ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Endpoint Detection and Response »

Описание функциональных характеристик

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	**Определение**
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 Endpoint Detection and Response.
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 Endpoint Detection and Response». В случае недоступности указанных систем формат взаимодействия осуществляется через электронный почтовый ящик.
APT	Advanced Persistent Threat, постоянная угроза повышенной сложности
DLP	Data Leak Prevention, Предотвращение утечек
IP	Internet Protocol
MAC	Media Access Control
MDP	F6 Malware Detonation Platform
MFT	Master File Table
MXDR	Программный комплекс Managed Extended Detection and Response (Managed XDR)

MXDR Console	F6 XDR, MXDR
NTFS	New Technology File System
pytest	Фреймворк для тестирования кода на Python.
RPM	RPM Package Manager
selenium	Инструмент для автоматизации действий веб-браузера.
SIEM	Security Information and Event Management
UEFI	Extensible Firmware Interface
USB	Universal Serial Bus

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящее описание функциональных характеристик содержит описание реализации программного обеспечения «F6 Endpoint Detection and Response» (далее – ПО, Endpoint Detection and Response, EDR).

1.2 Назначение ПО

«F6 Endpoint Detection and Response» — это модуль системы MXDR (Managed XDR) который специализируется на обнаружении, расследовании и реагировании на угрозы, направленные на конечные точки, такие как рабочие станции. ПО обеспечивает защиту от различных киберугроз, включая вредоносное ПО, программы-вымогатели и сложные атаки, такие как APT (Advanced Persistent Threat). При обнаружении угрозы ПО предлагает инструменты для быстрого реагирования на инциденты, что включает изоляцию, расследование и устранение угрозы. Решение также обладает мощными функциями форензики и анализа инцидентов, что помогает понять коренные причины атаки и предотвратить повторные инциденты. ПО поддерживает автоматизацию процессов защиты и позволяет настраивать политики безопасности в соответствии с потребностями организации, а также интегрируется с SIEM и другими системами для комплексного управления инцидентами. ПО доступно в виде клиента для операционных систем Windows, Linux и macOS.

1.3 Функциональные возможности ПО

1.3.1 Функциональные возможности ПО применительно к конечным станциям на базе ОС семейства Microsoft Windows

ПО обладает следующими функциональными возможностями:

– ПО обеспечивает совместимость с установленными антивирусами и DLP-системами заказчика.

– ПО не оказывает негативного влияния на производительность рабочей станции при соблюдении системных требований.

– ПО собирает следующие типы событий:

- События, связанные с процессами: создание и завершение процессов, создание потоков, подгрузка динамических библиотек.

- События, связанные с файлами: создание, открытие, удаление, изменение содержимого, имени и атрибутов файлов, создание ссылок, изменение теневых копий.
- События, связанные с сетью: открытие сетевых соединений, привязка портов к процессам, DNS-запросы, создание общих папок.
- События, связанные с системой: подключение периферийных устройств, создание объектов в диспетчере объектов Windows, выключение станции, создание сервисов и отложенных задач, изменения в настройках локального сетевого экрана.
- События, связанные с реестром: создание, открытие, удаление, переименование ключей и изменение их значений.

– ПО предоставляет функционал для сбора и передачи криминалистически значимых данных на MXDR Console, включая содержимое папки Temp, историю браузеров, журналы событий Windows, фрагменты реестра, NTFS MFT, дампы UEFI прошивки, файлы гибернации и подкачки, дампы оперативной памяти, списки автозагрузок, запущенных процессов и служб, отложенных задач, созданных именованных каналов и открытых сетевых соединений.

– ПО совместно с MXDR Console поддерживает возможность сетевой изоляции конечной станции от глобальной и локальной сети.

– ПО совместно с MXDR Console предоставляет возможность удаленного терминального доступа к конечной станции через веб-интерфейс, независимо от статуса сетевой изоляции.

– ПО обеспечивает логирование удаленного терминального подключения, запросов на сбор криминалистически значимых данных и запросов на сетевую изоляцию через веб-интерфейс.

– ПО позволяет настраивать отправку исполняемых файлов (.exe) и установочных файлов (.msi) для проверки в подсистему поведенческого анализа (MDP) по критериям, таким как недействительная или отсутствующая цифровая подпись, загрузка из интернета, удаление антивирусами.

– ПО автоматически блокирует и помещает в карантин вредоносные файлы, ранее проанализированные подсистемой поведенческого анализа.

– ПО обеспечивает инвентаризацию установленных и удаленных приложений.

– ПО предоставляет возможность настройки политик блокировки для различных действий, таких как запуск методов установки приложений, приложений с недействительной подписью, скриптовых файлов и appx приложений.

– ПО поддерживает создание индивидуальных правил блокировки запуска приложений.

– ПО совместно с MXDR Console создает события информационной безопасности по группе событий, основываясь на поведенческих правилах.

– События информационной безопасности включают полный перечень запущенных процессов, граф процессов, формирующих события, и индикацию вредоносных процессов.

– ПО предоставляет централизованное представление о работе каждого процесса, включая данные о взаимодействии на уровне реестра, файловой системы, сетевой активности, мьютексах, метаданные процесса и перечень импортированных динамических библиотек с результатами проверки цифровой подписи и потоками исполнения.

– ПО позволяет остановку процессов через веб-интерфейс.

– ПО поддерживает Sigma правила.

– ПО логирует IP и MAC адреса сетевых периферийных устройств конечной станции.

– Подсистема поддерживает установку на операционные системы Windows старше Windows 7 SP1 и Windows Server старше 2008 R2 x64.

1.3.2 Функциональные возможности ПО применительно к конечным станциям на базе ОС ядра Linux

ПО обладает следующими функциональными возможностями:

– ПО поддерживает установку на операционные системы с ядром версии старше 3.10 и дистрибутивы, такие как Arch-based (Arch, Manjaro), Debian-based (Ubuntu 20.04+, Ubuntu Server, Linux Mint), RedHat-based (CentOS 7+, Fedora 33+, Oracle Linux 8, RedOS), которые используют систему инициализации systemd.

– ПО совместимо с установленными антивирусами и DLP-системами заказчика.

– ПО не влияет на производительность рабочей станции при соблюдении системных требований.

– ПО осуществляет сбор различных типов событий, включая:

- События, связанные с процессами: создание новых процессов (clone, fork, exec), завершение процессов, изменение прав доступа к памяти процесса, отслеживание ptrace логов.
- События, связанные с файлами: создание, открытие, удаление файлов и изменение их содержимого, изменение имени, прав доступа и владельца файлов, создание и удаление директорий.
- События, связанные с сетью: открытие сетевых соединений, привязка портов к процессам, DNS-запросы.
- События, связанные с системой: подключение и отключение USB-устройств.

- События, связанные с аудит логами: создание и удаление пользователей и групп, авторизация и выход пользователей, запуск и остановка системных сервисов.

– (или EDR), совместно с MXDR Console, предоставляет функционал для сбора и передачи криминалистически значимых данных, включая:

- Приложения, установленные с помощью пакетных менеджеров pacman, RPM и Debian.
- Отложенные задачи, история оболочки shell, Linux lock file, аутентифицированные пользователи.
- Настройки SSH, SELinux, AppArmor, модули ядра.
- Сетевые маршруты, группы пользователей, файл /etc/shadow, Unix-сокеты, DNS резолвы, сетевые интерфейсы, периферийные устройства, информация о точках монтирования, fstab, init subsystem.

– ПО совместно с MXDR Console, поддерживает сетевую изоляцию конечной станции от глобальной и локальной сети.

– ПО обеспечивает удаленный терминальный доступ к конечной станции через веб-интерфейс, независимо от статуса сетевой изоляции.

– ПО поддерживает Sigma правила.

– MXDR Console логирует удаленное терминальное подключение, фиксируя перечень введенных команд и результаты их исполнения, запросы на сбор криминалистически значимых данных и запросы на сетевую изоляцию через веб-интерфейс.

1.3.3 Функциональные возможности ПО применительно к конечным станциям на базе ОС семейства macOS

– ПО поддерживает установку на операционные системы macOS 10.15.0 Catalina и выше.

– ПО совместимо с установленными антивирусами и DLP-системами заказчика.

– ПО не влияет на производительность рабочей станции при соблюдении системных требований.

– ПО осуществляет сбор различных типов событий, включая:

- События, связанные с процессами: создание и завершение процессов, изменение директорий процессов (только для macOS 10.15.1 и выше).

- События, связанные с файлами: создание файлов, закрытие файлов, изменение размера, переименование/перемещение файлов, удаление/изменение счетчика ссылок на файлы.
- События, связанные с сетью: входящие и исходящие соединения.

– ПО совместно с MXDR Console, предоставляет функционал для сбора и передачи криминалистически значимых данных, включая:

- Настройки SSH.
- Историю оболочки shell.
- Настройки профилей Apple.
- Настройки конфигураций автоматического старта процессов.
- Файлы из директории /etc/.
- Файлы с логами из всех стандартных папок, включая логи агента и системного расширения.

– ПО, совместно с MXDR Console, поддерживает сетевую изоляцию конечной станции от глобальной и локальной сети (за исключением системных обращений, которые нельзя изолировать).

– ПО поддерживает Sigma правила.

– MXDR Console логирует запросы на сбор криминалистически значимых данных и запросы на сетевую изоляцию хоста через веб-интерфейс.

1.4 Требования к ПО

ПО устанавливается на конечную точку (рабочую машину) или сервер.

1.5 Минимальные технические требования

1.5.1 Минимальные технические требования для оборудования на базе ОС семейства Microsoft Windows

Поддерживаемые операционные системы:

Тип ОС	Версии ОС
Компьютер	Windows 7 SP1 Windows 8 Windows 8.1 Windows 10 Windows 11
Сервер	Windows Server 2008 R2 x64 Windows Server 2012 x64 Windows Server 2012 R2 x64 Windows Server 2016 Windows Server 2019 Windows Server 2022

Минимальные системные требования:

Компонент	Требование
ОЗУ	Не менее 4 Гб
Процессор	Многоядерный процессор Intel® x86-64 не ниже intel **Core i3** или аналогичный
Жесткий диск	не менее **60Gb**, со скоростью не ниже **7200RPM**

1.5.2 Минимальные технические требования для оборудования на базе ОС ядра Linux

Проверенные интеграции:

- Canonical
  - Ubuntu 18.04, Ubuntu 20+
    - `dpkg`: cold installation, hot updating
  - Ubuntu Server 18.04, Ubuntu Server 20+
    - `dpkg`: cold installation, hot updating
  - Astra Linux 1.7.2, 1.7.3, 1.7.5 SE, 2.12.45, 2.12.46
    - `dpkg`: cold installation, hot updating

- Linux Mint 21*
  - `dpkg`: cold installation, hot updating
- Kali
  - `apt`: cold installation, hot updating
- Debian 11+
  - `dpkg`: cold installation, hot updating
- Kubuntu
  `dpkg`: cold installation, hot updating
- Red Hat
  - CentOS 7.9
    - `yum`: cold installation, hot updating
  - CentOS Stream 8+
    - `yum`: cold installation, hot updating
  - Fedora 33+
    - `dnf`: cold installation, hot updating
  - Oracle 8.6+
    - `dnf`: cold installation, hot updating
  - Oracle Server
    - `dnf`: cold installation, hot updating
  - Alt Linux 9+
    - `apt-get`: cold installation, hot updating
  - RHEL 7.9+
    - `rpm`: cold installation, hot updating

- Red OS 7.2+

  - `rpm`: cold installation, hot updating

- Arch

  - Arch Linux

    - `pacman`: cold installation, hot updating

  - Manjaro Linux

    - `pacman`: cold installation, hot updating

Минимальные системные требования:

Компонент	Требование
ОЗУ	Не менее 4 Гб
Процессор	Многоядерный процессор Intel® x86-64 не ниже intel **Core i3** или аналогичный
Жесткий диск	не менее **60Gb**, со скоростью не ниже **7200RPM**

1.5.3 Минимальные технические требования для оборудования на базе ОС семейства macOS

Компонент	Требование
ОС	MacOS 10.15.0 Catalina и выше
ОЗУ	Не менее 4 Гб
Процессор	Многоядерный процессор Intel® x86-64 не ниже intel **Core i3** или аналогичный или Apple Silicon (с тактовой частотой не менее 2 ГГц и SSE 4.2 или более поздней версии)
Жесткий диск	не менее **60Gb**, со скоростью не ниже **7200RPM**

2 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО

На Рисунок 1 изображены общие принципы функционирования ПО.

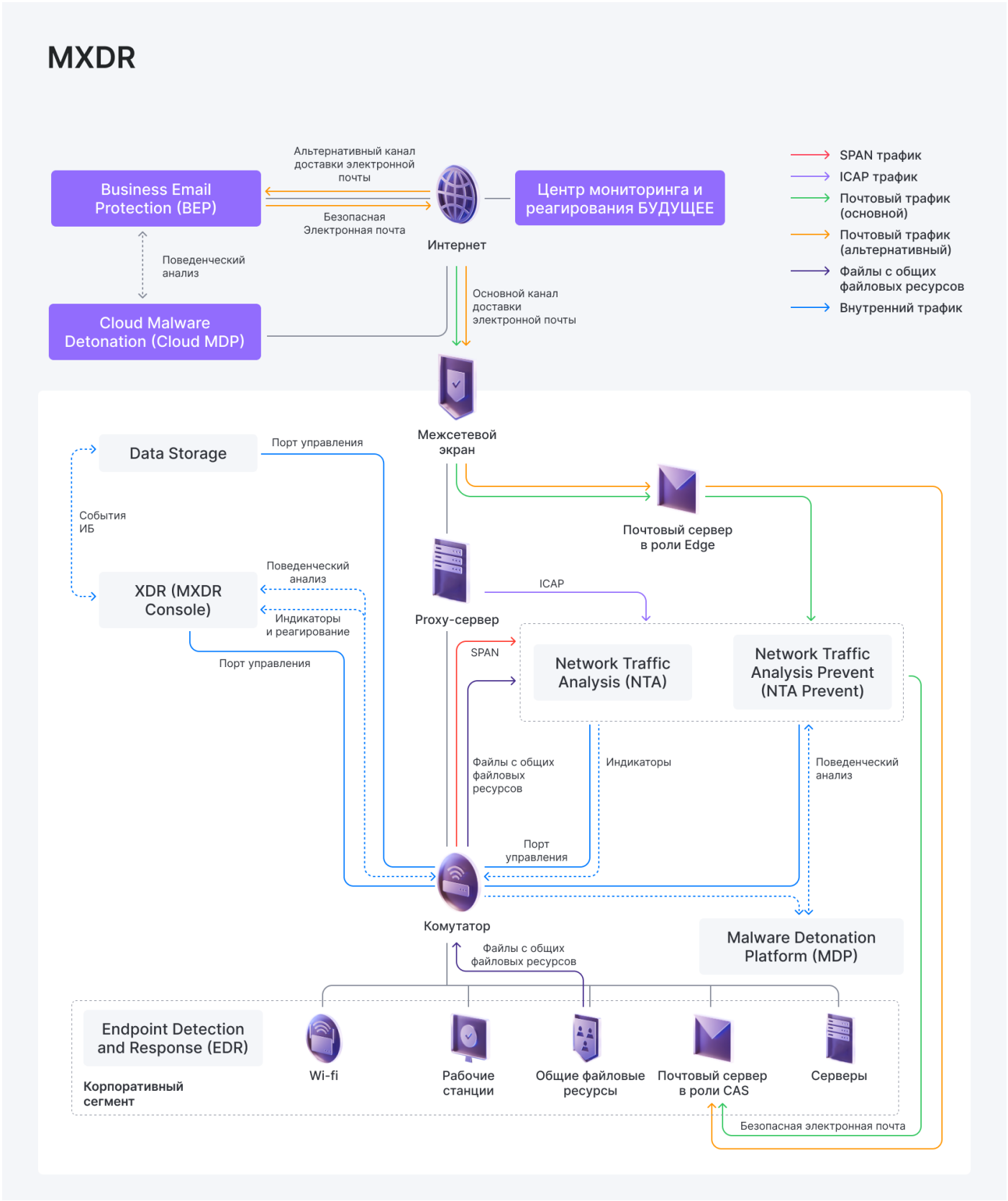

Рисунок 1. Общие принципы функционирования MXDR

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

«F6 Endpoint Detection and Response» выполняет функции обнаружения, мониторинга и реагирования на угрозы на уровне конечных точек, таких как компьютеры и серверы. ПО отслеживает активность на конечных устройствах, выявляет аномалии и подозрительные действия, указывающие на возможную угрозу, и автоматически или вручную реагирует на инциденты, изолируя заражённые устройства, блокируя процессы или удаляя вредоносные файлы.

Ключевая роль ПО заключается во взаимодействии с другими компонентами системы безопасности. Когда ПО обнаруживает подозрительное поведение или угрозу, он передаёт информацию об инциденте Центр мониторинга и реагированя, который отвечает за централизованный мониторинг и координацию всех действий по реагированию на инциденты. Центр использует эти данные вместе с информацией от сенсоров «F6 Network Traffic Analysis» для корреляции событий и анализа сетевой активности, что позволяет выявлять более сложные атаки и аномалии.

Кроме того, EDR интегрирован с модулем F6 XDR (MXDR Console), который служит центральной платформой для управления безопасностью, анализируя данные со всех компонентов системы, включая EDR. XDR использует данные от EDR для углубленного анализа инцидентов, а также для автоматизации процессов реагирования, таких как блокировка угроз или уведомление команды мониторинга.

3 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными ПО являются:

- Данные и события, связанные с активностью конечной точки:
- данные о процессах и приложениях
- действия с файлами
- сетевые подключения
- данные о сессиях

Выходными данными ПО является:

Проанализированная информация конечной точки:

- уведомления и оповещения об инцидентах
- данные для анализа и расследования
- результаты автоматизированного реагирования