ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Network Traffic Analysis»

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 Network Traffic Analysis, NTA.
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 Network Traffic Analysis». В случае недоступности указанных систем формат взаимодействия осуществляется через электронный почтовый ящик.
CEF	Common Event Format
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
JSON	JavaScript Object Notation
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
Kerberos	Система аутентификации

LAN	Local Area Network
MDP	F6 Malware Detonation Platform
MXDR	Программный комплекс Managed Extended Detection and Response (Managed XDR)
MXDR Console	F6 XDR, MXDR
NTLM	NT LAN Manager
RDP	Remote Desktop Protocol
SMB	Server Message Block
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TI	Threat intelligence
UDP	User Datagram Protocol
URI	Uniform Resource Identifier

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящее описание функциональных характеристик содержит описание реализации программного обеспечения «F6 Network Traffic Analysis» (далее – ПО, Network Traffic Analysis, NTA).

1.2 Назначение ПО

«F6 Network Traffic Analysis» — это программное обеспечение для обнаружения и реагирования на сетевые угрозы (Network Detection and Response), предназначенное для мониторинга, анализа и предотвращения кибератак в режиме реального времени. ПО предоставляет комплексный мониторинг сетевого трафика, анализируя его для выявления подозрительных действий и угроз. Используя передовые методы, такие как поведенческий анализ, машинное обучение и сигнатурный анализ, ПО может обнаруживать сложные атаки, в том числе сетевые атаки, использование вредоносного ПО, фишинговые атаки и эксплуатацию уязвимостей. Благодаря интеграции с другими продуктами АО «БУДУЩЕЕ», такими как «F6 Threat Intelligence», ПО повышает точность обнаружения угроз и позволяет более эффективно управлять инцидентами безопасности.

ПО также поддерживает функции охоты на угрозы (Threat Hunting) и проведения форензики, что позволяет специалистам детально анализировать инциденты и выявлять их причины и последствия.

Выявление вредоносной активности, аномалий и скрытых каналов в сетевом трафике осуществляется в несколько шагов:

1. Сетевой трафик проходит через модуль сигнатурного анализа.
2. Трафик сети анализируется с помощью ML-классификаторов.
3. Сетевые сигналы (алерты) автоматически соотносятся с другими инцидентами в XDR для последующего анализа.
4. Выделенные из потока объекты отправляются на анализ в MDP платформу контролируемого запуска («детонации») вредоносных программ.
5. В XDR отправляются подробные сетевые логи для проактивного поиска недетектируемых угроз.

1.3 Функциональные возможности ПО

ПО обладает следующими функциональными возможностями:

- ПО реализуется в виде программно-аппаратного комплекса для установки в стандартную 19-дюймовую стойку с наличием как минимум одного интерфейса 1000BASE-T для захвата сетевого трафика и одного интерфейса 1000BASE-T для управления и подключения к ЛВС.
- Подключение осуществляется к интерфейсу копии сетевого трафика без влияния на работу ЛВС и без вмешательства в анализируемое сетевое взаимодействие.
- По осуществляет захват сетевых фреймов на уровне L2, восстановление пакетов L4 - L7 и реализует следующие функций:
  - Сигнатурный анализ трафика на основе базы решающих правил.
  - Выявление инкапсуляции данных в трафике, включая ICMP tunneling, DNS tunneling, HTTP tunneling, DGA.
  - Запись трафика и сохранение его на сетевом хранилище в формате .pcap.
  - Регистрация информации обо всех сетевых соединениях на уровне TCP, UDP, IP, ICMP с фиксацией времени, числа пакетов и объема переданных данных.
  - Регистрация информации о DNS-запросах с фиксацией времени, источника и получателя запроса, содержимого запроса и ответа.
  - Регистрация информации о HTTP-запросах с фиксацией времени, источника и получателя, метода, URI и всех заголовков.
  - Регистрация информации о соединениях по протоколам RDP, SMB, DHCP, FTP, Kerberos, NTLM, SMTP, SSH, Telnet, SSL.
- ПО выявляет попытки горизонтального перемещения, атакующего внутри ЛВС и передает соответствующую информацию в XDR для формирования события информационной безопасности.
- ПО поддерживает обработку каналов с консолидированной пиковой загрузкой до 1 Гбит/сек.
- ПО имеет озможность инвентаризации сетевого оборудования и конечных устройств в пассивном режиме.
- ПО осуществляет передачу в XDR параметры телеметрии для отслеживания аварийных ситуаций, перегрузок и параметров работы, включая:

- Количество выделенной и свободной памяти.
- Среднюю загрузку процессора по ядрам.
- Число пакетов, поступивших на интерфейсы приема трафика.
- Общий объем данных, поступивших на интерфейсы приема трафика.
- Объем свободного пространства на жестком диске.
- Передача телеметрии и информации о событиях осуществляется через механизм Syslog в форматах JSON и CEF для интеграции с другими системами.

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 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	**1000**	**5000**	**10 000**
Процессор	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 оперативной памяти	64 GB	64 GB	128 GB
Объем хранилища	2 x 960 GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS RAID1	2 x 960 GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS RAID1	2 x 960 GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS RAID1
Сетевые интерфейсы			
Интерфейс управления	1 Ethernet	1 Ethernet	1 Ethernet
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.

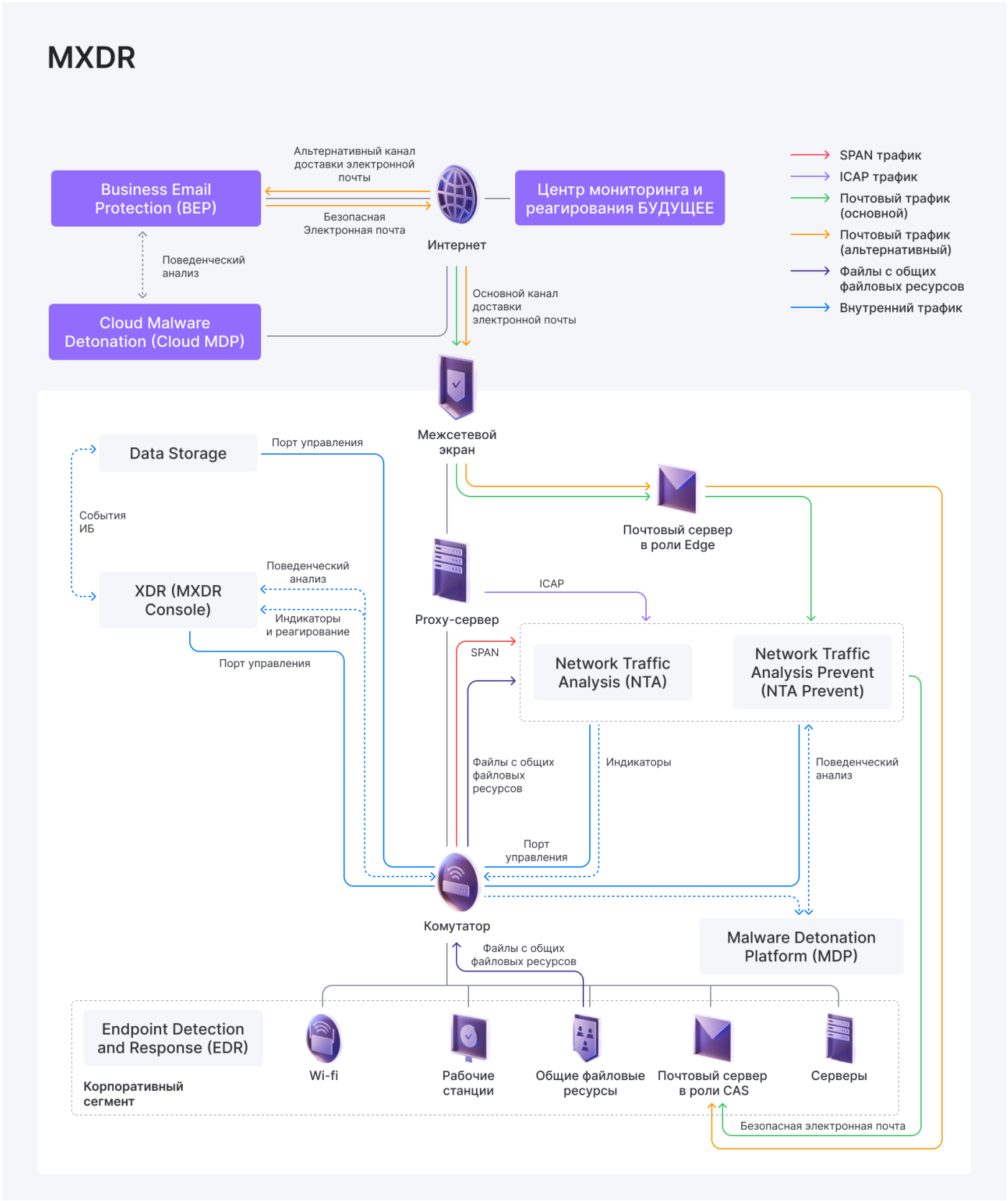

Рисунок 1. Общие принципы функционирования MXDR

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

ПО выполняет функции мониторинга и анализа сетевого трафика для обнаружения и предотвращения киберугроз. NTA непрерывно отслеживает весь сетевой трафик, анализируя пакеты и поведение сетевых устройств как внутри сети, так и при внешних взаимодействиях. Используя методы поведенческого анализа и машинного обучения, NTA выявляет аномалии в трафике, такие как необычные объёмы данных, подозрительные подключения или нестандартное поведение, которые могут указывать на возможную атаку. NTA также взаимодействует с другими компонентами, такими как межсетевые экраны и системы предотвращения вторжений, для автоматической блокировки подозрительного трафика или изоляции устройств в случае обнаружения угроз. Помимо этого, NTA собирает метаданные и логи сетевых соединений, что помогает проводить детализированные расследования инцидентов и выявлять пути распространения угроз.

3 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными ПО являются:

- Сетевые пакеты (сетевой траффик)
- Метаданные соединений
- Логи активностей

Выходными данными ПО является:

Проанализированная информация конечной точки:

- уведомления и оповещения об инцидентах
- Отчёты о сетевых инцидентах
- Метаданные для корреляции с другими системами
- Логи для расследования инцидентов