Программное обеспечение

«F.A.C.C.T. Storage»

Описание функциональных характеристик

Содержание

1 ОБЩИЕ СВЕДЕНИЯ 3

1.1 Введение 3

1.2 Назначение ПО 3

1.3 Общие принципы функционирования ПО 4

2 Программно-аппаратные среды функционирования ПО 5

3 Реализация ПО 7

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит описание функциональных характеристик программного обеспечения «F.A.C.C.T. Storage» (далее – ПО, F.A.C.C.T. Storage).

1.2 Назначение ПО

F.A.C.C.T. Storage – комплексное решение предназначено для выявления современных высокотехнологичных атак на ранней стадии, обеспечения процесса threat hunting (охота на угрозы), оптимизации процессов реагирования на инциденты и их последующего расследования внутри корпоративной, так и технологической инфраструктуры. Оно определяет заражения, которые пропускают стандартные средства защиты: антивирусы, межсетевые экраны, системы предотвращения вторжений. Применение «F.A.C.C.T. Storage» существенно снижает риски организации, помогая вовремя выявить и предотвратить хищения, финансовые мошенничества, попытки шпионажа, утечку конфиденциальной информации и другие инциденты.

1.3 Общие принципы функционирования ПО

На Рисунке 1 изображены общие принципы функционирования ПО с остальными модулями MXDR.

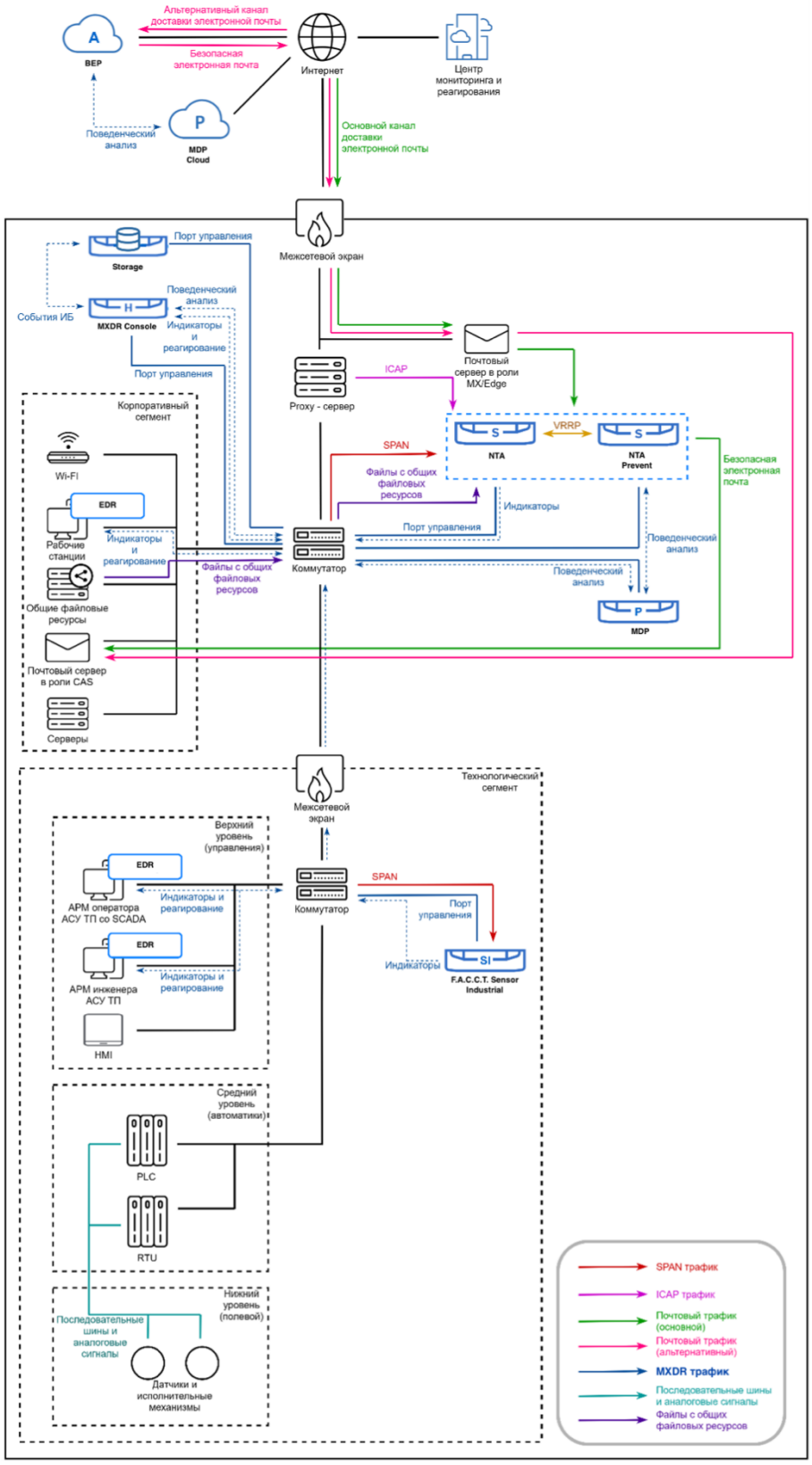

Рисунок 1. Общие принципы функционирования ПО

2 Программно-аппаратные среды функционирования ПО

ПО функционирует в следующих программно-аппаратных средах:

1. Аппаратные среды:
    a. Сервера со следующими техническими требованиями:

Таблица 1 – Технические требования для «F.A.C.C.T. Storage»

CPU	3.8 GHz, 6 C (2 threads per core), 12 MB
RAM, GB	64 GB, RDIMM
HDD, GB**	4 x 1,2Тбайт, 10000 об/мин, SAS 12 Гбит/с
Network	
Mgmt Ethernet	Ethernet

2. Виртуальные среды:
    a. Hyper-V;
    b. Vmware Esxi;
    c. Qemu;
    d. Xen-server.
3. Использование браузеров для доступа к системе:
    a. Windows Internet Explorer версии 8.0 и выше;
    b. Google Chrome версии 4.0 и выше;
    c. Mozilla Firefox версии 3.5 и выше;
    d. Apple Safari версии 4.0 и выше;
    e. Opera версии 10.5 и выше;
    f. iOS Safari версии 3.2 и выше;
    g. Opera Mobile версии 11.0 и выше;

h. Google Chrome for Android версии 11.0 и выше;

i. Mozilla Firefox for Android версии 26.0 и выше;

j. Windows Internet Explorer Mobile версии 10.0 и выше.

В браузере устройства пользователя должно быть включено исполнение скриптов JavaScript.

3 Реализация ПО

Архитектурно решение состоит из следующих модулей:

F.A.C.C.T. NTA

F.A.C.C.T. NTA предназначен для анализа входящих и исходящих пакетов данных. Он позволяет выявить взаимодействие зараженных устройств с командными центрами злоумышленников, общие сетевые аномалии и необычное поведение устройств. Для работы F.A.C.C.T. NTA использует собственные сигнатуры и поведенческие правила.

Особенности системы:

- Постоянно обновляемые базы – информация из кибербразведки и системы криминалистики;
- Единый интерфейс с тикет-системой;
- Интеграция с почтой/icap;
- Анализ трафика до 20 Gb/s;
- Возможность виртуальной установки/HW Appliance;
- Интеграция с SIEM и другими системами.

F.A.C.C.T. Sensor Industrial

F.A.C.C.T Sensor Industrial предназначен для анализа входящих и исходящих пакетов данных. Он позволяет выявить взаимодействие зараженных устройств с командными центрами злоумышленников, общие сетевые аномалии и необычное поведение устройств. Для работы F.A.C.C.T Sensor Industrial использует собственные сигнатуры и поведенческие правила.

Особенности системы:

- Постоянно обновляемые базы – информация из кибербразведки и системы криминалистики;
- Единый интерфейс с тикет-системой;
- Интеграция с почтой/icap;

- Анализ трафика до 20 Gb/s;
- Возможность виртуальной установки/HW Appliance;
- Интеграция с SIEM и другими системами.

F.A.C.C.T. MDP

Данная система предназначена для поведенческого анализа подозрительных объектов в безопасной среде. Полученные по электронной почте или скачанные из интернета файлы проверяются до попадания на компьютеры пользователей. Применение технологий машинного обучения позволяет выявить ранее неизвестные вредоносные программы без использования сигнатур, а также блокировать их доставку пользователям.

Особенности системы:

- Запатентованная технология обнаружения обхода песочницы;
- Эмуляция действий пользователей;
- Специально подготовленные образы для обнаружения 0-Day уязвимостей и различного вида ВПО (вредоносного программного обеспечения);
- Анализ файлов с измененными расширениями;
- Запатентованный низкоуровневый монитор, выявляющий все возможные действия в том числе и выполнение кода на уровне CPU;
- Дешифровка запароленных архивов с паролем в теле письма/вложенном файле/по словарю;
- Ретроспективный анализ.

F.A.C.C.T. XDR

Центр управления, мониторинга, хранения событий и обновлений, устанавливаемый внутри инфраструктуры заказчика. XDR интегрируется с другими компонентами комплекса MXDR (NTA, MDP, EDR) и значительно расширяет функционал решения за счет новых возможностей.

Особенности системы

- Оркестрация всех компонентов XDR и управлением ими из единого интерфейса;
- Анализ больших данных, выявление новых инструментов и инфраструктуры атакующих;
- Хранение логов и аналитической информации по инцидентам;
- Визуализация инцидента на ранней стадии атаки;
- Удаленное реагирование на конечных станциях;
- Внутренний Threat Hunting (охота на угрозы) по логам;
- Сбор криминалистических данных для расследования инцидентов.

F.A.C.C.T. Storage

Данная система предназначена для обеспечения гибкого масштабирования архитектуры системы для наращивания производительности в случае необходимости.