Программное обеспечение

«F.A.C.C.T. Business Email Protection»

Описание функциональных характеристик

Содержание

1 ОБЩИЕ СВЕДЕНИЯ

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

2 Назначение ПО

Business Email Protection – Программное обеспечение для поведенческого анализа, обеспечивающее выявление ранее неизвестного вредоносного кода с использованием передовых алгоритмов машинного обучения. Решение позволяет эффективно выявлять ранее неизвестные угрозы, осуществляя анализ файлов в изолированной среде. Он позволяет предотвратить заражения в результате фишинговых рассылок, либо загрузки/получения вредоносных файлов, осуществляющих заражения с использованием ранее неизвестных вредоносных программ и инструментов.

Использование модуля Business Email Protection обеспечивает обнаружение ранее неизвестного вредоносного ПО и сложных целевых атак.

Основными целями создания Системы являются:

- Предоставление интерфейса с отображением результатов проведения поведенческого анализа объектов;
- Повышение качества и количества раскрываемых преступлений;
- Предоставление прозрачной статистической и аналитической информации.

3 Программно-аппаратные среды функционирования ПО

- ПО функционирует в следующих программно-аппаратных средах:
- Windows Internet Explorer версии 8.0 и выше;
- Google Chrome версии 4.0 и выше;
- Mozilla Firefox версии 3.5 и выше;
- Apple Safari версии 4.0 и выше;
- Opera версии 10.5 и выше;
- iOS Safari версии 3.2 и выше;
- Opera Mobile версии 11.0 и выше;
- Google Chrome for Android версии 11.0 и выше;
- Mozilla Firefox for Android версии 26.0 и выше;
- Windows Internet Explorer Mobile версии 10.0 и выше.

4 Общие принципы функционирования ПО

Внутри Системы используется набор виртуальных машин с различными операционными системами. Анализируемый объект в автоматизированном режиме запускается на виртуальной машине. После запуска происходит запись следов работы внутри операционной системы в результате запуска объекта, исходя из показателей компрометации. Показатели компрометации могут обновляться в соответствии с понимаем современного ландшафта киберпреступлений. По итогам анализа доступен подробный отчет со следующими информационными блоками:

- Развернутая информация о файле;
- Поведенческие маркеры;
- Сведения о сетевая активности;
- Дерево процессов;
- Видео.

На рисунке изображены общие принципы функционирования ПО Business Email Protection с остальными модулями MXDR.

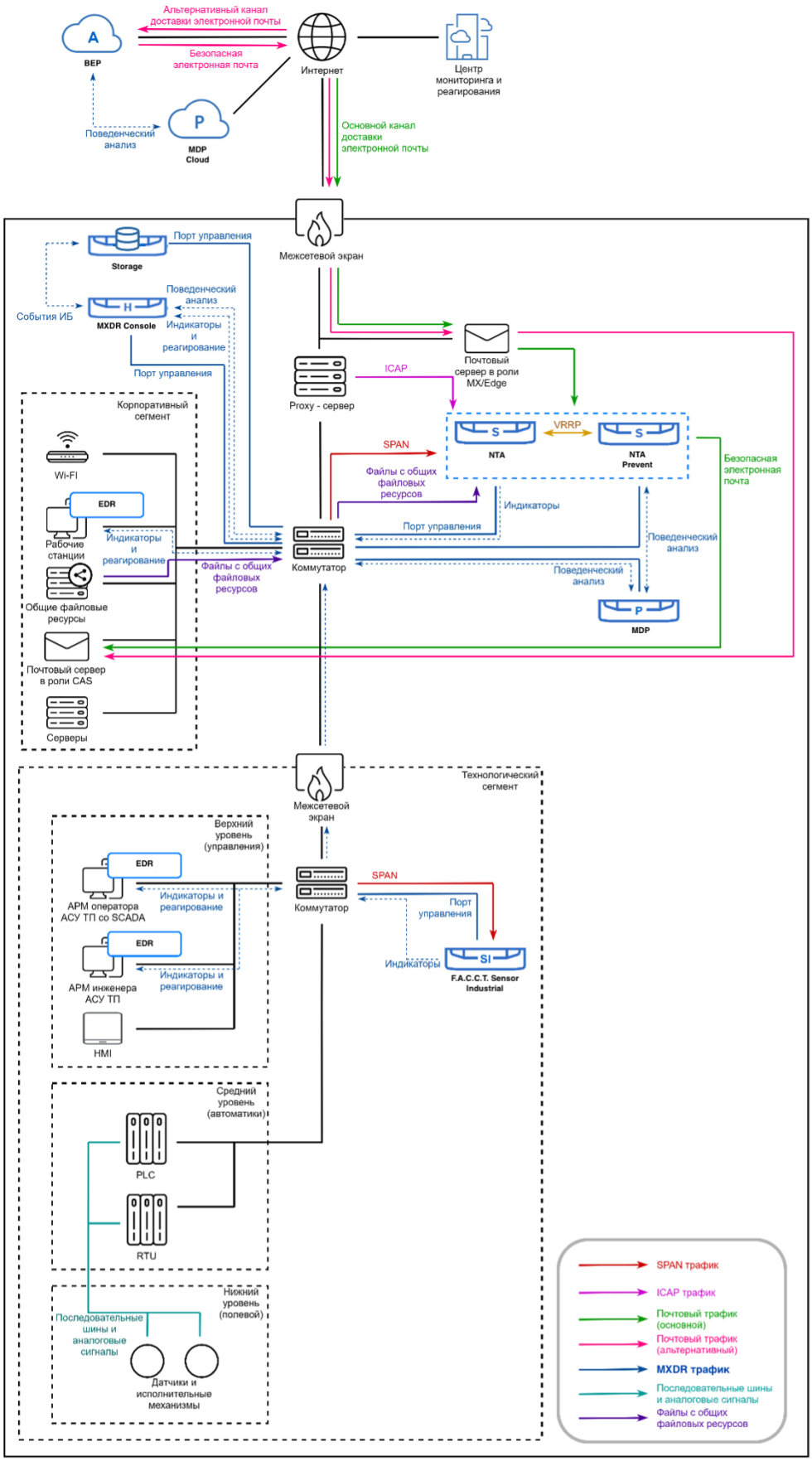
Альтернативный канал доставки электронной почты
Безопасная электронная почта
ВЕР
Интернет
Центр мониторинга и реагирования
Поведенческий анализ
MDP Cloud
Основной канал доставки электронной почты
Межсетевой экран
Порт управления
Storage
Поведенческий анализ
События ИБ
MXDR Console
Индикаторы и реагирование
Порт управления
Почтовый сервер в роли MX/Edge
ICAP
Proxy - сервер
Корпоративный сегмент
SPAN
VRRP
NTA
NTA Prevent
Безопасная электронная почта
Wi-FI
EDR
Файлы с общих файловых ресурсов
Индикаторы
Порт управления
Рабочие станции
Индикаторы и реагирование
Файлы с общих файловых ресурсов
Коммутатор
Поведенческий анализ
Поведенческий анализ
Общие файловые ресурсы
MDP
Почтовый сервер в роли CAS
Серверы
Технологический сегмент
Межсетевой экран
Верхний уровень (управления)
EDR
Коммутатор
SPAN
АРМ оператора АСУ ТП со SCADA
Индикаторы и реагирование
Порт управления
EDR
Индикаторы
SI
F.A.C.C.T. Sensor Industrial
АРМ инженера АСУ ТП
Индикаторы и реагирование
HMI
Средний уровень (автоматики)
PLC
RTU
Нижний уровень (полевой)
Последовательные шины и аналоговые сигналы
Датчики и исполнительные механизмы
SPAN трафик
ICAP трафик
Почтовый трафик (основной)
Почтовый трафик (альтернативный)
MXDR трафик
Последовательные шины и аналоговые сигналы
Файлы с общих файловых ресурсов

Таблица 1 – Технические требования для «F.A.C.C.T. Business Email Protection»

BEP	Standard	Enterprise
CPU	2.1 GHz, 20 C (2 threads per core), 27.5 MB	2.1 GHz, 40 C (2 threads per core), 27.5 MB
RAM, GB	128 GB, RDIMM	256 GB, RDIMM
SSD, GB**	2 x 480	2 x 480
Mgmt Ethernet	1 Ethernet	1 Ethernet

5 Реализация ПО

Системы состоит из следующих модулей:

- Модуль предоставления возможности загрузки ПО в Систему;
- Модуль предоставления результатов анализа;
- Модуль защиты удаленного доступа и контроля изменений.

В рамках предоставляемого интерфейса операторы системы имеют возможность загружать ПО и файлы в Систему и получать данные по результатам анализа.

5.1 Модуль предоставления возможности загрузки ПО в Систему

В разделе «Управление -> Анализ файлов» представлена возможность загрузить ПО и/или набор файлов для проведения поведенческого анализа.

5.2 Модуль предоставления результатов анализа

В разделе «Управление -> Анализ файлов» предоставляется список работ по анализу ПО и/или файлов. Каждая строка отражает задачу анализа. По задаче анализа предоставляется детализированная информация:

- Развернутая информация о файле;
- Поведенческие маркеры;
- Сведения о сетевая активности;
- Дерево процессов;
- Видео.

5.3 Модуль защиты удаленного доступа и контроля изменений

Модуль защита удалённого доступа обеспечивает:

- сохранение конфиденциальности и целостности передаваемой информации;
- возможность ограничения доступа к системе для всех адресов кроме указанного в настройках;

неотключаемый протокол внесения изменений в Систему и выгрузки данных из системы:

- загрузка новых данных;
- изменение параметров пользователей Системы;
- выгрузка данных в отдельный файл со скачиванием через клиентский браузер;
- создание новых пользователей Системы;
- выдача пользователю дополнительных прав.