# Программное обеспечение

# «F.A.C.C.T. Sensor Industrial»

Описание функциональных характеристик

# Содержание

# 1 ОБЩИЕ СВЕДЕНИЯ

## 1.1 Введение

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

## 1.2 Назначение ПО

F.A.C.C.T. Sensor Industrial — сенсор анализа данных, подключаемый к копии сетевого трафика защищаемой организации. Работает в технологических и корпоративных сетях. Является так же модулем почтовой интеграции для проведения анализа почтовых сообщений совместно с F.A.C.C.T. XDR.

Использование модуля F.A.C.C.T. Sensor Industrial обеспечивает обнаружение ранее неизвестного вредоносного ПО и сложных целевых атак.

Основными целями создания ПО являются:

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

# 2 Технические требования

## 2.1 Минимальные технические требования

Ниже приведены минимальные технические требования для Sensor Industrial.

| **Sensor Industrial (нагрузка Mbps)** | **500** | **1000** | **2000** |
|---|---|---|---|
| **CPU** | 4 GHz, 6 C, (2 threads per core), 12 MB | 4 GHz, 6 C, (2 threads per core), 12 MB | 2.1 GHz, 20 C, (2 threads per core), 27.5 MB |
| **RAM, GB** | 32 GB, DDR 4 | 32 GB, DDR 4 | 64 GB, RDIMM |
| **HDD, GB** | 2 x 1200 | 2 x 1200 | 2 x 1200 |
| **Network** | | | |
| **mgmt Ethernet** | 1 | 1 | 1 |
| **Span** | до 4 Ethernet | до 4 Ethernet or SFP | до 4 SFP/SFP+ |

## 2.2 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.

# 3 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 1 изображены общие принципы функционирования ПО F.A.C.C.T. Sensor Industrial с остальными модулями MXDR.

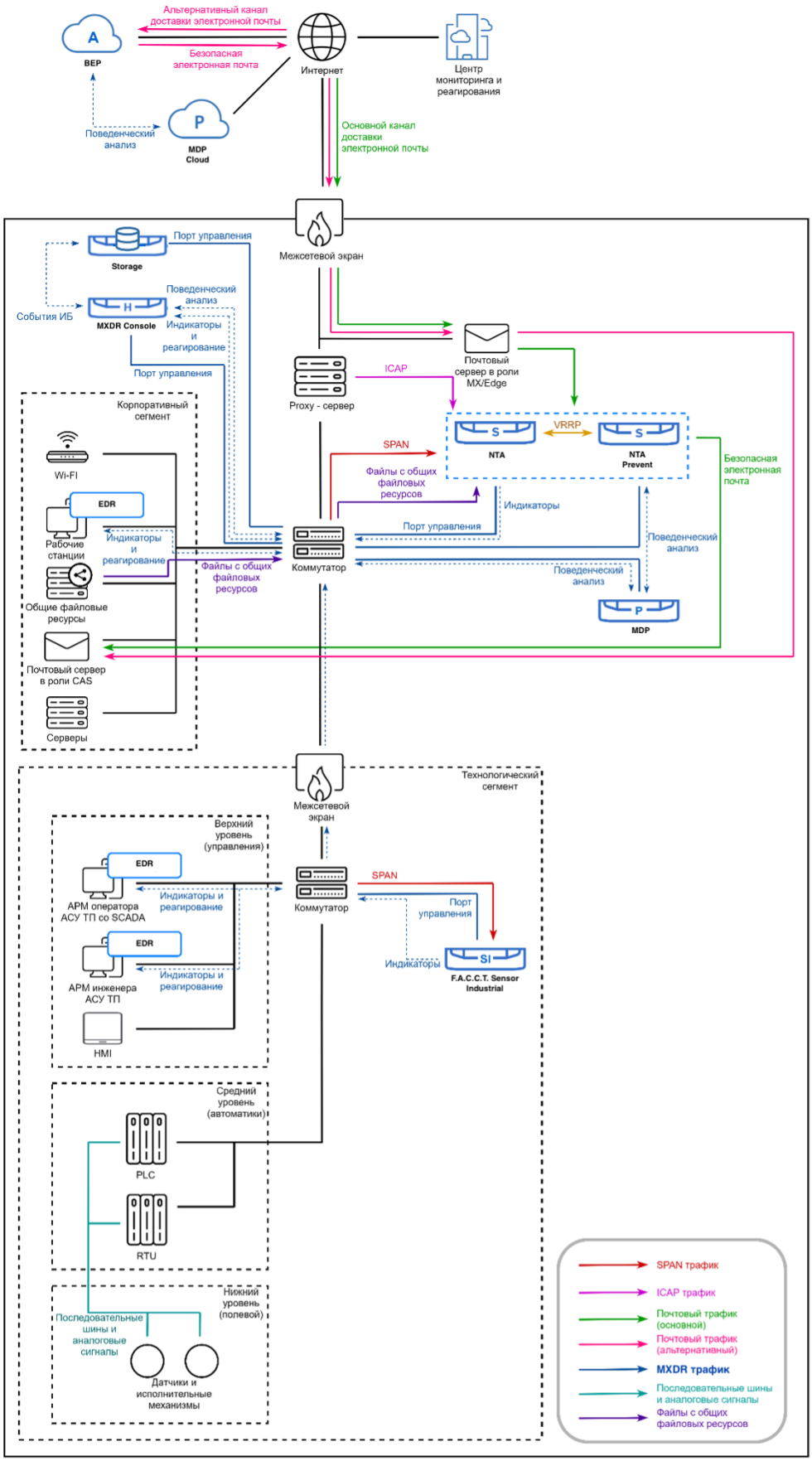


Рисунок 1. Общие принципы функционирования ПО

XDR - система анализа, корреляции, принятия решений и управления всеми компонентами комплекса.

NTA - сенсор анализа данных, подключаемый к копии сетевого трафика защищаемой организации. Является так же модулем почтовой интеграции для проведения анализа почтовых сообщений совместно с MDP

MDP (песочница) - модуль поведенческого анализа файлов, получаемых из почты, целевых хостов (с помощью EDR), файловых хранилищ, ICAP клиентов. Позволяет детектировать неизвестные ранее угрозы и продвинутые целевые атаки.

EDR – программное обеспечение для сбора данных о поведении пользователя и программ, обеспечивающее фиксацию полной хронологии событий на системе, блокировку аномального поведения, изоляцию хоста, отправку данных в удаленное хранилище для последующего анализа.

ПО — это комплексное решение, направленное на повышение качества обнаружения новых и неизвестных угроз, атак без использования вредоносных программ, обеспечение процесса threat hunting, оптимизацию процессов реагирования на инциденты и их последующего расследования именно внутри корпоративной инфраструктуры.

# 4 Реализация ПО

ПО 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 ПО имеют возможность загружать ПО и файлы в систему и получать данные по результатам анализа.

## 4.1 Модуль предоставления возможности загрузки ПО в систему

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

## 4.2 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.

## 4.3 Модуль защиты удаленного доступа и контроля изменений

Модуль защиты 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 ПО:
    - загрузка новых данных;
    - изменение параметров пользователей ПО;

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