ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 XDR»

Описание функциональных характеристик

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	**Описание**
ПО	Программное обеспечение «F6 XDR», «MXDR Console»
API	Application Programming Interface
CEF	Common Event Forma
JSON	JavaScript Object Notation
ICAP	Internet Content Adaptation Protocol
SMPT	Simple Mail Transfer Protocol
SOC	Security Operations Center
TI	Threat Intelligence
TTP	тактики, техники и процедуры

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящее описание функциональных характеристик содержит описание реализации программного обеспечения «F6 XDR» (далее – ПО, MXDR Console).

1.2 Назначение ПО

«F6 XDR» является центральным элементом в составе программного комплекса Managed XDR (MXDR), представляя собой высокоинтегрированную платформу для управления, мониторинга и реагирования на киберугрозы. Консоль предоставляет единый интерфейс для сбора и анализа данных из различных источников, включая сетевые устройства, системы защиты конечных точек и журналы событий, что обеспечивает централизованное управление безопасностью всей инфраструктуры безопасности. ПО поддерживает функции продвинутого поиска угроз (threat hunting) и детализированного анализа инцидентов, позволяя выявлять сложные и скрытые атаки. Автоматизация процессов реагирования на инциденты минимизирует время отклика и снижает нагрузку на команды SOC. Интеграция с внешними источниками данных о киберугрозах обеспечивает доступ к актуальной информации в режиме реального времени. Кроме того, ПО поддерживает коллективную работу, что упрощает координацию действий между специалистами. Функциональность отчетности и визуализации данных в «F6 XDR» позволяет эффективно отслеживать состояние безопасности и принимать обоснованные решения.

1.3 Функциональные возможности ПО

- Реализация центра обновлений, централизованной системы хранения данных, пользовательского интерфейса, нативной интеграции с TI-решением и API-взаимодействия.
- Поддержка развертывания в двух вариантах:
  - Cloud, где ПО размещается в инфраструктуре разработчика
  - On-prem, когда все данные остаются внутри защищаемого периметра.
- Корреляция событий всех подсистем в единой базе данных для выявления потенциальных инцидентов, а также объединение зарегистрированных событий из дочерних подсистем в единое событие информационной безопасности.
- Возможность автоматической и ручной консолидации событий информационной безопасности в единую сущность.

– Обеспечение безопасного взаимодействия между дочерними модулями через центр обновлений.

– Надежное и масштабируемое хранение данных в централизованной системе с поддержкой кластеризации для горизонтального масштабирования.

– Функционал для изоляции конечных станций от сети, блокировки вредоносных процессов и файлов с целью локализации инцидента.

– Возможность изучения инфраструктуры атакующих через регулярное сканирование IPv4-адресов и визуализацию данных в виде графа, обогащенного контекстом из системы Threat Intelligence.

– Пользовательский интерфейс в формате веб-приложения с доступом через HTTP и возможностью шифрования трафика, а также функции корреляции записей, поиска и построения отчетов.

– Настройка почтовых уведомлений для пользователей системы, включая уведомления о новых событиях, изменении статуса, ошибках интеграции и взаимодействии с центрами мониторинга.

– Поддержка почтовых уведомлений при блокировке сообщений.

– Передача на другие подсистемы обновлений сигнатур, решающих правил, индикаторов угроз и обновлений программного обеспечения.

– Возможность передачи телеметрии и информации о событиях через Syslog в форматах JSON и CEF, а также API для интеграции с другими решениями.

– Функционал для управления группами статических Suricata правил и загрузки пользовательских Suricata и YARA правил.

– Взаимодействие с Центром обновлений для обновления внутреннего ПО.

– Возможность автоматического поиска угроз на основе тактик, техник и процедур (TTP по матрице MITRE ATT&CK) с ретроспективным анализом файлов, метаинформации о сетевых соединениях и проанализированных почтовых сообщений. Технические требования к составу оборудования при размещении в инфраструктуре Заказчика

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 - Standard или Enterprise.

Параметр	Standard	Enterprise
Процессор(ы)	Intel Xeon Gold 6336Y 2.4GHz, 24C/48T, 11.2GT/s, 36M Cache, Turbo 3,6GHz, HT (185W) DDR4-3200	2 x Intel Xeon Gold 6336Y 2.4GHz, 24C/48T, 11.2GT/s, 36M Cache, Turbo 3,6GHz, HT (185W) DDR4-3200
Объем оперативной памяти	128GB	256GB
Объем хранилища Для установок MXDR Console с модулем Storage	**RAID1** 2 x 960GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS **RAID0** 2 x 960GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS	**RAID1** 2 x 960GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS **RAID0** 2 x 960GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS
Объем хранилища Для установок MXDR Console без модуля Storage	**RAID1** 2 x 960GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS **RAID5** 4 x 960GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS	**RAID1** 2 x 960GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS **RAID5** 4 x 960GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS
Сетевой интерфейс	1 Ethernet port	1 Ethernet port

1.6 Минимальные технические требования для виртуальной машины

Ниже приведены минимальные технические требования к конфигурации оборудования виртуальной машины в зависимости от типа ПО Standard или Enterprise.

Параметр	Standard	Enterprise
Виртуальный процессор	40	80
Объем оперативной памяти	128GB	256GB
Объем хранилища	**Disk 1:** 960 GB SSD, Random write 44500 IOPS **Disk 2:** 5760 GB SSD, Random write 44500 IOPS	**Disk 1:** 960 GB SSD, Random write 44500 IOPS **Disk 2:** 5760 GB SSD, Random write 44500 IOPS
Сетевой интерфейс	1 Ethernet port	1 Ethernet port

2 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО

На Рисунок 1 изображены общие принципы функционирования ПО.

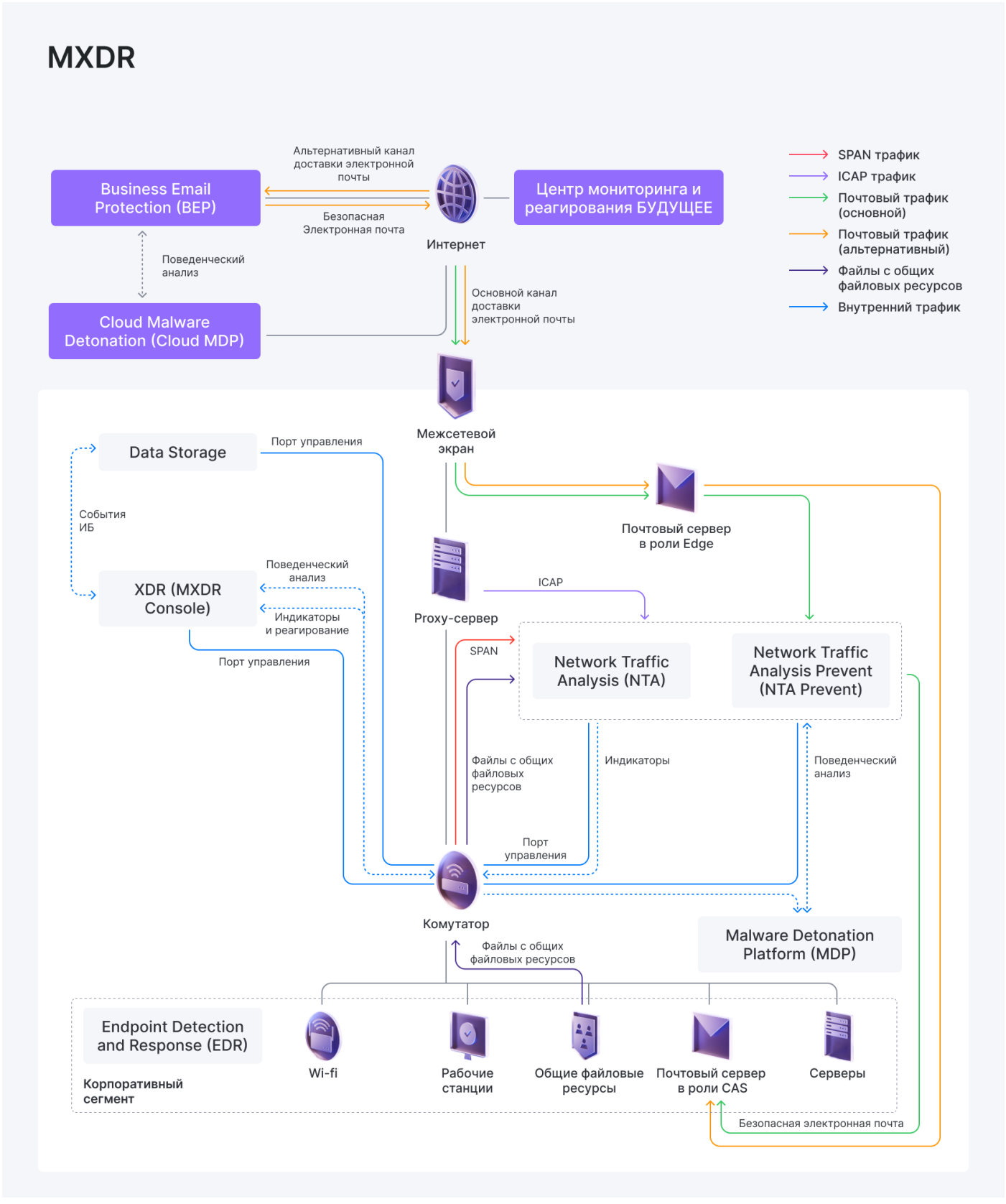

Рисунок 1. Общие принципы функционирования ПО

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.

3 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными ПО являются:

Данные от модулей системы и управляющие команды пользователей.

Выходными данными ПО является:

Проанализированная информация от модулей системы, которая разбивается на определенные группы. С их помощью проводится мониторинг, реагирование на инциденты и проведение расследований в защищаемой инфраструктуре.