и техподдержки от CERT-GIB 24/7. Автоматизированный Threat Hunting.

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
- **Cloud** – использование центральной облачной версии Huntbox

Архитектура Threat Hunting Framework

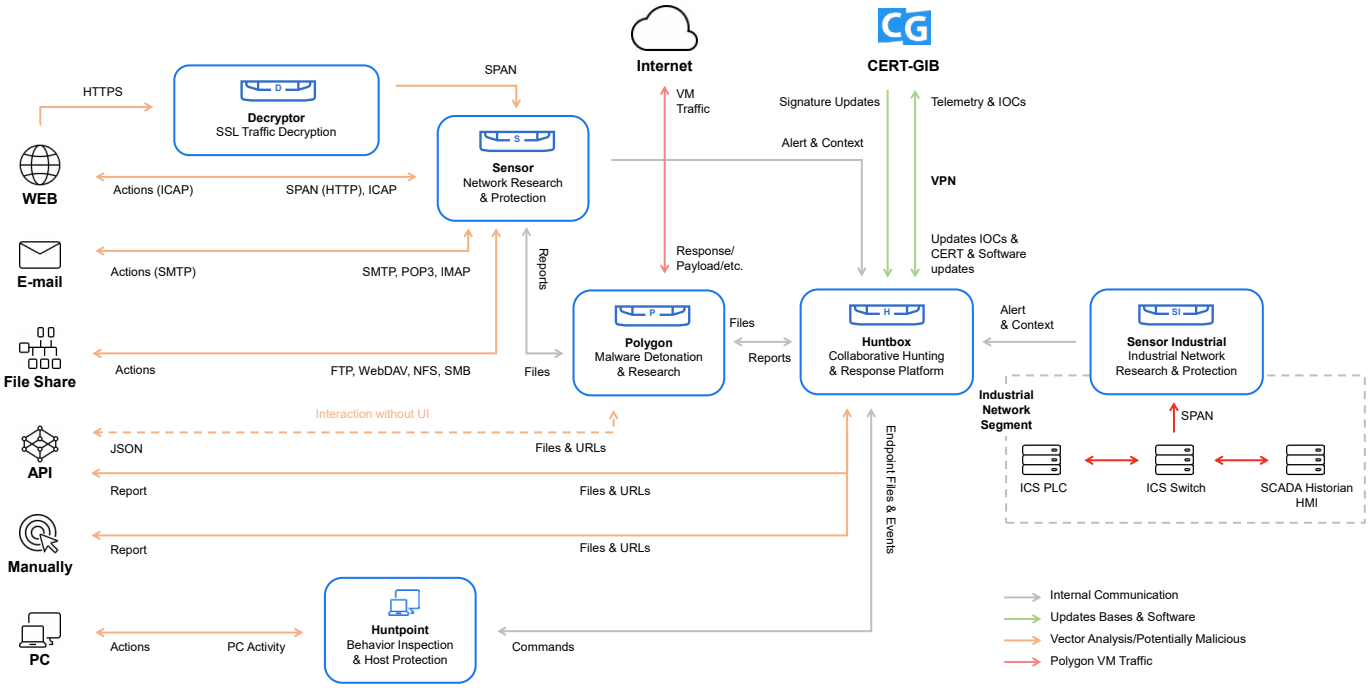
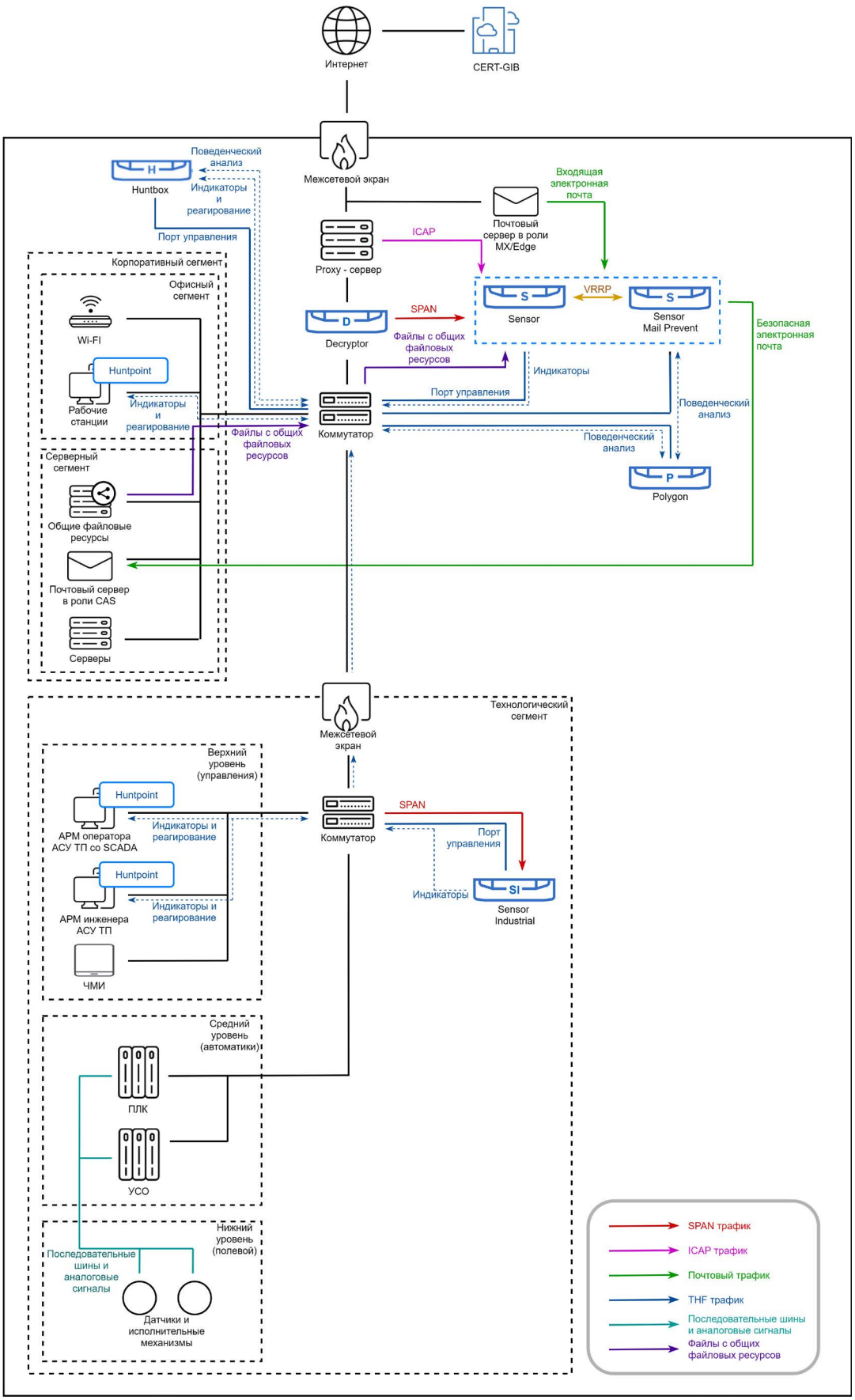


Схема интеграции



	Huntbox Standard	Huntbox Enterprise	Huntbox Storage
Количество подключенных Endpoint, шт.	<1000	1000-2000	*
Емкость накопителя	2x 960 GB(SSD) + 4x 1,2 TB(HDD)	2x 960 GB(SSD) + 4x 1,2 TB(HDD)	2x 960 GB(SSD) + 2x 1,2 TB(HDD)
Сетевые интерфейсы	4x 1000 BASE-T	4x 1000 BASE-T	4x 1000 BASE-T
Форм-фактор	1U	1U	1U
Порт IPMI (задняя панель)	1	1	1
Порты USB (задняя панель)	2	2	2
Последовательный порт (задняя панель)	1	1	1
Порт VGA	1	1	1
Блок питания переменного тока (Вт)	2 x 750	2 x 750	2 x 550
Максимальная потребляемая мощность (Вт)	705	705	517
Размеры (ВхШхГ), мм	43 x 434 x 755	43 x 434 x 755	43 x 434 x 755
Вес устройства в отдельности (кг)	22	24	19,9
Heat dissipation (max)	2x 2891 BTU/h	2x 2891 BTU/h	2x 2107 BTU/h
Сертификаты соответствия	ТР ТС 004/2011; ТР ТС 020/2011	ТР ТС 004/2011; ТР ТС 020/2011	ТР ТС 004/2011; ТР ТС 020/2011
Соответствие нормативам	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE
Рабочая температура	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment
Рабочая относительная влажность	10% to 80% relative humidity with 29°C (84.2°F) maximum dew point	10% to 80% relative humidity with 29°C (84.2°F) maximum dew point	10% to 80% relative humidity with 29°C (84.2°F) maximum dew point

* HB Storage используется при увеличении объема и длительности хранения информации. HB Storage используется совместно с HB Standard/ Enterprise.

→

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