ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Business Email Protection»

Описание функциональных характеристик

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Определение
Алерт	Предупреждение об опасности. «Немедленное» оповещение о том, что информационная система и сеть подвергаются атаке или находятся в опасности вследствие аварии, сбоя или человеческой ошибки.
АС	Автоматизированная Система
Заказчик	зарегистрированный пользователь в системе заказчика передавший третьим лицам все необходимы данные и реквизиты для управления приложением или выполняющий указания третьих лиц за вознаграждение
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО БУДУЩЕЕ; • Компанией-интегратором, по выбору Заказчика
ОС	Операционная система
ПО	Программное обеспечение «F6 Business Email Protection»
ТС	(«Технический Сервис») Система взаимодействия Заказчика, позволяющая обмениваться сообщениями и создавать цепочки обращений, которая представляет из себя отдельный раздел «Службу Поддержки» в панели управления «F6 Business Email Protection». В случае недоступности указанных систем формат взаимодействия осуществляется через электронный почтовый ящик.
HTTP	HyperText Transfer Protocol
IPv4	Internet Protocol version 4
JSON	JavaScript Object Notation
MDP	Модуль F6 MDP (Malware detonation platform)
MXDR	Программный комплекс Managed Extended Detection and Response (Managed XDR)

NTA	Модуль F6 Network Traffic Analysis
XDR	Модуль F6 XDR (MXDR Console)
pytest	Фреймворк для тестирования кода на Python
selenium	Инструмент для автоматизации действий веб-браузера
SOC	Security Operation Center
TI	ПО F6 Threat Intelligence
TTP	Tactics, Technics, Procedures (Тактики, Техники, Процедуры). Набор тактик, техник и процедур, используемых злоумышленниками • тактика — как злоумышленник действует на разных этапах своей операции, какая цель или задача злоумышленника на определенным шаге; • техника — как злоумышленник достигает цели или поставленной задачи, какие использует инструменты, технологии, код, эксплоиты, утилиты и так далее; процедура — как эта техника выполняется и для чего.

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящее описание функциональных характеристик содержит описание реализации программного обеспечения «F6 Business Email Protection» (далее – ПО, BEP).

1.2 Назначение ПО

«F6 Business Email Protection» - это модуль системы MXDR (Managed XDR) который специализируется на анализе и мониторинге электронной почты для выявления киберугроз. Этот модуль сканирует входящие письма для обнаружения фишинга, спама и других видов угроз, направленных на компрометацию пользователей. ПО фокусируется на проверке содержимого писем и выявлении потенциальных угроз. В качестве платформы детонации используется модуль Malware Detonation Platform (MDP). В случае обнаружения угроз модуль формирует отчеты и отправляет уведомления, обеспечивая оперативное реагирование специалистов по кибербезопасности.

1.3 Функциональные возможности ПО

ПО обладает следующими функциональными возможностями:

– Поддержка развертывания в трех вариантах:

- Cloud релей – перенаправление входящего почтового потока через измененные MX-записи в инфраструктуру разработчика для анализа и принятия решений о блокировке.
- Cloud почтовый шлюз – анализ почтового потока в инфраструктуре разработчика при использовании существующего почтового сервера заказчика.
- On-prem шлюз – анализ почтового потока с существующего почтового сервера через подсистему интеграции и анализ контента в инфраструктуре заказчика.

– Возможность настройки маршрутов для почты с указанием приоритетности и веса серверов для балансировки нагрузки и распределения почтового потока.

– Отправка почтовых сообщений по заданным маршрутам после анализа, если сообщение признано безопасным, с применением всех заданных политик фильтрации.

– Возможность создания белых списков для исключения индикаторов из анализа по следующим параметрам: email-адреса, URLs, хеш-суммы, IP-адреса.

– Поведенческий анализ файлов в специально подготовленных виртуальных машинах.

– Статический и эвристический анализ контента писем, заголовков и ссылок на предмет социальной инженерии, включая BEC-атаки и спам, с отчетом о сработавших правилах.

– Возможность применения настраиваемых политик фильтрации для снижения рисков получения нежелательных рассылок и/или вредоносного контента.

– Настройка политик проверки форматов содержимого по критериям: file_name, file_magic, url, recipient, sender, spf, dkim, dmarc.

– Настройка политик действий с непроверенным контентом, включая зашифрованные архивы и недоступные ссылки.

– Возможность добавления пользовательских YARA-правил и настройки политики действий на основе их срабатывания.

– Возможность принудительной отправки заблокированных почтовых сообщений как получателю, указанному в заголовках письма, так и на заданный администратором адрес.

– Представление технических заголовков и структуры почтового сообщения в виде графа.

– Использование низкоуровневого монитора для выявления поведенческих маркеров.

– Применение элементов машинного обучения для улучшения обнаружения угроз.

– Анализ файлов в изолированной среде с использованием русифицированного образа ОС Windows.

– Поддержка анализа файлов до 100 Мб.

– Поведенческий анализ файлов различных расширений и типов в изолированной среде.

– Анализ потенциально вредоносных файлов с возможностью определения различных типов файлов по содержимому.

– Интерфейс для загрузки файлов на анализ в ручном режиме с возможностью задания параметров виртуализации и анализа.

– Подключение к виртуальной машине во время анализа файла по протоколу RDP.

– Поведенческий анализ архивов с паролем и поиск паролей из различных источников.

– Использование гипервизора для анализа, контроль событий ОС, статический сигнатурный анализ и автоматическое обнаружение техник обхода анализа.

– Формирование отчета по результатам анализа с детализированными данными о процессах, сетевой активности, файловых взаимодействиях и сработавших правилах.

– Обнаружение и извлечение конфигурационных файлов ВПО, атрибуция к известным инструментам и возможность экспорта файлов для дальнейшего анализа.

– Гибкое горизонтальное масштабирование для наращивания производительности при необходимости.

– Возможность изменения маршрута для вывода трафика из виртуальных машин.

– Кастомизация виртуальных машин, включая изменение домена, имени компьютера и имени пользователя.

– Автоматический подбор конфигурации виртуальной машины, эмуляция пользовательской активности, технологии компьютерного зрения, извлечение и запуск дополнительных команд из реестра, опция поддельного SMTP-сервера и использование Mitmproxy.

1.4 Требования к ПО

ПО может быть установлено либо на физический сервер, либо на виртуальную машину.

1.5 Минимальные технические требования для физического сервера

Ниже приведены минимальные технические требования к серверу в зависимости от типа ПО. Основным параметром выбора минимального оборудования является сервер NTA Prevent, в связке с которым работает BEP в независимости от типа поставляемой лицензии (BEP Standard, BEP Pro, BEP Enterprise)

Параметр	1000	5000	10 000
Процессор(ы)	Intel Xeon Gold 5315Y 3.2GHz, 8C/16T, 11.2 GT/s, 12MB Cache, Turbo 3.6GHz, HT (140W) DDR4-2933	Intel Xeon Gold 6336Y 2.4GHz, 24C/48T, 11.2GT/s, 36M CacheTurbo 3,6GHz HT (185W) DDR4-3200	Intel Xeon Gold 6348 2.6GHz, 28C/56T, 11.2GT/s, 42 M Cache Turbo 3,5GHz, HT (235W) DDR4-3200
Объем хранилища	2 x 480GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS SSD RAID1	2 x 960 GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS RAID1	2 x 960GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS RAID1
Интерфейс управления	1 Ethernet	1 Ethernet	1 Ethernet
Объем оперативной памяти	64 GB	64 GB	128 GB
Интерфейс анализатора сетевого трафика (NTA)	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter

1.6 Минимальные технические требования для виртуальной машины

Ниже приведены минимальные технические требования к конфигурации оборудования виртуальной машины.

Параметр	1000	5000	10 000
Виртуальный процессор	16	40	56
Объем хранилища	480 GB SSD, Random write 44500 IOPS	960 GB SSD, Random write 44500 IOPS	960 GB SSD, Random write 44500 IOPS
Объем оперативной памяти	64 GB	64 GB	128 GB
Интерфейс анализатора сетевого трафика (NTA)	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter

2 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО

На Рисунок 1 изображены общие принципы функционирования ПО.

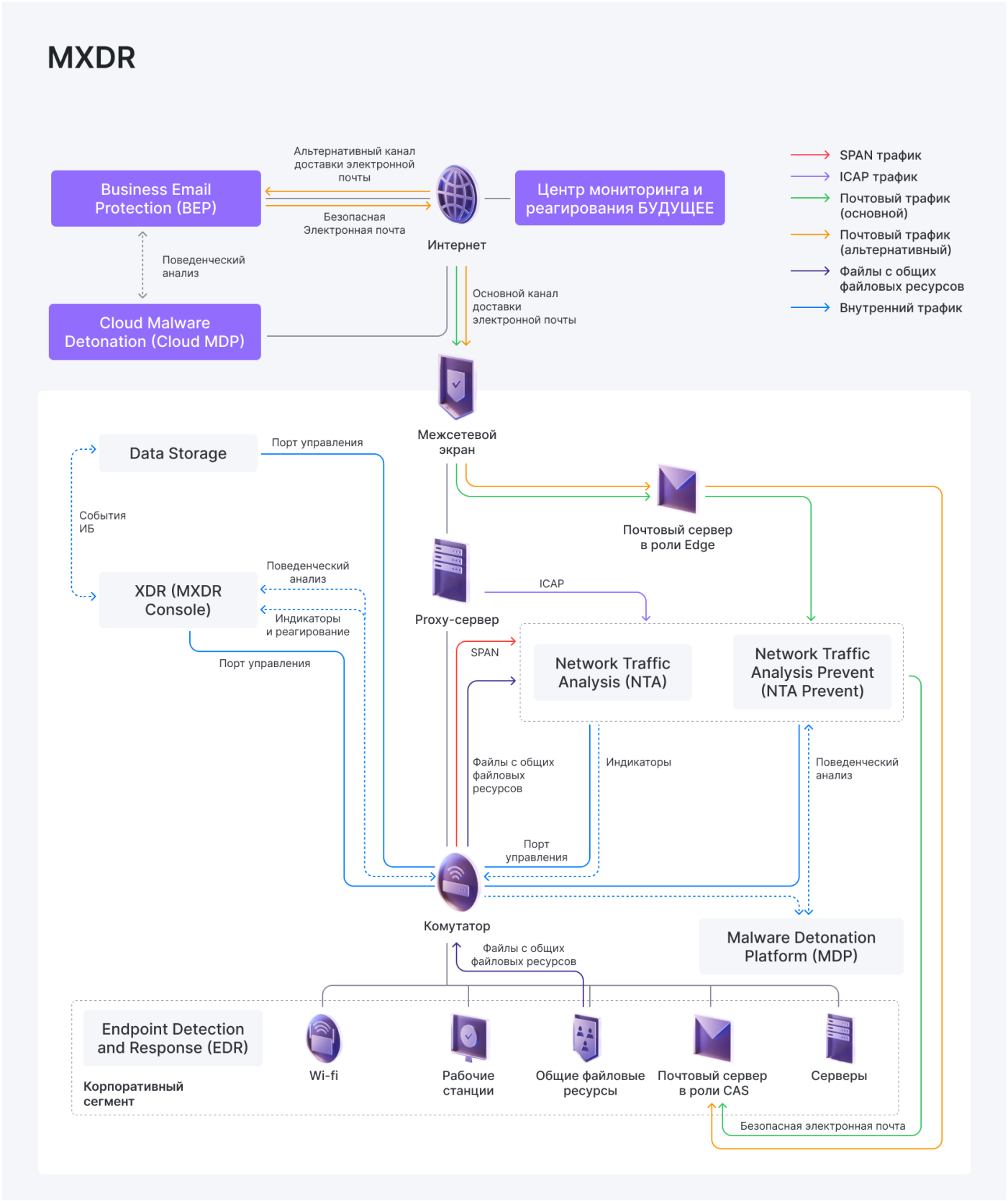

Рисунок 1. Общие принципы функционирования MXDR

XDR (MXDR Console) – набор инструментов, необходимых для команд мониторинга, реагирования на инциденты и проведения компьютерных расследований в защищаемой инфраструктуре. Является системой управления всеми модулями решения.

Network Traffic Analysis (NTA) – модуль системы MXDR, предназначенный для анализа входящих и исходящих пакетов данных. Используя собственные сигнатуры и поведенческие правила NTA позволяет выявлять взаимодействие зараженных устройств с командными центрами злоумышленников, общие сетевые аномалии и необычное поведение устройств.

Malware Detonation Platform (MDP) – модуль поведенческого анализа файлов, извлекаемых из электронных писем, сетевого трафика, файловых хранилищ, персональных компьютеров и автоматизированных систем, посредством интеграции через API, или загружаемых вручную. *MDP* дополняет функциональность системы MXDR, расширяя возможности по обнаружению вредоносных файлов, нацеленных на защищаемую инфраструктуру.

Endpoint Detection and Response (EDR) – программное обеспечение для обнаружения угроз на хосте, фиксации полной хронологии событий на системе, блокировки аномального поведения, изоляции хоста, сбора криминалистически значимых данных.

Data Storage – модуль, предназначенный для хранения данных. Позволяет оптимизировать распределение хранящихся данных из имеющегося набора.

2.1 Описание взаимодействия компонентов системы

Первичные данные, такие как электронные письма, файлы из внешней сети поступают проходят через модуль защиты корпоративной почты **Business Email Protection (BEP)** и облачную платформу **Cloud/on-prem Malware Detonation (Cloud MDP)**. Интернет-трафик отслеживается через сенсор ***Network Traffic Analysis (NTA)***. Эти системы обеспечивают первичную фильтрацию и анализ угроз, после чего данные направляются во внутреннюю инфраструктуру через защищённые межсетевые экраны.

После прохождения через межсетевые экраны данные поступают в модуль **XDR (MXDR Console)**, который является «связующим звеном» всей системы MXDR, расширяющий список возможностей каждого модуля системы. XDR собирает информацию из различных источников, включая сетевые устройства, системы защиты конечных точек и журналы событий, и объединяет их в едином интерфейсе для анализа и обработки. XDR поддерживает продвинутый поиск угроз (threat hunting) и позволяет выявлять сложные и скрытые атаки, которые могли бы быть пропущены другими

системами. В случае обнаружения угрозы XDR автоматически инициирует процессы реагирования, сокращая время отклика и снижая нагрузку на команды SOC.

Коммутационные устройства и протоколы, такие как **ICAP** и **SMTP**, обеспечивают правильное направление трафика и передачу данных между различными компонентами системы.

2.2 Описание схемы BEP

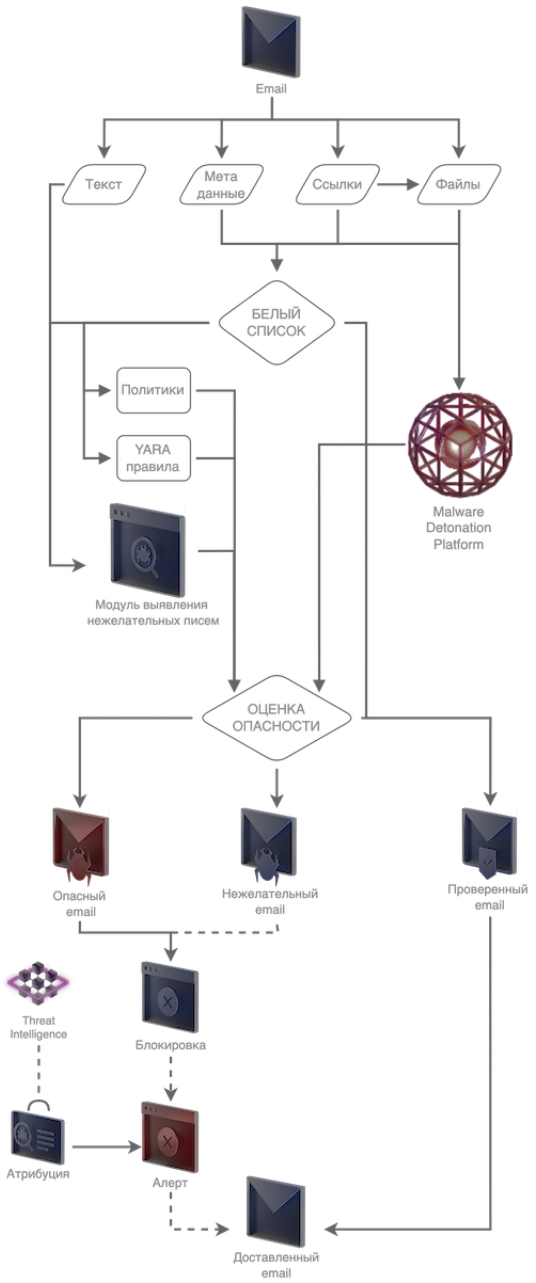

Рисунок 2. Общие принципы функционирования BEP

1. **Входящее письмо:** Письмо поступает в систему и проходит начальный этап обработки.
2. **Анализ компонентов письма**:

- **Текст**: анализируется содержимое текста письма.

- **Метаданные**: проводится анализ заголовков и других метаданных письма.
- **Ссылки**: проверяются ссылки, содержащиеся в письме.
- **Файлы**: анализируются прикрепленные файлы.

3. **Белый список:** на этом этапе проверяется, не входит ли письмо, ссылки или файлы в белый список. Если элементы письма находятся в белом списке, они исключаются из дальнейшего анализа.
4. **Политики и YARA правила:**

- **Политики:** применяются настройки, определяющие правила обработки и фильтрации письма.
- **YARA правила:** используются YARA правила для поиска признаков угроз в содержимом письма.

5. **Модуль выявления нежелательных писем:** письмо анализируется на предмет спама и других нежелательных сообщений.
6. **Malware Detection Platform (Платформа обнаружения вредоносного ПО):** Система анализирует письмо на наличие вредоносного ПО.
7. **Оценка опасности:** на основании результатов всех предыдущих этапов проводится итоговая оценка безопасности письма.
8. **Решение по письму:**

- **Опасный email: письмо классифицируется как опасное и блокируется.**
- **Нежелательный email: письмо классифицируется как нежелательное.**
  - **Threat Intelligence**: если письмо связано с конкретной угрозой, его отправляют на дальнейший анализ.
  - **Блокировка**: если письмо подтверждается как угроза, оно блокируется.
  - **Алерт в системе XDR**: при выявлении угрозы генерируется оповещение (алерт) в системе MXDR для дальнейшего реагирования.
- **Прозрачный email:** Письмо признано безопасным и доставляется получателю.

3 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными ПО являются:

Входящий почтовый трафик, данные от модулей системы и управляющие команды пользователей.

Выходными данными ПО является:

Проанализированная информация входящего трафика.