DATASHEET

Group-IB Threat Hunting Framework / Sensor

Group-IB Threat Hunting Framework / Sensor

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».

Sensor

Sensor — модуль продукта Group-IB Threat Hunting Framework, предназначенный для анализа входящих и исходящих пакетов данных. Используя собственные сигнатуры и поведенческие правила Sensor позволяет выявлять взаимодействие зараженных устройств с командными центрами злоумышленников, общие сетевые аномалии и необычное поведение устройств в сети. Модуль также позволяет извлекать объекты анализа из различных источников для передачи в Polygon.

Технический подход

1	**Использование технологии Machine learning для:**	• Выявления горизонтального перемещения по сети (lateral movement); • Выявления эксфильтрации данных в прикладных протоколах; • Выявления сетевых аномалий.	
2	**Сигнатурный анализ:**	• Эвристический подход при анализе сетевых потоков; • Обновление не менее трех раз в сутки;	• Возможность подключать собственные сигнатуры.
3	**YARA-правила для дополнительной тщательной кастомизации анализа файлов и ссылок *(Использование Polygon, Huntpoint)**		
4	**Сбор метаинформации о сетевой активности для охоты за угрозами**		
5	**Извлечение файлов из потоков данных:**	• сетевой трафик; • файловые хранилища; • почтовый трафик; • прокси сервера (ICAP интеграция);	• ссылки; • SSL-трафик* (совместно с Decryptor).
6	**Анализ почтовых сообщений, в т.ч. ретроспективный анализ на предмет отложенных атак* (совместно с Polygon).**		
7	**Внедрение комплекса в следующие потоковые системы:**	• Почтовая подсистема (SMTP/S, POP3/S, IMAP/S); • Общие файловые хранилища (SMB, WebDAV, NFS, FTP);	• Прокси-сервера с поддержкой протокола ICAP;
8	**Интеграция с аналитическими системами:**	• SysLog-интеграция с SIEM системами; • SNMP-интеграция с системами мониторинга состояния.	

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.

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

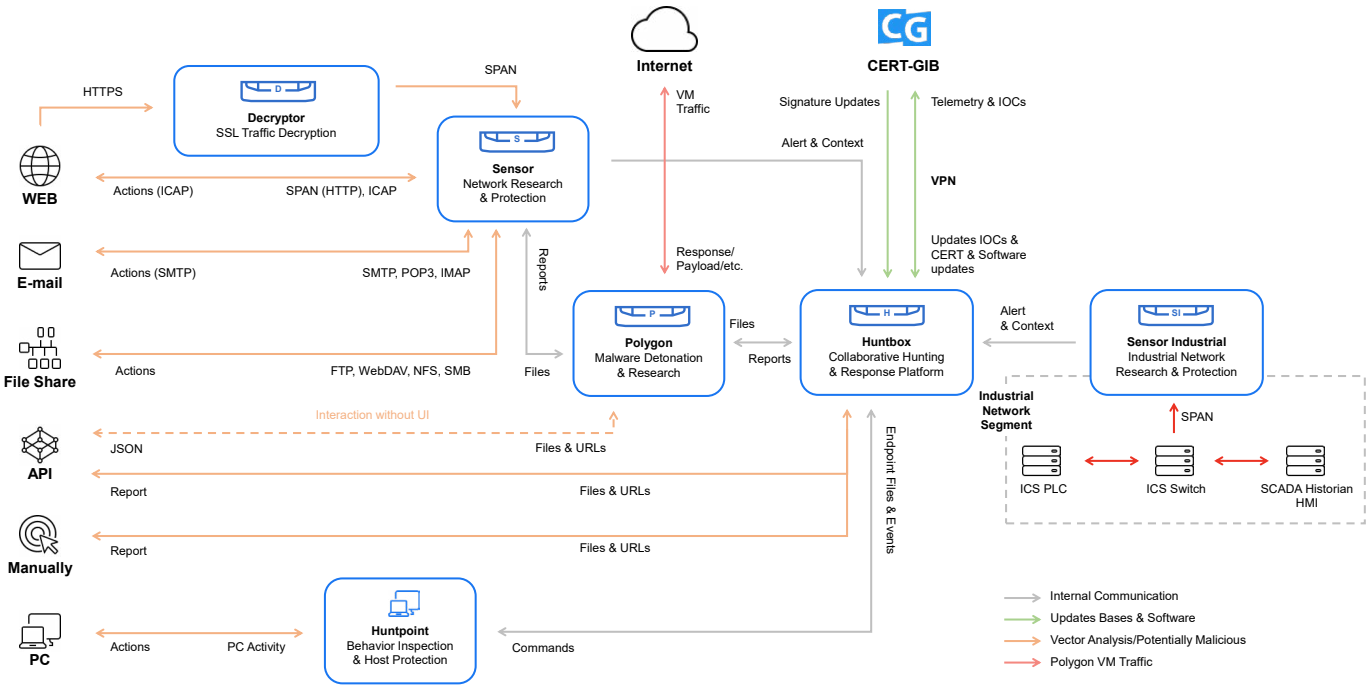
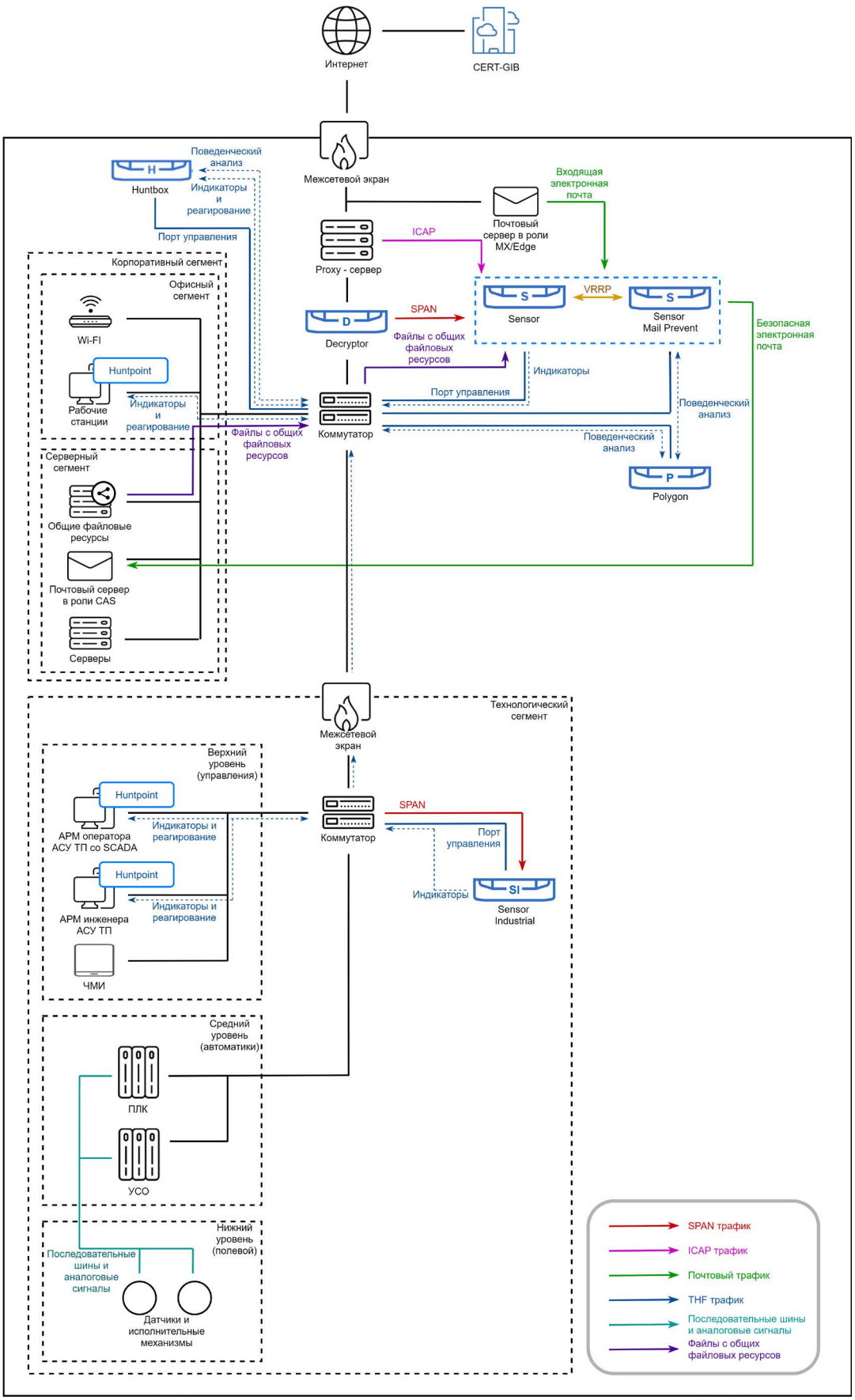


Схема интеграции



	Sensor-250	Sensor-500	Sensor-1000	Sensor-2000	Sensor-5000	Sensor-10000
Пиковая производительность, Мбит/сек	250	500	1000	2000	5000	10000
Порты мониторинга (SPAN)	4x 10/100/1000 BASE-T	4x 10/100/1000 BASE-T	4x 10/100/1000 BASE-T	4x 1000 BASE-T 2x 10GBASE-SR/LR	4x 1000 BASE-T 2x 10GBASE-SR/LR	4x 1000 BASE-T 2x 10GBASE-SR/LR
Сетевые порты (LAN)	2x 1000 BASE-T	2x 1000 BASE-T	2x 1000 BASE-T	2x 1000 BASE-T	2x 1000 BASE-T	2x 1000 BASE-T
Порт IPMI (задняя панель)	1	1	1	1	1	1
Форм-фактор	1U	1U	1U	1U	1U	1U
Емкость накопителя	2 x 1,2 TB SAS	2x 1,2 TB SAS	2x 1,2 TB SAS	2x1,2 TB SAS	2x 1,2 TB SAS	2x 1,2 TB SAS
Порты USB (задняя панель)	2	2	2	2	2	2
Порты USB (передняя панель)	2	2	2	2	2	2
Последовательный порт (задняя панель)	1	1	1	1	1	1
Порт VGA	1	1	1	1	1	1
Блок питания переменного тока (Вт)	1 x 250	1 x 250	1 x 250	2 x 550	2 x 550	2 x 750
Максимальная потребляемая мощность (Вт)	235	235	235	517	517	705
Размеры (ВхШхГ), мм	43 x 434 x 552	43 x 434 x 552	43 x 434 x 552	43 x 434 x 678	43 x 434 x 678	43 x 434 x 678
Вес устройства в отдельности / в фунтах (кг)	11	11	11	16	16	16
Heat Dissipation (max)	1039 BTU/h	1039 BTU/h	1039 BTU/h	2x 2107 BTU/h	2x 2107 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	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	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	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	0% to 80% Relative Humidity with 29 °C (84.2°F) maximum dew point	0% to 80% Relative Humidity with 29 °C (84.2°F) maximum dew point	0% to 80% Relative Humidity with 29 °C (84.2°F) maximum dew point	0% to 80% Relative Humidity with 29 °C (84.2°F) maximum dew point	0% to 80% Relative Humidity with 29 °C (84.2°F) maximum dew point	0% to 80% Relative Humidity with 29 °C (84.2°F) maximum dew point

Технические характеристики виртуального Sensor*

CPU 6 ядер, 2 потока на каждое ядро

ОЗУ 32 ГБ

HDD 480 ГБ

СЕТЬ минимум 2 сетевых интерфейса: для порта управления и для приема зеркалируемого трафика.

*Рассчитано для нагрузки 250 Мбит/сек на SPAN-интерфейсе.

→

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