Программное обеспечение

«F.A.C.C.T. Network Traffic Analysis»

Описание функциональных характеристик

Содержание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящее описание функциональных характеристик содержит описание реализации программного обеспечения «F.A.C.C.T. Network Traffic Analysis» (далее – ПО, F.A.C.C.T. Network Traffic Analysis, NTA).

1.2 Назначение ПО

ПО - комплексное решение предназначено для выявления современных высокотехнологичных атак на ранней стадии, обеспечение процесса threat hunting, оптимизацию процессов реагирования на инциденты и их последующего расследования внутри корпоративной инфраструктуры. Оно определяет заражения, которые пропускают стандартные средства защиты: антивирусы, межсетевые экраны, системы предотвращения вторжений. Применение XDR существенно снижает риски организации, помогая вовремя выявить и предотвратить хищения, финансовые мошенничества, попытки шпионажа, утечку конфиденциальной информации и другие инциденты.

1.3 Минимальные технические требования для физического сервера

Ниже приведены минимальные технические требования к физическому серверу в зависимости от типа Network Traffic Analysis - 1000, 5000 или 10K.

При наличии нескольких процессоров модуль NTA на физическом сервере не будет поддерживать анализ SPAN-трафика.

Параметр	**250**	**1000**	**5000**	**20 000**
Процессор	3,9 GHz, 4 C, 8 MB	3,9 GHz, 4 C, 8 MB	2.4 GHz, 14 C, 35 MB	2.4 GHz, 14 C, 35 MB
Объем оперативной памяти	32 GB	32 GB	64 GB	128 GB
Объем хранилища	2 x 480	2 x 1200	2 x 1200	2 x 1200
Сетевые интерфейсы				
Интерфейс управления	1 Ethernet	1 Ethernet	1 Ethernet	1 Ethernet

Параметр	250	1000	5000	20 000
Интерфейс анализатора сетевого трафика (NTA)	1 port, Intel Ethernet	1 port, Intel Ethernet	1 port, Intel Ethernet	1 port, Intel Ethernet

1.4 Минимальные технические требования для XDR

Параметр	Enterprise	Performance	Storage
Процессор	2.4 GHz, 14 C, 35 MB	2.4 GHz, 28 C, 35 MB	2.4 GHz, 14 C, 35 MB
Объем хранилища	4 x 1200	4 x 1200	2 x 1200 HDD +2 x 960 SSD
Объем оперативной памяти	96	128	64
Интерфейс анализатора сетевого трафика (NTA)	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter

1.5 Минимальные технические требования для EDR

Параметр	Windows 7	Windows 8/8.1	Windows 10
Процессор	Не ниже Intel core i3 второго поколения	Не ниже Intel core i3 второго поколения	Не ниже Intel core i3 второго поколения
Объем хранилища	100	100	100
Объем оперативной памяти	4	4	4
Network	Связь с XDR	Связь с XDR	Связь с XDR

1.6 Программные и виртуальные среды

1. Виртуальные среды:

a. Hyper-V

b. Vmware Esxi

c. Qemu

d. Xen-server

2. 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

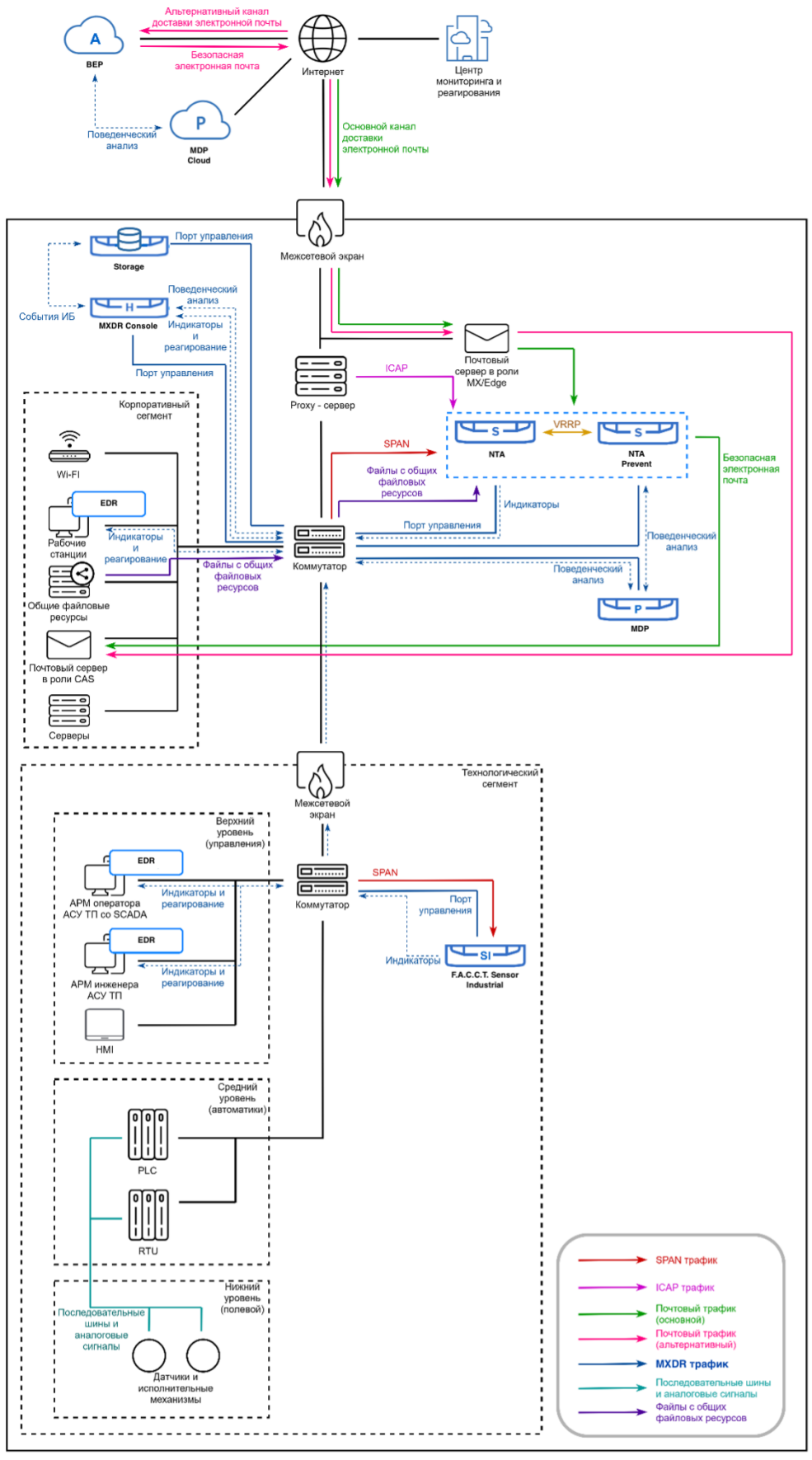
h. Google Chrome for Android версии 11.0 и выше

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.

2 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.

3 Реализация ПО

Архитектурно решение состоит из следующих модулей:

1. **NTA**

Сенсор 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 сенсор использует собственные сигнатуры и поведенческие правила.

Особенности системы:

- Постоянно обновляемые базы – информация из киберразведки 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

2. 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.

3. Центр управления, мониторинга, хранения событий и обновления

Специалисты Центра управления мониторинга АО «БУДУЩЕЕ» (SOC) отслеживают и анализируют события, выявленные NTA и MDP. Эксперты SOC немедленно уведомляют специалистов организации о критичных угрозах по электронной почте и телефону, а также дают рекомендации по их устранению. Поддержка работает круглосуточно, 365 дней в году. Центр Управления также может быть развернут внутри сети заказчика в виде MXDR.

4. 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 MXDR 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 по логам

- Сбор криминалистических данных для расследования инцидентов

Гибкая схема установки

- On-Premise / Cloud / Hybrid
- Различные способы взаимодействия с инфраструктурой АО «БУДУЩЕЕ» (см. руководство администратора «Обновления и потоки данных»)

4 Интеграция с сетевым трафиком

Система обеспечивает анализ трафика, подаваемого на оборудование NTA из разных источников:

- SPAN/RSPAN трафик
- SPAN/RSPAN трафик в GRE-туннеле
- ICAP (файлы из трафика)

При интеграции по ICAP возможно настроить режим блокировки - вредоносные вложения не будут доступны для загрузки пользователям.

5 Интеграция с почтовой системой

Поддерживаются несколько различных способов получения писем для поведенческого анализа:

- Получение писем по SMTP
- Получение писем с помощью механизма скрытой копии (BCC) через POP3/IMAP

Поддерживается возможность блокировки вредоносных писем посредством интеграции NTA в режиме MTA (Mail Transfer Agent). Внутренний MTA режим обеспечивает возможность настройки почтовой инфраструктуры любой сложности - с любым количеством почтовых серверов и настройкой различных правил пересылки. При этом обеспечивается отказоустойчивость и балансировка нагрузки.

6 Типовые схемы подключения

6.1 Режим анализа копии трафика и файлов из трафика

В этом режиме MDP осуществляет пассивный мониторинг файлов из трафика. Объекты анализа поступают от NTA и отправляются в облако MDP Cloud.

6.2 Режим анализа копии трафика и файлов из трафика в GRE туннеле

NTA поддерживает возможность организовывать GRE-туннели. Когда нет возможности напрямую подать SPAN/RSPAN, поскольку между сенсором и зеркалирующим оборудованием находится L3 оборудование, либо необходимо получить трафик с фермы виртуальных машин, можно использовать GRE-инкапсуляцию, для передачи SPAN трафика в MXDR.

6.3 Режим анализа почты

Поддерживаются несколько различных способов получения писем для поведенческого анализа:

- Получение писем по SMTP.
- Получение писем с помощью механизма скрытой копии (BCC)

Получение писем по SMTP

При данной интеграции NTA выступает как MTA (или SMTP Relay), получаю копию всей входящей почты через SMTP. Единственное отличие этого режима, от режима с блокировкой, что письма тут не пересылаются дальше, а просто анализируются.

Получение писем с помощью механизма скрытой копии (BCC)

При данной интеграции создаётся дополнительный почтовый ящик, куда осуществляется копирование всей входящей почты. NTA подключается к подготовленному ящику и забирает письма для анализа.

Получение писем по SMTP с блокировкой (inline-режим)

Основной режим интеграции с почтой, когда почта проходит через NTA как через SMTP Relay, и доставляется дальше после анализа. Соответственно вредоносные письма блокируются. Отказоустойчивость обеспечивается либо на уровне DNS, либо на уровне

SMTP-сервера, где настраивается несколько релеев, либо на уровне VRRP, когда несколько устройств делят виртуальный IP адрес.