DATASHEET

Group-IB Threat Hunting Framework / Polygon

Group-IB Threat Hunting Framework / Polygon

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».

Polygon

Polygon — модуль продукта Group- IB Threat Hunting Framework, позволяющий осуществлять поведенческий анализ файлов, извлекаемых из электронных писем, сетевого трафика, файловых хранилищ, персональных компьютеров и автоматизированных систем посредством интеграции через API или загружаемых вручную. Polygon дополняет функциональность продукта, расширяя возможности по обнаружению вредоносных файлов, нацеленных на защищаемую инфраструктуру.

Технический подход

1 **Детонация ВПО**

Автоматическое выявление необходимости использования дополнительных образов ОС или параметров и функций для выявления всех вредоносных возможностей анализируемого объекта

2 **Анализ файловых объектов из следующих потоков:**

- почтовый трафик
- веб-трафик* (ICAP-интеграция с проксирующими решениями)
- SPAN-трафик
- локальные файловые хранилища
- легитимные публичные файловые хранилища
- АРМ пользователей* (необходим Huntpoint)
- SSL-трафик* (Decryptor или ICAP)

3 **Поддержка 294 форматов анализируемых объектов**

4 **Анализ содержимого ссылок, вложенных в почтовые сообщения или файлы**

5 **Ретроспективный анализ файлов и ссылок для выявления отложенных атак**

6 **Защита от противодействия поведенческому анализу:**

- winAPI-мониторинг
- перезапуск с необходимыми временными параметрами для ВПО, учитывающих временные рамки (большая загрузка CPU, длинные паузы и т.п.)
- Использование и эмуляция реалистичных системных параметров среды анализа
- Использование крайних версий прикладного офисного ПО в среде анализа
- Ретроспективный анализ ссылочной информации
- Выявление дополнительных условий детонации ВПО
- (перезагрузка ОС, макросы закрытия / открытия приложений, запуск по времени и т.п.)
- Вскрытие многотомных контейнеров с ветвлениями
- Система эмуляции пользовательской активности (клики по определенным местам экрана, закрытие документа и т.д.)
- Компьютерное зрение
- Извлечение и выполнение дополнительных команд из реестра (не выполняющихся по умолчанию)

7 **Вскрытие запароленных архивов с учетом следующих контекстов:**

- содержимое письма
- заголовки письма
- письма в одной цепочке (соседние письма в цепочке)
- вложенные файлы
- содержимое ссылок
- внутренний словарь

8	**Мультиверсионный анализ**	Windows XP, Windows 7 - x86/x64, Windows 10 - x86/x64, ENG/RUS
9	**YARA-правила для дополнительной тщательной кастомизации анализа файлов и ссылок**	
10	**API-интеграция с системами контроля инцидентов и анализа файловых объектов для получения вердиктов детонации ВПО *(Необходим Huntbox)**	

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

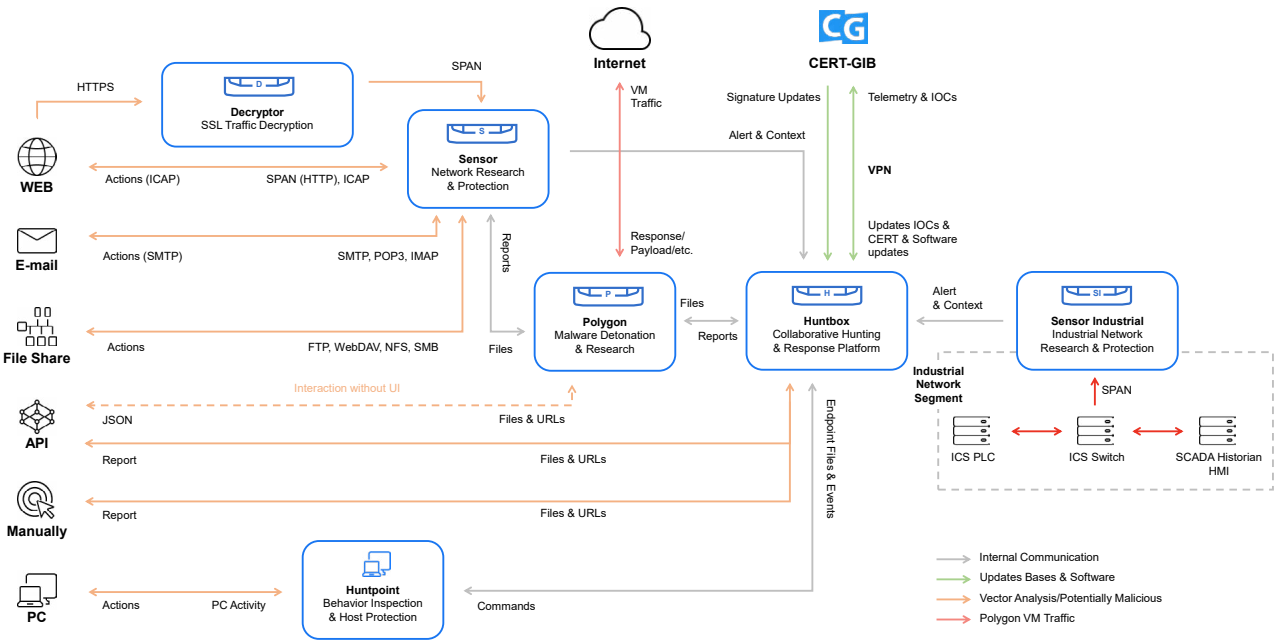
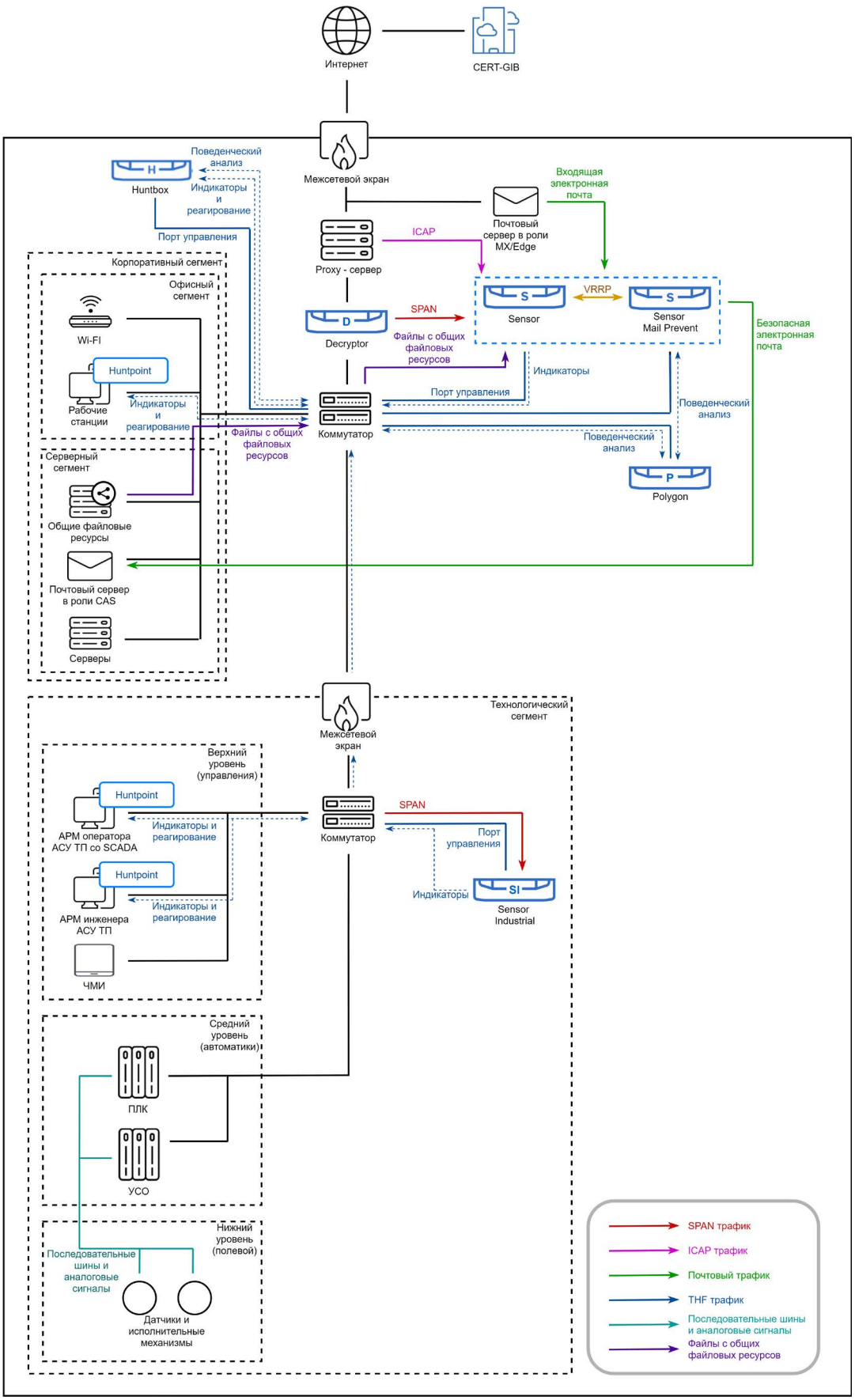


Схема интеграции



	Polygon Cloud	Polygon Standard	Polygon Enterprise
Пиковая производительность, Файлов/день	любая	9000	19000
Сетевые порты (LAN)	—	4x 10/100/1000 BASE-T	4x 10/100/1000 BASE-T
Порт IPMI (задняя панель)	—	1	1
Форм-фактор	Cloud	1U	1U
Емкость накопителя	—	2x 480GB SSD	2x 480GB SSD
Порты USB (задняя панель)	—	2	2
Порты USB (передняя панель)	—	2	2
Последовательный порт (задняя панель)	—	1	1
Порт VGA	—	1	1
Блок питания переменного тока (Вт)	—	2 x 550	2 x 550
Максимальная потребляемая мощность (Вт)	—	517	517
Размеры (ВхШхГ), мм	—	43 x 434 x 678	43 x 434 x 678
Вес устройства в отдельности (кг)	—	16	16
Heat Dissipation(max)	—	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
Соответствие нормативам	—	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
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

→

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