ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Malware Detonation Platform»

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
ЛВС	Локальная вычислительная сеть
ОС	Операционная Система
ПО	Программное обеспечение F6 Malware Detonation Platform, MDP.
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 Malware Detonation Platform». В случае недоступности указанных систем формат взаимодействия осуществляется через электронный почтовый ящик.
CV	Computer vision
MXDR	Программное обеспечение «F6 XDR»
BEP	Программное обеспечение «F6 Business Email Protection»
EDR	Программное обеспечение «F6 Endpoint Detection and Response»
NTA	Программное обеспечение «F6 Network Traffic Analysis»
SMPT	Simple Mail Transfer Protocol

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящее описание функциональных характеристик содержит описание реализации программного обеспечения «F6 Malware Detonation Platform» (далее – ПО, Malware Detonation Platform, MDP).

1.2 Назначение ПО

«F6 Malware Detonation Platform» представляет собой специализированное решение для анализа вредоносного программного обеспечения, которое запускает подозрительные файлы в изолированной среде (песочнице), чтобы безопасно изучить их поведение (поведенческий анализ). ПО позволяет детально отслеживать взаимодействие вредоносного ПО с операционной системой, реестром, файлами и сетевыми ресурсами, предоставляя полную картину его активности без риска заражения реальной информационной инфраструктуры. ПО не только анализирует простые вредоносные файлы, но и помогает выявлять эксплойты — программы, использующие уязвимости систем для выполнения атак. Платформа поддерживает различные типы файлов для анализа, включая исполняемые файлы, документы и скрипты.

1.3 Функциональные возможности ПО

ПО обладает следующими функциональными возможностями:

– Подсистема реализуется в виде программно-аппаратного комплекса для установки в стандартную 19-дюймовую стойку с наличием как минимум одного интерфейса 1000BASE-T для подключения к ЛВС и управления.

– Анализ потенциально вредоносных файлов осуществляется в изолированной среде для обнаружения ранее неизвестных угроз.

– Использование низкоуровневого монитора для выявления поведенческих маркеров.

– Применение элементов машинного обучения для анализа.

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

– Архитектура подсистемы поддерживает гибкое горизонтальное масштабирование для повышения производительности.

– Подсистема поддерживает анализ файлов размером до 100 Мб.

– Возможность поведенческого анализа до 14,000 уникальных объектов в сутки.

– Подсистема поддерживает анализ файлов различных форматов (7z, exe, pdf и др.) в изолированной среде.

– Определение типов файлов по содержимому (Android application, архивы, Windows DLL и др.) для эффективного детектирования угроз.

– Поддержка ручной загрузки файлов на анализ с настройкой параметров виртуализации и анализа.

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

– Поведенческий анализ архивов с паролем и поиск паролей в анализируемом контексте.

– Использование гипервизора для выполнения анализа.

– Статический сигнатурный анализ и противодействие техникам обхода систем поведенческого анализа (VMEvasion, Sandbox-evasion).

– Формирование отчета по результатам анализа с детализированной информацией о процессах, сетевой активности и файловой системе.

– Создание MITRE ATT&CK матриц с указанием задействованных тактик и техник.

– Запись экрана виртуальной машины за период проведения анализа.

– Извлечение конфигурационных файлов вредоносного ПО с указанием командных центров и параметров работы.

– Атрибуция проанализированных объектов к известным инструментам, группировкам и семействам вредоносного ПО.

– Экспорт анализируемых файлов и объектов для их дальнейшего анализа сторонними экспертами.

– Поддержка операционных систем Windows XP, Windows 7, Windows 10 (x64/x86) и Android 7.

– Поддержка локализации на русском и английском языках.

– Возможность изменения маршрута для вывода трафика из виртуальных машин.

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

– Автоматический подбор конфигурации виртуальной машины для анализа экземпляров вредоносного ПО.

– Эмуляция пользовательской активности (движения мыши, нажатие клавиш, переключение между окнами).

– Использование технологии CV.

– Извлечение и запуск дополнительных команд из реестра.

– Поддержка поддельного SMTP-сервера для проведения анализа.

– Включение Mitmproxy для анализа.

1.4 Требования к ПО

ПО может быть установлено только на физический сервер.

1.5 Минимальные технические требования для физического сервера

Ниже приведены минимальные технические требования к физическому серверу в зависимости от типа Malware Detonation Platform - **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	128 GB	256 GB
Объем хранилища	2 x 960 GB SSD, SATA 6 Gb/s, Mixed Use, Random write 44500 IOPS RAID1	2 x 960 GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS RAID1
Сетевой интерфейс	1 Ethernet port	1 Ethernet port

2 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО

На Рисунок 1 изображены общие принципы функционирования ПО.

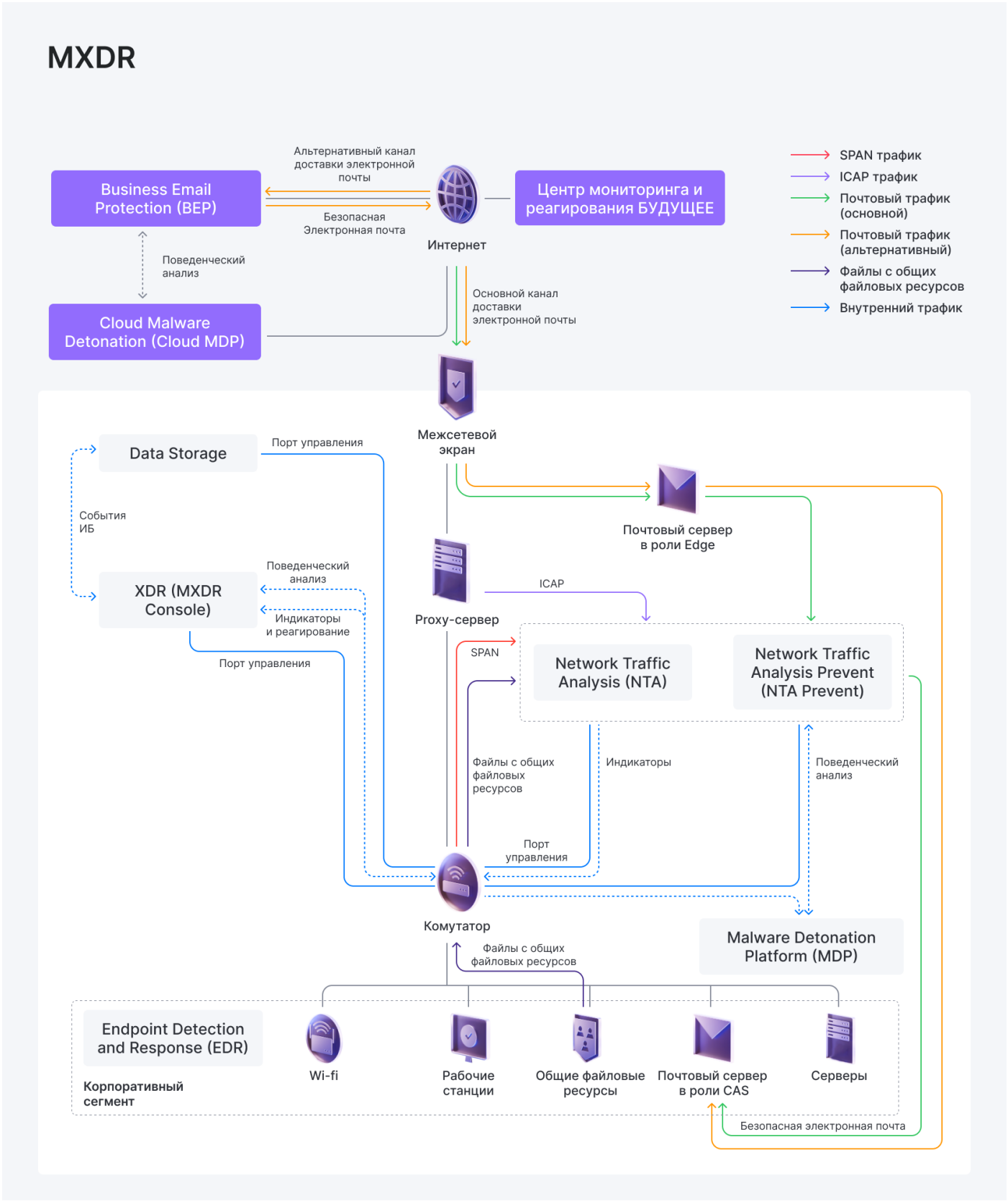

Рисунок 1. Общие принципы функционирования MXDR

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

ПО выполняет детонацию файлов и ссылок в изолированной среде, используя низкоуровневый мониторинг для поведенческого анализа и выявления неизвестных угроз. Эти объекты могут поступать от различных компонентов системы, включая NTA, EDR, BEP.

Например, при обнаружении подозрительного траффика NTA обнаруживает подозрительный сетевой трафик или подозрительные файлы, они могут быть переданы на анализ в MDP для дальнейшей детонации. Если анализ сетевого трафика выявляет подозрительное взаимодействие с внешними серверами, возможно содержащими вредоносные файлы, такие объекты будут направлены в MDP для детонации и анализа их поведения. При этом основной задачей MDP является не простое подтверждение факта вредоносности, а извлечение файловых и сетевых индикаторов компрометации, которые будут использоваться в EDR, NTA, BEP.

После завершения анализа в MDP, результаты детонации — включая графы распространения угроз, поведенческие маркеры, данные о блокировках и классификацию угроз по MITRE ATT&CK — передаются в XDR а также, MDP, EDR и NTA, и предоставляет единое представление для операторов центра безопасности.

3 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными ПО являются:

- Сетевые пакеты (сетевой траффик)
- Входящая почта
- Ссылки на файлы
- Логи активностей

Выходными данными ПО является:

Проанализированная информация конечной точки:

- Уведомления и оповещения об инцидентах
- Отчёты об индикаторах
- Метаданные для корреляции с другими системами
- Логи для расследования инцидентов