



|GROUP|IB|

|GROUP|IB|

DATASHEET

Group-IB Threat Hunting
Framework / Sensor Industrial

■ Group-IB Threat Hunting Framework / Sensor Industrial

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, предоставляемые мониторинг событий и выявление инцидентов, исследование ВПО, локализация инцидентов и рекомендации.

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

■ Sensor Industrial

Sensor Industrial — решение Group-IB Threat Hunting Framework, предназначенное для детектирования атак на ранних стадиях в технологическом сегменте предприятия. Анализируя пакеты данных технологического трафика собственными сигнатурами и поведенческими правилами, Sensor Industrial позволяет выявлять передачу нелегитимных команд управления между уровнями АСУ ТП, обнаруживать использование служебных команд АСУ ТП с целью перепрошивки ПЛК, подмены программы управления, остановки технологических процессов и других нарушений.

■ Технический подход

- | | | |
|---|--|--|
| 1 Алгоритмы машинного обучения для выявления: | <ul style="list-style-type: none"> • Lateral Movement из корпоративной сети • Выявление аномалий в прикладных протоколах | <ul style="list-style-type: none"> • Изменения в оборудовании сети АСУ ТП • Изменения в сетевых сессиях АСУ ТП-сегмента |
| 3 Пассивный контроль целостности ПО в технологическом оборудовании | | |
| 2 Контроль команд, посылаемых в технологическое оборудование: | <ul style="list-style-type: none"> • подключение к технологическому оборудованию; • остановка технологического процесса; | <ul style="list-style-type: none"> • модификация/скачивание/загрузка программы управления. |
| 2 Предотвращение атак из корпоративного сегмента: | <ul style="list-style-type: none"> • Блокировка целевых почтовых рассылок * (необходимы Sensor + Polygon для inline-режима) • Блокировка скачивания ВПО из сети Интернет * (Необходима ICAP интеграция с Web-прокси) | <ul style="list-style-type: none"> • Удаление ВПО из файловых хранилищ * (необходим Polygon) • Блокировка атак на уровне АРМ * (необходим Huntpoint) |
| 6 Поддержка анализа открытых и проприетарных протоколов производителей технологического оборудования | | |
| 2 Интеграция с аналитическими системами: | <ul style="list-style-type: none"> • SysLog-интеграция с SIEM системами • SNMP-интеграция с системами мониторинга состояния | |
| 2 Поддерживаемые протоколы анализа: | <ul style="list-style-type: none"> • Сетевые протоколы DNS, FTP, HTTP, RDP, SMB, SMTP, SSH, POP3 и др. • Открытые (документированные) промышленные протоколы: CIP, DNP3, IEC 60870-5-104, | <ul style="list-style-type: none"> IEC 61850-MMS, Modbus TCP, OPC-DA, OPC-UA, MQTT • Проприетарные протоколы производителей оборудования АСУ ТП: Siemens, Schneider Electric, Rockwell Automation, Emerson |

■ Централизованное управление

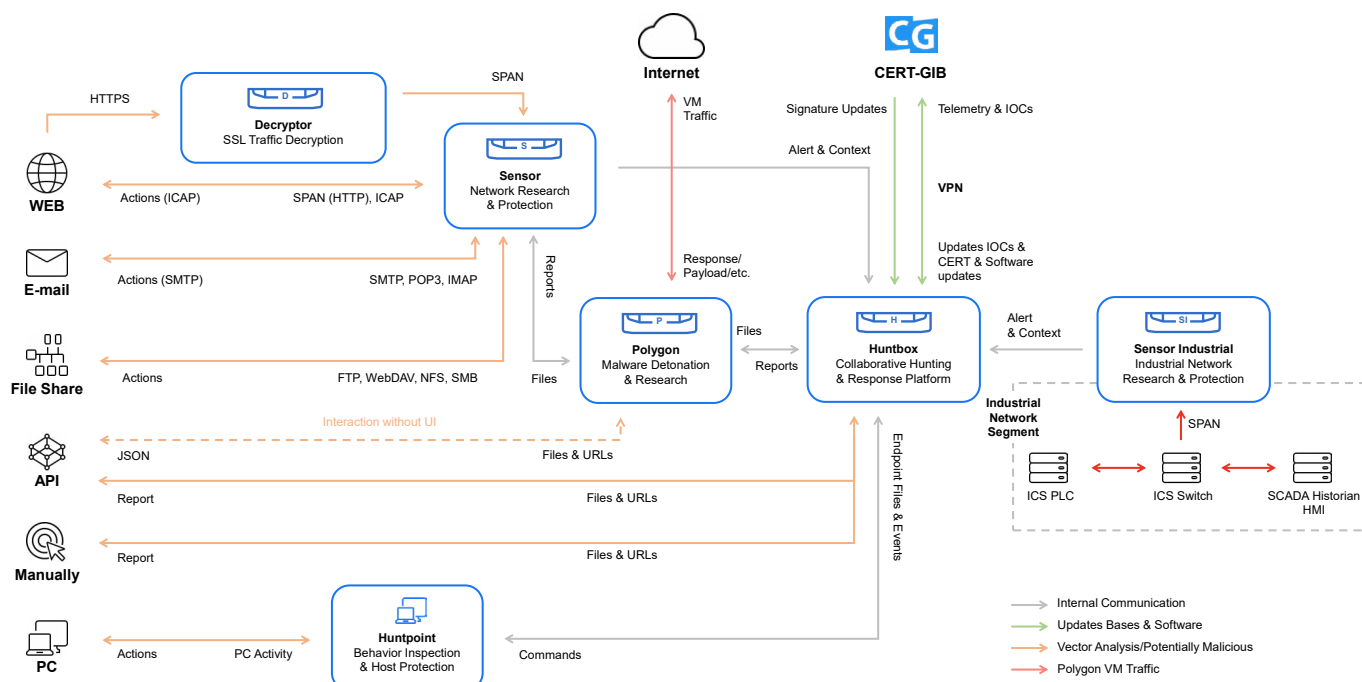
Huntbox предоставляет:

- 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.

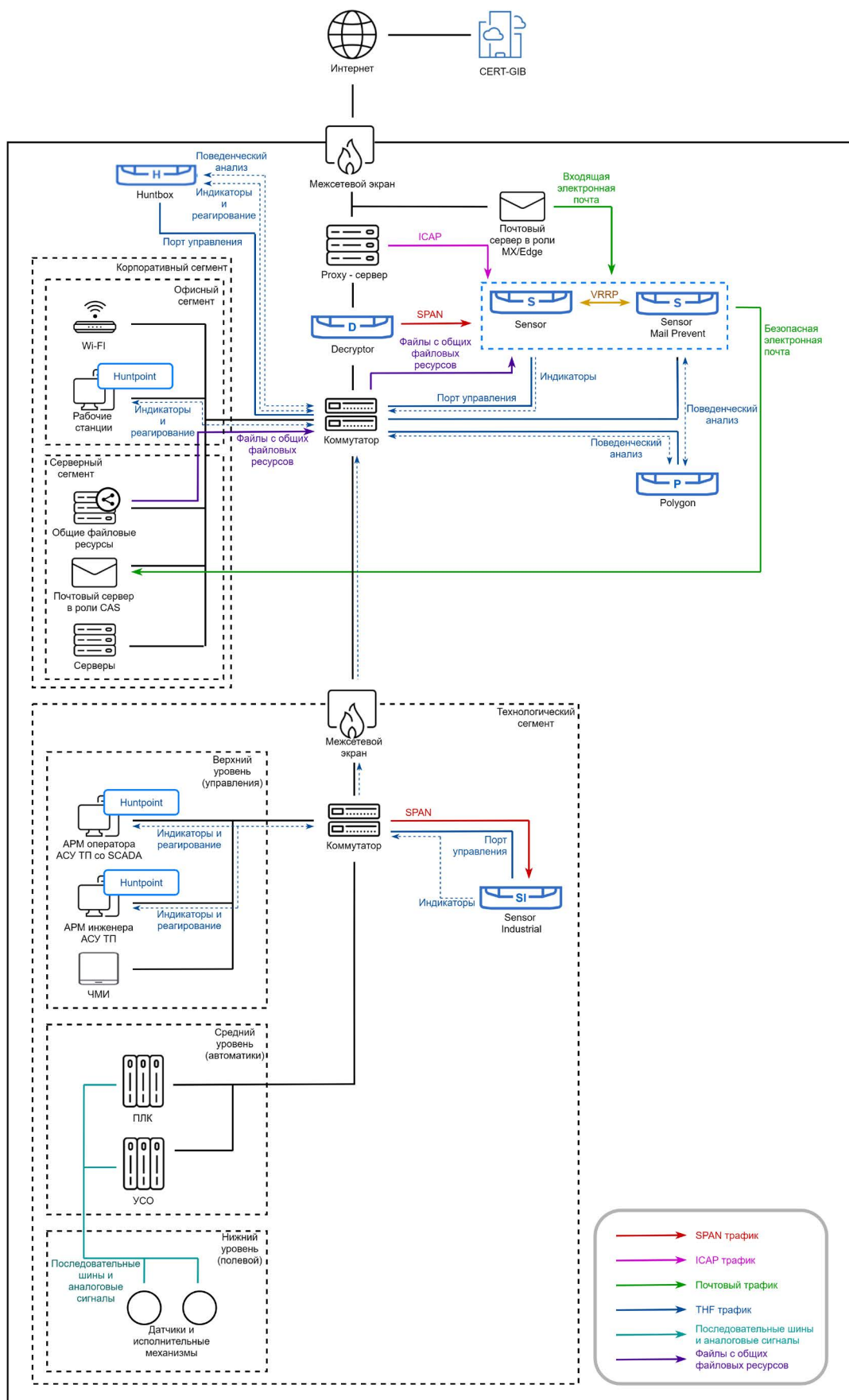
Варианты поставки:

- **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 Industrial-500	Sensor Industrial-1000	Sensor Industrial-2000
Пиковая производительность, Мбит/сек	500	1000	2000
Порты мониторинга (SPAN)	4x 10/100/1000 BASE-T	4x 10/100/1000 BASE-T	4x 1000 BASE-T 2x 10GBASE-SR/LR
Сетевые порты (LAN)	2x 1000 BASE-T	2x 1000 BASE-T	2x 1000 BASE-T
Порт IPMI (задняя панель)	1	1	1
Форм-фактор	1U	1U	1U
Емкость накопителя	2x 1,2 TB SAS	2x 1,2 TB SAS	2x 1,2 TB SAS
Порты USB (задняя панель)	2	2	2
Порты USB (передняя панель)	2	2	2
Последовательный порт (задняя панель)	1	1	1
Порт VGA	1	1	1
Блок питания переменного тока (Вт)	1 x 250	1 x 250	2 x 550
Максимальная потребляемая мощность (Вт)	235	235	517
Размеры (ВхШхГ), мм	43 x 434 x 552	43 x 434 x 552	43 x 434 x 678
Вес устройства в отдельности (кг)	11	11	16
Heat Dissipation (max)	1039 BTU/h	1039 BTU/h	2x 2107 BTU/h
Сертификаты соответствия	TP TC 004/2011 TP TC 020/2011	TP TC 004/2011 TP TC 020/2011	TP TC 004/2011 TP TC 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	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 Industrial*

CPU 4 ядра, 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.

|GROUP|IB|

|GROUP|IB|



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](https://twitter.com/GroupIB_GIB)



Узнайте больше
о возможностях
Threat Hunting
Framework

