Программное обеспечение

«F.A.C.C.T. Network Traffic Analysis»

Руководство по установке и эксплуатации

СОДЕРЖАНИЕ

Аннотация

Настоящий документ содержит руководство администратора программного обеспечения «F.A.C.C.T. Network Traffic Analysis» (далее – ПО).

1. Назначение ПО

F.A.C.C.T. Network Traffic Analysis — решение для обнаружения и реагирования на сетевые угрозы (NDR), обеспечивающее мониторинг, анализ и предотвращение кибератак в реальном времени. ПО использует поведенческий анализ, машинное обучение и сигнатурный подход для выявления сложных угроз, включая атаки, вредоносное ПО и фишинг. ПО также поддерживает функции охоты на угрозы (Threat Hunting) и проведения форензики, что позволяет специалистам детально анализировать инциденты и выявлять их причины и последствия.

ПО функционирует в следующих программно-аппаратных средах:

1. Аппаратные среды:
    a. Сервера со следующими техническими требованиями:

Таблица 1 Технические требования для NTA

NTA Сенсор (нагрузка Mbps)	250	1000	5000	20000
CPU	3,9 GHz, 4 C, 8 MB	3,9 GHz, 4 C, 8 MB	2.4 GHz, 14 C, 35 MB	2.4 GHz, 14 C, 35 MB
RAM, GB	32	32	64	128
HDD, GB	2 x 480	2 x 1200	2 x 1200	2 x 1200
Network				

mgmt Ethernet	1	1	1	1
Span	до 4 Ethernet	до 4 Ethernet or SFP	до 4 SFP/SFP+	до 4 SFP+

Таблица 2 Технические требования для XDR

XDR	Enterprise	Performance	**Storage**
CPU	2.4 GHz, 14 C, 35 MB	2.4 GHz, 28 C, 35 MB	2.4 GHz, 14 C, 35 MB
RAM, GB	96	128	64
HDD, GB	4 x 1200	4 x 1200	2 x 1200 HDD + 2 x 960 SSD
Network			
mgmt Ethernet	1 или более	1 или более	1 или более

Таблица 3 Технические требования для EDR

Операционная система	Windows 7	Windows 8/8.1	Windows 10/11
CPU	Не ниже Inter core i3 второго поколения	Не ниже Intel core i3 второго поколения	Не ниже Intel core i3 второго поколения
RAM, GB	4	4	4
HDD, MB	100	100	100
Network			
Тип соединения	Связь с XDR	Связь с XDR	Связь с XDR

2. Виртуальные среды:
    a. Hyper-V
    b. Vmware Esxi
    c. Qemu
    d. Xen-server
3. Использование браузеров для доступа к системе:
    a. Windows Internet Explorer версии 8.0 и выше
    b. Google Chrome версии 4.0 и выше
    c. Mozilla Firefox версии 3.5 и выше
    d. Apple Safari версии 4.0 и выше
    e. Opera версии 10.5 и выше
    f. iOS Safari версии 3.2 и выше
    g. Opera Mobile версии 11.0 и выше
    h. Google Chrome for Android версии 11.0 и выше
    i. Mozilla Firefox for Android версии 26.0 и выше
    j. Windows Internet Explorer Mobile версии 10.0 и выше

В браузере устройства пользователя должно быть включено исполнение скриптов JavaScript

2. Настройки доступа и учетных записей

Доступ к ПО предоставляется через Веб-интерфейс.

Доступ к Веб-интерфейсу доступен авторизованным клиентам.

Доступ через Веб-интерфейсу предоставляется по запросу.

Внимание! При возникновении проблем со входом в Систему обратитесь в службу Технической поддержки Разработчика по электронной почте mxdr@facct.ru.

3. Общие принципы функционирования ПО

XDR - система анализа, корреляции, принятия решений и управления всеми компонентами комплекса.

NTA - сенсор анализа данных, подключаемый к копии сетевого трафика защищаемой организации. Является так же модулем почтовой интеграции для проведения анализа почтовых сообщений совместно с MDP

MDP - модуль поведенческого анализа файлов, получаемых из почты, целевых хостов (с помощью EDR), файловых хранилищ, ICAP клиентов. Позволяет детектировать неизвестные ранее угрозы и продвинутые целевые атаки.

EDR – программное обеспечение для сбора данных о поведении пользователя и программ, обеспечивающее фиксацию полной хронологии событий на системе, блокировку аномального поведения, изоляцию хоста, отправку данных в удаленное хранилище для последующего анализа.

ПО - это комплексное решение, направленное на повышение качества обнаружения новых и неизвестных угроз, атак без использования вредоносных программ, обеспечение процесса threat hunting, оптимизацию процессов реагирования на инциденты и их последующего расследования именно внутри корпоративной инфраструктуры.

4. Обязанности и функции администратора заказчика

В обязанности администратора входит следующее:

- Произвести встраивание ПО в защищаемую инфраструктуру
- Поддерживать функционирование ПО

5. Порядок встраивания

Для встраивания ПО в защищаемую инфраструктуру необходимо выполнить следующие шаги:

- Выбор схемы встраивания в инфраструктуру;
- Выбор типа взаимодействия ПО с АС АО «Будущее»;
- Определение точек съёма трафика в инфраструктуре заказчика для сигнатурного анализа;
- Определение способа интеграции с почтовыми серверами заказчика;
- Определение необходимости подключения ПО к файловым хранилищам заказчика для поведенческого анализа файлов
- Встраивание XDR с выбранным режимом работы в инфраструктуру заказчика;
- Встраивание XDR с учётом точек съёма трафика, почтовой интеграции, интеграции с файловыми хранилищами и с учётом установки XDR;
- Установка EDR на защищаемых хостах заказчика;
- Встраивание MDP с учётом установки NTA, EDR, XDR;
- Обеспечение связности всех модулей с XDR;
- Определить перечень IP-подсетей заказчика, которые будут определены как защищаемые и ввести эти данные в ПО;
- Интеграция почтовой системы;
- Интеграция файлового хранилища;

5.1. Выбор схемы встраивания в инфраструктуру

Существует следующие критерии встраивания в инфраструктуру:

1. Почтовая интеграция:
    a. BCC

   b. Inline
2. Сетевая интеграция:
   a. SPAN
   b. RSPAN
   c. SPAN over GRE
3. Файловая интеграция:
   a. ICAP
   b. Файловые хранилища
   c. Анализ файлов из трафика

5.1.1. Почтовая интеграция

Поддерживаются несколько различных способов получения писем для поведенческого анализа:

1. BCC – анализ копии писем
   a. Получение писем по SMTP.
   b. Получение писем с помощью механизма скрытой копии (BCC)
2. Inline – анализ оригинальных писем. Получение писем по SMTP с блокировкой.

Получение писем по SMTP

При данной интеграции NTA выступает как MTA (или SMTP Relay), получаю копию всей входящей почты через SMTP. Единственное отличие этого режима, от режима с блокировкой, что письма тут не пересылаются дальше, а просто анализируются.

Получение писем с помощью механизма скрытой копии (BCC)

При данной интеграции создаётся дополнительный почтовый ящик, куда осуществляется копирование всей входящей почты. NTA подключается к подготовленному ящику и забирает письма для анализа.

Получение писем по SMTP с блокировкой (inline-режим)

Основной режим интеграции с почтой, когда почта проходит через NTA как через SMTP Relay, и доставляется дальше после анализа. Соответственно вредоносные письма блокируются. Отказоустойчивость обеспечивается либо на

уровне DNS, либо на уровне SMTP-сервера, где настраивается несколько релеев, либо на уровне VRRP, когда несколько устройств делят виртуальный IP адрес.

5.1.2. Сетевая интеграция

Съём трафика осуществляется с коммутаторов заказчика либо с маршрутизаторов с наличием SPAN функций. Система обеспечивает анализ трафика, подаваемого на оборудование NTA из разных источников:

- SPAN
- RSPAN трафик
- SPAN/RSPAN траффик в GRE-туннеле

SPAN и RSPAN определяют копирование трафика на уровне L2 модели OSI.

SPAN/RSPAN over GRE определяют копирование трафика на уровне L3 модели OSI.

5.1.3. Файловая интеграция

По мимо получения файлов для поведенческого анализа из почтового трафика, имеется следующие возможности:

a. ICAP
b. Файловые хранилища
c. Анализ файлов из трафика

ICAP обеспечивает интеграцию с проксирующими решениями для получения скачиваемых файлов и их последующего анализа в модуле BEP.

Интеграция с файловыми хранилищами обеспечивает поведенческий анализ файлов и автоматическое удаление найденного вредоносного программного обеспечения (ВПО).

Анализ файлов из трафика позволяет собирать из анализируемого SPAN трафика файлы для поведенческого анализа, в случае если трафик нешифрованный.

5.2. Выбор типа взаимодействия ПО с АС АО «Будущее»

Тип взаимодействия ПО с АС АО «Будущее» определяет список обмениваемых данных между заказчиком и производителем. Расположение настройки описано в одноимённом разделе в пунктах описывающих интерфейс ПО.

- Не обновлять систему

Данный режим подразумевает полностью закрытую инсталляцию. XDR никак не взаимодействует с серверами. Обновление программного обеспечения, IOC и сетевых сигнатур не производится.

- Получать только обновление ПО и правил

Данный режим позволяет оборудованию получать обновления ПО для XDR и всех подключённых к нему устройств. Обновление индикаторов и сигнатур не производится. В данном режиме нет возможности загружать данные по инфраструктуре атакующих и отсутствует взаимодействие с SOC для получения поддержки по инцидентам в режиме 24/7. Обновления доставляются с сервера - `92.53.76.98:443/tcp`

- Обновления + одностороннее получение TI

Данный режим дополняет предыдущий и позволяет получать обновление индикаторов атак и сигнатур для подключённых к XDR устройств. В данном режиме невозможно получать мониторинг и поддержку от CERT (SOC). В данном режиме имеется возможность загружать данные по инфраструктуре атакующих вручную.

- Обновление + двухсторонний обмен индикаторами

Данный режим дополняет предыдущий и позволяет выгружать данные об обнаруженных инцидентах в сервера. Имеется возможность автоматически получать информацию по инфраструктуре атакующих. В данном режиме имеется возможность мониторинга и поддержки от CERT в режиме 24/7.

5.3. Определение точек съёма трафика в инфраструктуре заказчика для сигнатурного анализа

При организации зеркалирования следует учитывать, что трафик пользователей корпоративных прокси-серверов и сегментов сети, расположенных за NAT'ом, должен зеркалироваться до проксирования/натирования, как можно ближе к пользовательскому сегменту, до любого фильтрующего оборудования, чтобы в заголовках пакетов были видны оригинальные IP-адреса клиентов, а также для исключения фильтрации части трафика средствами межсетевых экранов. Это упростит реагирование на выявленные сетевые инциденты.

5.4. Определение способа интеграции с почтовыми серверами заказчика

Доступные способы интеграции:

- BCC via POP3/IMAP
- BCC via SMTP
- Inline режим via SMTP

Выбор почтовой интеграции определяется следующими критериями:

a. Особенности почтовой инфраструктуры клиента – общая рекомендация, использовать BCC via SMTP интеграцию – самую простую в реализации и наиболее эффективную при организации мониторинга атак через почтовую систему.
b. Необходимость автоматической блокировки опасных писем – использование inline режима.

5.5. Определение необходимости подключения ПО к файловым хранилищам заказчика для поведенческого анализа файлов

ПО имеет возможность проводить поведенческий анализировать файлов, хранящихся на файловых хранилищах заказчика в момент их изменения или запроса пользователями.

Поддерживаемые протоколы подключения:

- SMB

- FTP
- WebDav

5.6. Встраивание XDR с выбранным режимом работы в инфраструктуру заказчика

Для работы должен быть доступен для подключения сетевой адрес:

- Для получения обновлений используется адрес - 92.53.76.98:443/tcp
- Для получения данных по инфраструктуре преступников и использования преимуществ SOC АО «Будущее»

При необходимости работа XDR с SOC может осуществляться через прокси-сервер. В этом случае должен поддерживаться метод CONNECT. Дополнительные сетевые настройки доступны в разделах XDR активация и Прокси-сервер

5.6.1. XDR активация

Перед настройкой решение необходимо активировать, то есть зарегистрировать лицензионный ключ, полученный при покупке или тестировании решения на серверах.

Для первичной активации XDR должен иметь доступ до инфраструктуры АО «Будущее»

Сетевые настройки для присваивания IP адреса доступны в консоли XDR. Обратитесь в раздел Подключение к консоли XDR

Web-интерфейс доступен по адресу https://ip_addr_xdr.

При открытии web-интерфейса вас будет приветствовать меню активации XDR.

Шаг 1: Информация о компании

Данные занесённые в разделе Информация о компании будут использованы для активации лицензии и должны соответствовать реальным данным клиента.

- Название организации

- E-mail администратора - будет использоваться в качестве имени пользователя при аутентификации в системе
- Пароль / Подтверждение пароля - пароль администратора для входа в систему
- Часовой пояс

Шаг 2: Активация лицензии

- Адрес сервера лицензии - https://soc.facct.com:40500
- Серийный номер - номер выданный при покупке или тестировании XDR
- (Опционально) - прокси-сервер в формате http(s)://user:password@proxyFQDN:port

Шаг 3: Создание удостоверяющего центра

Создать CA - запускает процесс генерации мастер-пароля для дальнейшей настройки и добавления оборудования (сенсоров и BEP).

Сохраняйте ваш мастер-пароль в надёжном месте - он будет использоваться при подключении компонентов BEP, MDP, EDR.

Начать Пользоваться - позволяет завершить процесс активации XDR.

5.6.2. Подключение к консоли XDR

Консоль XDR доступна администратору следующими способами:

- С помощью KVM (D-SUB для видео и USB для клавиатуры).
- С помощью последовательного порта:
  - Baudrate: 115200
  - 8-bit
  - Flow control: ON
- Через SSH при условии настроенного сетевого подключения.

Логин / Пароль консоли XDR

Для управления сервером используйте учетную запись с логином tds и паролем tds.

После ввода логина и пароля на экран будет выведена основная информация о XDR.

Для входа в главное меню выберите Enter the Shell.

Не забудьте изменить пароль по умолчанию!

5.6.3. Главное меню XDR

Пункты главного меню:

Show current network settings: просмотр и изменение настройки сети.

a. Configure network:
b. Configure proxy:
c. Configure managment interface:
d. Back: вывод основной информации о статусе сервера. Эта информация также выводится при входе в систему.

Configure network

Доступны следующие варианты настроек:

a. DHCP: автоконфигурация адреса и прочих настроек по протоколу DHCP. Производится автоконфигурация интерфейса и перезапуск сети.
b. Static: статическая конфигурация параметров. Требуется ввод всех сетевых параметров вручную, после чего производится перезапуск сети. Для отмены ввода параметров в любой момент используется сочетание Ctrl+C.
c. Cancel: возврат на уровень меню выше.

Configure proxy

Настройка прокси-сервера для доступа к обновлениям и облачному сервису. XDR позволяет настроить использование прокси-сервера для доступа к обновлению базы сигнатур и правил анализа трафика для всех компонент XDR. В процессе настройки устройство запрашивает конфигурационную строку в следующем формате: Login:pass@domen_proxy:port

При этом необходимо выбрать тип проксирования: http-proxy или socks-proxy.

Проверьте введенные значения:

Proxy Settings -> Show current proxy settings

Для успешного использования прокси-сервера, он должен поддерживать метод CONNECT с открытием соединений на 443 порт.

Configure managment interface

В данном меню предоставляется возможность выбора из доступных на XDR интерфейсов управляющий. Управляющий интерфейс будет использоваться всеми компонентами для работы с XDR.

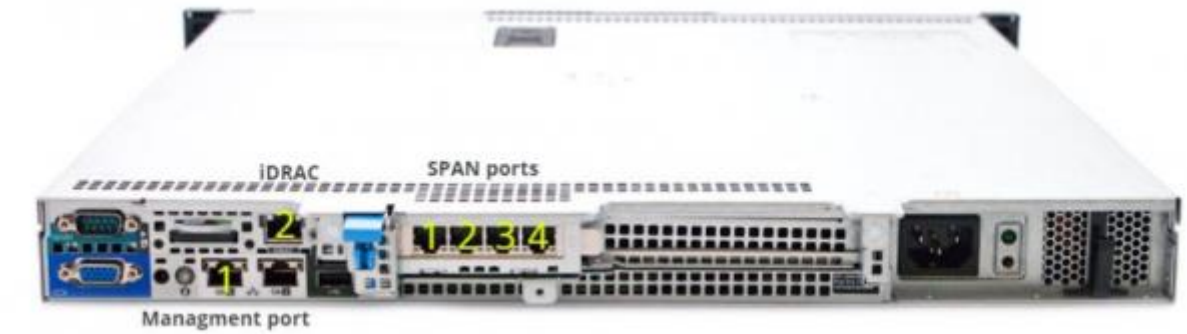
5.7. Встраивание NTA с учётом точек съёма трафика, почтовой интеграции, интеграции с файловыми хранилищами и с учётом установки XDR

В базовой комплектации NTA имеет четыре сетевых интерфейса для приема трафика и один порт для подключения к сети и управления.

При необходимости работа NTA с Group- SOC / XDR может осуществляться через прокси-сервер. В этом случае должен поддерживаться метод CONNECT для установления подключений на 443 порт.

5.7.1. Подключение к сети и захват трафика

На Изображении отмечены все необходимые интерфейсы, используемые при интеграции и нормального функционирования:



Изображении 1. Интерфейсы NTA

Интерфейс №1 (см. Изображении 1) расположены на задней панели и используется для управления устройством и связи с SOC / XDR, а также для коммуникации с модулем MDP. По умолчанию интерфейс сконфигурирован для получения настроек сети по протоколу DHCP. Сетевые настройки порта управления можно поменять при помощи технической консоли. Интерфейсы для захвата трафика расположены справа от порта управления и нумеруются от 1 до 4. (см. Изображение 1).

Для работы устройства один или несколько портов захвата трафика должны быть соединены кабелем с источником трафика. Таким источником может быть сетевое устройство с настроенным зеркалированием (SPAN/RSPAN в терминах оборудования CISCO), либо TAP-устройство, копирующее ethernet-кадры на самом низком уровне, либо GRE-туннель со SPAN-траффиком.

NTA захватывает зеркалированый трафик на уровне L2.

L3 mirroring, включая ERSPAN не поддерживается устройством и не является допустимым способом зеркалирования трафика на устройство.

NTA сенсор поддерживает SPAN in GRE: Когда необходимо пропустить SPAN-трафик через несколько устройств уровня L3, либо взять его с фермы виртуальных машин, возможно создать GRE-туннель между XDR и источником SPAN-трафика.

При организации зеркалирования следует учитывать, что трафик пользователей корпоративных прокси-серверов и сегментов сети, расположенных за NAT’ом, должен зеркалироваться до проксирования/натирования, как можно ближе к пользовательскому сегменту, до любого фильтрующего оборудования, чтобы в заголовках пакетов были видны оригинальные IP-адреса клиентов, а также для исключения фильтрации части трафика средствами межсетевых экранов. Это упростит реагирование на выявленные сетевые инциденты.

На задних панелях серверов NTA, правее от порта управления, расположены порты iDRAC. (см. Изображении 1 и Изображении 2). Данный интерфейс позволяет реализовать такие функции, как развертывание, обновление, мониторинг и обслуживание серверного оборудования.

5.7.2. Активация сенсора и синхронизация с XDR

Активация сенсора - включает функционал сенсора.

Синхронизация сенсора - привязывает сенсор к XDR либо к SOC, тем самым предоставляя возможность управления сенсором через обозначенные системы.

Для взаимодействия сенсора с XDR необходимы следующие порты:

- 443/tcp - для первичной активации и привязки сенсора (единоразово)
- 1443/udp - для дальнейшего взаимодействия сенсора с XDR
- 3000/tcp - для взаимодействия сенсора с MDP

Активация и синхронизация осуществляется через консоль NTA.

На данном этапе статус Galaxy Connection равен Fail. Так как сенсор не привязан к XDR.

После нажатия Enter the Shell(рис.1) в открывшемся меню пункт Activation отвечает за активацию и синхронизацию.

В меню выбора Central Authority задаётся сервер синхронизации. Он определяет дальнейший режим работы сенсора: on-premise или on-cloud. Доступные пункты меню:

- On-cloud инсталляция. Оркестрация сенсором осуществляется через SOC
- On-premise инсталляция. Оркестрация сенсором осуществляется через XDR

При выборе On-premise необходимо задать доменное имя или IP адрес XDR.

При выборе On-cloud необходимо задать доменное имя или IP адрес SOC. (задано по умолчанию)

При работе сенсора через прокси сервер задайте адрес прокси в формате:

Login:pass@domen_proxy:port

В пункте Device UUID задаётся номер лицензии (UID) полученного в пункте добавления нового оборудования в соответствующем меню XDR

При нажатии OK запускается процесс регистрации и синхронизации сенсора с выбранным сервером. Внимание: после данной операции мигрировать сенсор с одной инфраструктуры на другую невозможно без вмешательства технической поддержки АО «Будущее».

После регистрации сенсора консоль будет приветствовать пользователя своим UUID введённым на предыдущем шаге.

Панель инструментов в консоли сенсора будет отображать Galaxy Connection со статусом OK.

Меню Настройки -> Устройства -> Сенсор в веб интерфейсе XDR будет предоставлять информацию по состоянию подключенного устройства.

5.7.3. Подключение XDR к NTA

Доступ к консоли NTA можно получить любым из нижеперечисленных способов:

- С помощью KVM (D-SUB для видео и USB для клавиатуры).
- С помощью последовательного порта:
  - Baudrate: 115200
  - 8-bit
  - Flow control: ON
- Через SSH при условии настроенного сетевого подключения.

Для управления сервером используйте учетную запись с логином tds и паролем tds.

После ввода логина и пароля на экран будет выведена основная информация о NTA. Для входа в главное меню выберите Enter the Shell.

Не забудьте изменить пароль по умолчанию!

5.7.4. Меню CLI NTA

Пункты главного меню:

1. Network menu: просмотр и изменение настройки сети.

2. Change password: меню изменения административного пароля пользователя tds.
3. Debug shell: доступ до инструментов отладки в режиме командной строки
4. Power management: меню выключения или перезагрузки устройства.
5. Back: вывод основной информации о статусе сервера. Эта информация также выводится при входе в систему.

5.7.5. Настройка сети NTA

Пункты меню настройки сети:

1. Show current network settings: вывод текущий настройки сетевого интерфейса управления.
2. Configure network: настройка сетевого интерфейса.
3. Configure proxy: настройки прокси для работы с SOC / XDR.
4. Configure managment interface: настройки управляющего интерфейса.
5. Traffic monitor Setup: меню для ввода пула адресов, принадлежащих внутренней сетевой инфраструктуре, а также для указания SPAN интерфейсов.
6. Back: возврат на уровень меню выше.

Configure network

Доступны следующие варианты настроек:

1. DHCP: автоконфигурация адреса и прочих настроек по протоколу DHCP. Производится автоконфигурация интерфейса и перезапуск сети.
2. Static: статическая конфигурация параметров. Требуется ввод всех сетевых параметров вручную, после чего производится перезапуск сети. Для отмены ввода параметров в любой момент используется сочетание Ctrl+C.
3. Cancel: возврат на уровень меню выше.

Configure proxy

Настройка прокси-сервера для доступа к обновлениям и облачному сервису или локальному сервису XDR. NTA позволяет настроить использование прокси-сервера для доступа к обновлению базы сигнатур и правил анализа трафика, а

также связи с облачным сервисом или локальным сервисом XDR. В процессе настройки устройство запрашивает конфигурационную строку в следующем формате:

Login:pass@domen_proxy:port

При этом необходимо выбрать тип проксирования: http-proxy или socks-proxy.

Проверьте введенные значения:

Proxy Settings -> Show current proxy settings

Для успешного использования прокси-сервер должен поддерживать возможность осуществления запросов методом CONNECT с открытием соединений на 443 порт.

Configure managment interface

Предоставляет возможность задания управляющего интерфейса в NTA. Для задания выберите из списка интерфейсов нужны и нажмите ок.

Traffic Monitor Setup

Позволяет указать локальные интерфейсы, а также интерфейсы для SPAN/RSAN/SPANinGRE:

- Укажите локальные адреса, принадлежащие сети, а также адреса локальных Proxy. Введите список локальных подсетей и исключите из них адреса Proxy-серверов (!proxy-ip). Это позволит отличить взаимодействие с внешними узлами.

Configure network -> Configure Homenet

- Выберите SPAN-интерфейсы:

Configure network -> Setup monitored ifaces

5.8. Установка EDR на защищаемых хостах заказчика

Установка EDR перед началом установки необходимо получить файл:

- gibep.msi

и 2 конфигурационных файла:

- config_tds.txt
- config_tds.sign.txt

Эти файлы необходимо поместить в локальную директорию. Важно, что полный путь до директории не должен содержать кириллических символов и пробелов. Для примера поместим эти файлы в C:\EDR

После этого необходимо запустить cmd.exe с правами Администратора, перейти в директорию с установочным и конфигурационными файлами и выполнить команду:

- msiexec /i gibep.msi /qn /L*V install.log CONFIG_FILE=C:\EDR\config_tds.txt CONFIG_SIGN_FILE=C:\EDR\config_tds.sign.txt

5.9. Встраивание MDP с учётом установки NTA, EDR, XDR

Настройка MDP производится в настройках NTA, а для EDR обеспечивается XDR после синхронизации.

Настройка располагается по адресу WUI ->Настройки -> Устройства -> Сенсор -> Редактировать настройки и предлагает возможность интегрировать выбранный NTA с определенным MDP для осуществления функций поведенческого анализа.

Интеграция NTA с MDP

В меню задаётся запись в виде доменного имени или IP адреса MDP. Возможно задать больше чем одну запись, дабы обеспечить распределение нагрузки по поведенческому анализу. Управление очередью производится на стороне сенсора. Сенсор делает опрос всех подключённых к нему MDP на предмет размера очереди поведенческого анализа и выбирает минимальную для следующего анализа.

Язык анализа

Задаёт использование определённых образов операционных систем внутри подключённых MDP. Данные операционные системы будут настроены для

поддержания защиты от актуальных угроз в регионах с выбранной языковой системой (По умолчанию поддерживаются Русский и Английский языки).

5.10. Обеспечение связности всех модулей с XDR

Для работы ПО необходима связность на сетевом уровне всех модулей, а также связь на уровне протоколов ниже:

XDR

- Для доступа к инфраструктуре :
  - :443/tcp - режим "TI Feed", т.е. с туннелем
  - 92.53.76.98:443/tcp (для режима доставки обновлений через https)
- Для доступа к устройствам NTA и MDP для их обновления и поддержки:
  - 22/tcp каждого из устройств
- Прямой NAT наружу в интернет для выпуска виртуальных машин MDP, если он происходит через XDR

NTA

- Для связи с XDR:
  - 1443/udp на ip-адрес XDR
- Доступ к Proxy-серверу, либо прямой NAT наружу для скачивания ссылок

MDP

- Для связи с XDR:
  - 1443/udp на ip-адрес XDR
- Прямой NAT наружу в интернет для выпуска виртуальных машин MDP, если он происходит автономно, мимо XDR

5.11. Определение перечня IP-подсетей заказчика, которые будут определены как защищаемые и ввод этих данных в ПО

Настройка находится по адресу WUI -> Настройки -> Устройства -> Сенсор –> Редактировать настройки -> Анализ сетевого трафика

Важнейший раздел при настройке сигнатурного анализа. Данный раздел даёт системе понимание "инородного" трафика относительно легитимного. Позволяет указать локальные интерфейсы, а также интерфейсы для SPAN/RSAN/SPANinGR.

Укажите локальные адреса, принадлежащие сети, а также адреса локальных Proxy. Введите список локальных подсетей и исключите из них адреса Proxy-серверов (!proxy-ip). Это позволит отличить взаимодействие с внешними узлами.

5.12. Интеграция почтовой системы

Настройки по выбранному типу интеграции находятся в разделах:

Интеграция NTA с почтовой системой

- Интеграция по POP3/IMAP
- Интеграция по SMTP

Inline-режим почтовой интеграции

- Требования к Inline интеграции
- Включение MTA-режима

6. Интерфейс администратора

Интерфейс доступен при открытии в браузере страницы https://ip_addr_XDR. Пользователю будет предложена форма аутентификации. Для входа в систему используйте логи/пароль администратора, заданные в процессе активации XDR или выданные вам данные, созданные в разделе Пользователи.

Смена языка интерфейса доступна на странице ввода имени пользователя и пароля в верхнем правом углу. А также в меню настроек пользователей.

6.1. Dashboard

Меню предоставляет возможность наблюдения за общими показателями всех компонент системы в графическом виде. Каждый виджет предоставляет возможность наблюдать различные показатели подсистем и настраивается под нужды пользователя.

Для создания нового виджета кликните по кнопке **Добавить виджет** в правом верхнем углу панели и выберите тип из выпадающего списка. Виджеты возможно реорганизовывать в необходимом пользователю порядке. Для этого зажмите кнопку в виде пересекающихся стрелок в правом верхнем углу виджета и перетащите виджет в нужное место. Для удаления виджета выберете кнопку **Удалить**.

6.1.1. Состояние устройства

Виджет предоставляет данные о CPU, RAM, HDD по всем подключенным к XDR устройствам. Данные по нагрузке предоставляются в режиме онлайн. По отключенным / несинхронизированным устройствам данные будут пустыми.

По каждому устройству доступно:

- Тип устройства

Тип компоненты решения XDR

- Имя устройства

Имя заданное при создании заведении нового устройства в разделе настройки

- CPU/RAM/HDD

Нагрузка на оборудование в данный момент

Примечание: нагрузка по ПК с установленными EDR не выдаётся. Вместо неё описывается количество хостов с онлайн статусом

6.1.2. Последние алерты

Виджет предоставляет список крайних по дате алертов возникших в системе. По щелчку на алерте происходит переход к полному описанию в разделе Алерты. Что бы перейти к списку всех алертов нажмите Show All в правом верхнем углу виджета. По каждому алерту доступно:

- Цель

Сущность, участвующая в инциденте в качестве жертвы (IP, domainname, email)

- Время

Время первого события связанного с данным алертом в формате гггг-мм-дд чч:мм

6.1.3. Статистика алертов по классификатору и критичности

Виджет предоставляет диаграмму с количеством алертов за выбранный период по выбранному сенсору.

В правом верхнем углу виджета находится меню выбора классификатора

Доступные данные по выбранному классификатору:

- Алертов - общее количество алертов
    - Активных - в процессе разрешения
    - Решенных - решенные инциденты
    - Ложных - ложные срабатывания
- Критичность
    - Низкий
    - Средний
    - Высокий
    - Критический

6.1.4. Статистика событий по классификатору

Предоставляет данные по количеству событий сразу по всем классификаторам за выбранный временной период в виде диаграммы.

6.1.5. График событий по классификатору

Представляет график количества событий по каждому классификатору за выбранный период времени. Каждая кривая описывает статистику одного классификатора по всем подключенным к XDR компонент данного типа (классификатора).

График возможно фильтровать - отображать на нём отдельные кривые. По умолчанию все фильтры отключены. При выборе одного из фильтров кривая соответствующая названию фильтра перестаёт отображаться (вычёркивается).

Доступные фильтры:

- MDP

Количество событий от всех компонентов типа MDP подключенных к XDR.

- Sensor

Количество событий от всех компонент типа NTA подключенных к XDR.

- Endpoint

Количество событий от всех компонент типа EDR подключенных к XDR.

6.1.6. График SPAN интеграции

График зависимости общей нагрузки на всех SPAN интерфейсах выбранного сенсора к выбранному периоду времени. Так же предоставляет данные по дропам ядра в том же масштабе. Для отображения данных задайте сенсор через меню выбора сенсора.

График возможно фильтровать - отображать на нём отдельные кривые. По умолчанию все фильтры отключены. При выборе одного из фильтров кривая соответствующая названию фильтра перестаёт отображаться (вычёркивается).

Доступные фильтры:

- Мбит/сек

Нагрузка на всех SPAN интерфейсах

- Дропы в ядре

Потери пакетов на уровне ядра операционной системы.

6.1.7. Статистика SPAN интеграции

Предоставляет диаграмму с данными по нагрузке на SPAN интерфейсы выбранного сенсора в режиме онлайн. Отображаемые данные:

- Лицензионное ограничение

Максимально допустимая нагрузка на сенсор в соответствии с приобретённой лицензией (Мбит/с).

- Текущая нагрузка

Нагрузка к данному моменту времени.

- Свободный канал

Свободная нагрузочная полоса для приёма SPAN трафика. Разница между первым и вторым пунктами.

- Минимальная нагрузка

Минимальная нагрузка с момента заведения SPAN трафика на анализ в выбранный сенсор.

- Максимальная нагрузка

Максимальная нагрузка с момента заведения SPAN трафика на анализ в выбранный сенсор.

- Дропы на интерфейсе

Потери пакетов в физической среде передачи SPAN трафика.

- Дропе в ядре

Потери пакетов на уровне операционной системы сенсора.

6.1.8. График электронной почты

График отображает статистику по принятым почтовым сообщениям и проанализированным вложениям у выбранного сенсора на указанном отчётном периоде. По меню выбора сенсора доступны подключенные к XDR сенсоры:

График возможно фильтровать - отображать на нём отдельные кривые. По умолчанию все фильтры отключены. При выборе одного из фильтров кривая соответствующая названию фильтра перестаёт отображаться (вычёркивается). Доступные фильтры:

- Envelope

Количество входящих (принятых) письменных сообщений.

- File

Количество вложенных в принятых почтовых сообщениях файлов.

6.1.9. Статистика почтовой интеграции

Предоставляет диаграмму с данными по количеству принятых письменных сообщений и письменных сообщений с вложениями на выбранном сенсоре.

6.1.10. График числа online-хостов с EDR

График отображает количество ПК с установленными на них EDR со статусом онлайн на временной шкале. Временная шкала задаётся в меню выбора отчётного периода.

6.1.11. График числа системных событий EDR

График отображает статистику по числу событий на всех EDR обнаруженных за указанный отчётный период.

6.2. Алерты

Данный раздел предоставляет информацию о всех происходящих потенциальных инцидентах, детектируемых компонентами NTA, MDP, EDR подключенными к XDR. Таким образом в разделе реализуются функции мониторинга и реагирования на события информационной безопасности. Система предоставляет список алертов с общими данными. Внутри каждого алерта доступна подробная информация, а именно:

- График активности - граф связности событий по данному алерту
- События с полным описанием релевантной данному алерту информацией
- Хронология событий - комментарии и история работы по алерту.
- Информация по инфраструктуре атакующих связанная с данным алертом
- Инструменты для блокирования хостов - если на них установлены EDRt

6.2.1.Алерт

Алерт - потенциально зловредное воздействие на инфраструктуру клиента. Состоит из множества событий скоррелированных из различных подсистем XDR и атрибутированных определенной угрозе и (возможно) группе злоумышленников. В алертах отображаются события, зарегистрированные подсистемами:

- Сигнатурного анализа: NTA выявляет случаи совпадения содержимого сетевых сессий с известными шаблонами вредоносного трафика;
- Поведенческого анализа: MDP - технология анализа поведения файлов. Поведенческие маркеры и классификатор позволяет выявить вредоносную активность файла;
- Агент контроля рабочих станций: EDR- установленный агент на ПК.

Список алертов

Каждый пункт представляет из себя алерт состоящий из множества событий различных подсистем XDR

Общие данные по алертам:

1. Создан - время и дата создания алерта. То есть формальная дата обозначения набора событий, как потенциально вредоносных. Вообще говоря, может быть позже, чем даты событий, породивших данный алерт.
2. Статус - атрибут, служащий для отображения информации о текущем статусе работ по решению заявки.
    a. Обнаружен - выявлена потенциально вредоносная активность, требуется реакция.
    b. Заблокирован - вредоносная активность была заблокирована системой XDR.
3. Причина - отображаются модули системы XDR:
    a. endpoint_activity - активность агента контроля рабочей станции;
    b. network_anomaly - сигнатурный анализ;
    c. malicious_file - файл, проанализированный модулем поведенческого анализа.
4. События - количество событий.
5. Сенсор - наименование сенсора.

6. Цель - в данном столбце указывается адрес назначения и адрес источника, IP-адрес, наименование компьютера. Символизирует цель атаки злоумышленников.
7. Уровень опасности - цветовая индикация на левой границе алерта

   Каждому алерту выдаётся уровень опасности. Уровень опасности определяет степень критичности алерта в соответствии с классификатором уровней угроз.

   Доступные уровни опасности:

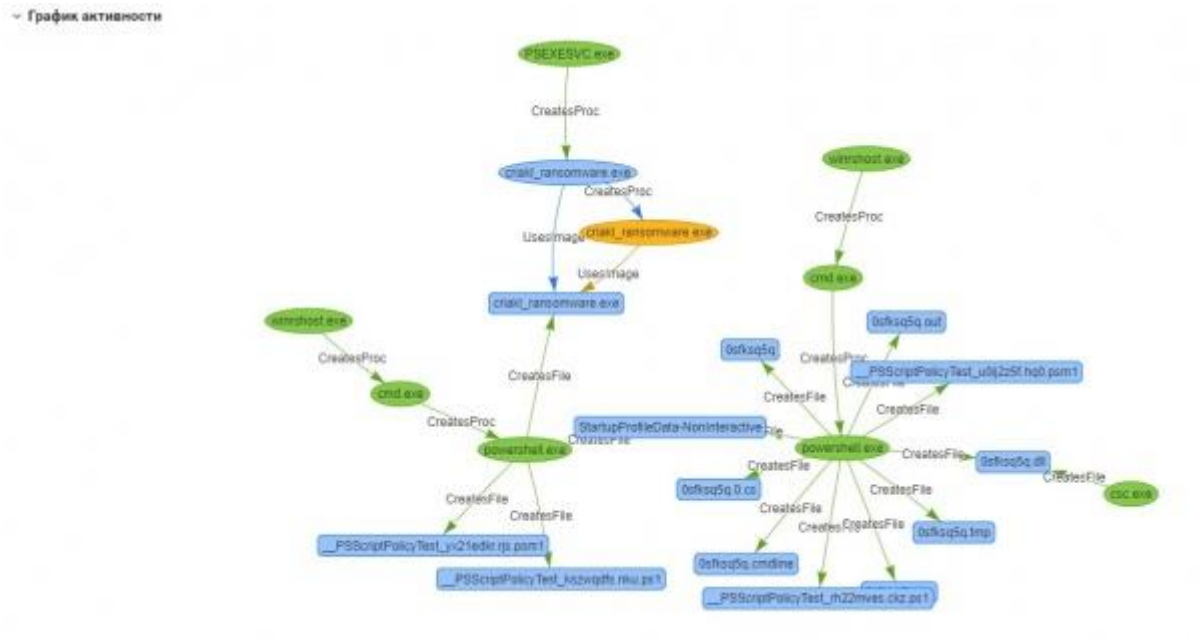
   - Критический - события с красным уровнем угроз, указывающие на таргетированные атаки и критические заражения устройств в сети, требующие моментального реагирования.
   - Средний - события с желтым уровнем угроз, также могут свидетельствовать о потенциально выявленных угрозах.
   - Низкий - события с зеленым уровнем угроз, нарушающие политику безопасности в организации, например, нежелательное ПО, легальные шпионские плагины и т.д.

6.2.2. Информация об алерте

После раскрытия алерта предоставляется полная информация по потенциальному инциденту и инструменты по работе с обнаруженными событиями.

6.2.2.1. График активности

График активности представляет из себя связный направленный граф, в котором узлами являются задействованные в алерте артефакты событий, а ребрами указывается воздействие или взаимодействие артефактов событий друг с другом. График активности предоставляет ретроспективный взгляд на развитие алерта во времени. По графику возможно определить точку начала атаки, а так же дальнейшие пути её распространения со всеми затронутыми артефактами на ПК, в случае, если используется компонент EDRt. Граф возможно масштабировать, а так же менять в нём абсолютное расположение вершин не меняя связности графа для более удобного изучения аналитиком.



6.2.2.2. Временная шкала событий

Временная шкала событий представляет из себя формальное описание всех событий, связанных с алертом. Источником данных событий могут служить:

- NTA
- MDP
- EDR
- Внешний threat hunting

Фильтрация временной шкалы событий

События выстроены в виде убывающего по времени списка (крайние по времени события отображаются первыми).

Листать события возможно с помощью кнопок в левом нижнем углу. По мимо этого имеется возможность фильтрации событий следующими инструментами:

- Поиск - текстовый поиск по всем полям событий
- Уровень угрозы - отображает только события заданного уровня угроз. Не путайте уровень угроз события и уровень угроз алерта - это разные показатели!
    - Низкий
    - Средний
    - Критический

- Источник событий - отображает только события полученные из выбранной компоненты.
    - Сенсор
    - Полигон
    - Endpoint

Общие данные по временной шкале событий:

- Дата

Дата возникновения события в ПК, трафике, почте или при проверке передаваемых файлов.

- Время

Время возникновения события в ПК, трафике, почте или при проверке передаваемых файлов.

- Event

Событие, связанное с выбранным алертом в сокращённом виде. Подразумевает под собой потенциально вредоносное, вредоносное или связанное с вредоносным воздействие, выявленное одной из компонент системы.

- Индикаторы

Индикатор события. Краткий перечень важных артефактов события (IP адреса, домены, ссылки, файлы). Полный перечень доступен при раскрытии события. Временная шкала событий может содержать различное количество различных событий от различных источников (компонент) системы. Ниже описываются три типа событий (по типу источника).

6.2.2.2.1. Сигнатурный анализ

События, зарегистрированные системой сигнатурного анализа - это случаи совпадения содержимого сетевых сессий с известными шаблонами вредоносного трафика. По клику на любое из событий открывается более подробная информация о каждом из событий.

По клику на любое из событий открывается подробная информация о событии (рис. Подробная информация о событии), которая включает:

- Сведения об источнике
  - ID сенсора - уникальный номер оборудования NTA;
  - Протокол, Интеграция - указывает на способ интеграции и протокол реализации;
  - Время - время и дата сработки;
  - От кого - источник, инициировавший коммуникацию;
  - Кому - адрес назначения;
- Сведения об угрозе
  - URLs - запрошенный URI участвующий в зловредной коммуникации
  - SID - уникальный номер сигнатуры
  - Удаленные хосты - хосты использовавшиеся для проведения атаки
- Исходные данные

  Предоставляет заголовок коммуникаций, относящихся к данному событию в различных форматах. При анализе события существует возможность увидеть данные в формате: HTTP, ASCII, HEX

6.2.2.2.2. Поведенческий анализ

Данный тип событий предоставляет базовые детали об объекте анализа.

- Сведения об источнике - состав сведений меняется в зависимости от типа интеграции и используемого протокола
  - ID сенсора - идентификатор сенсора через который объект анализа был отправлен на MDP
  - Протокол, Интеграция - протокол и способ интеграции по средствам которого был получен объект анализа
  - Время - время получения объекта анализа
  - От кого - источник коммуникации из которого получен объект анализа
  - Кому - получатель коммуникации из которой получен объект анализа
- Сведения об угрозе - состав зависит от типа интеграции и используемого протокола
  - Удалённые хосты - хост используемый для атаки в результате которой был получен объект анализа

    - URI - полная ссылка на ресурс, из-за обращения на которую был получен объект анализа
    - Тема - Тема письма из которого был получен объект анализа
    - Имя файла
    - MD5/SHA1/SHA256 - Значение хешей объекта анализа
    - Вердикт - результат анализа (подробнее в разделе Вердикт ниже)
    - SID
- Исходные данные

6.2.2.2.3. Вердикт поведенческого анализа

При клике на Вердикт страница перенаправляет пользователя на детальный анализ семпла в песочнице MDP. В блоке “Видео” содержится видео выполнения (открытия) объекта анализа так, как оно выглядело бы на мониторе при открытии на полноценном компьютере. По данному видео часто можно судить о природе атаки и даже о достоверности зарегистрированного события. Следует учесть, что некоторые виды вредоносного ПО скрывают всю свою вредоносную активность от пользователя.

Общие данные

- Доступные данные:
- Оценка вредоносности

  Вероятностная оценка степени вредоносности анализируемого объекта. Высчитывается методами машинного обучения исходя из выявленных в ходе поведенческого анализа индикаторов.
- Известные имена

  Имена ВПО под которыми оно может быть известно
- MD5/SHA1/SHA256
- Время анализа

  Время окончания анализа объекта
- Размер файла
- Иконка
- Тип файла

Файловая структура

Блок определяет способ организации, хранения и именования файлов в анализируемом объекте.

Таким образом объект может состоять из нескольких объектов анализа. Каждый объект в данной структуре может быть раскрыт для более детального рассмотрения информации по нему.

Для удобства восприятия в файловой структуре применяется цветовое различие типов объектов:

- Оранжевый – исполняемые объекты
- Жёлтый – контейнеры
- Голубой – документы
- Чёрный – прочие файлы

Поведенческие маркеры

Блок перечисляет причины, почему данный объект был отнесен к вредоносным. Большинство маркеров имеют индикаторы, подтверждающие вредоносность поведения - например, изменяемые ключи реестра, создаваемые файлы, изменения в чужих процессах и т.д. Индикаторы должны использоваться аналитиком для подтверждения угрозы.

Каждый маркер раскрывается для получения конкретной информации по анализируемому объекту относительно данного маркера.

Разделяют следующие типы маркеров:

- Вредоносные

  Однозначно вредоносные
- Прочие

  Маркеры не являющиеся вредоносные, но которые могут помочь при детальном анализе ВПО аналитиком

Сетевая активность

В блоке фиксируются детали о сетевом трафике, сгенерированном после открытия (выполнения) анализируемого объекта. В частности, в нем содержится

информация о DNS- и HTTP-запросах и доступна возможность скачивания PCAP-файла с полным дампом данных запросов.

Дерево процессов

В блоке содержится дерево процессов в состоянии после запуска объекта анализа. Применяется цветовая легенда: Красным цветом выделяются процессы исследуемого объекта, желтым - процессы созданных (дропнутых) файлов. При клике на любой из процессов можно получить детали по активности процесса и вносимых системных изменениях.

6.2.2.3. Хронология событий

Описывает общие события по алерту, начиная с первого события связанного с алертом и продолжая последующей работой ведущейся по данному инциденту. Включает в себя комментарии по работе с данным инцидентом.

Реагирование на инциденты

При реагировании на алерт, рекомендуется оставлять комментарии. Для добавления вложений необходимо нажать на кнопку 

Для закрытия тикета, требуется отметить галочкой напротив события и нажать на **пометить решенными.**

Если же событие является ложноположительным, то необходимо нажать на **пометить ложными.**

Блокировать заражённый хост

Данный функционал доступен только при наличии EDR установленного на ПК. После активации блокирует все входящие и исходящие сетевые соединения ПК за исключением общения с XDR.

6.2.3. Фильтры

Фильтры типов

По кнопке фильтры в левом верхнем углу веб-интерфейса открывается меню фильтрации.

Доступные фильтры для алертов:

- Уровень угрозы - выбор алертов с выбранным уровнем угроз:
  - Низкий.
  - Средний.
  - Критический.
  - Пусто.
- Блокировка - статус файлов:
  - Да - отображать только заблокированные файлы.
  - Нет - отображать только незаблокированные файлы.
- Ложное срабатывание - false-postitive срабатывания.
  - Да - отобразить только срабатывания помеченные как ошибочные.
  - Нет - убрать все ложные срабатывания из выборки алертов.
  - Пусто - отображать ложные алерты в общей выборке.
- Решенные - отображение разрешенных алертов:
  - Да - отображать только решённые.
  - Нет - убрать все решенные из общей выборки алертов.
  - Пусто - отображать решенные алерты в общей выборке.
- Система интеграции - выбор алертов содержащих в себе события выбранного способа интеграции:
  - Сетевой трафик - события из анализируемого SPAN трафика.
  - Endpoint - события с ПК с установленной компонентой EDR.
  - Почтовый сервер - события полученные после анализа почтовых сообщений при SMTP интеграции
  - Почтовый ящик - события полученные после анализа почтовых сообщений при BCC интеграции
  - ICAP-сервер - события полученные при анализе файлов от ICAP клиентов
  - Файловый сканер - события полученные при анализе файлов файловых хранилищ
  - Пусто - отображать алерты всех типов событий в выборке.
- Классификатор - выбор алертов содержащих события от выбранной подсистемы(компоненты) XDR :
  - Sensor - события от сенсоров.
  - MDP - события из "песочницы" MDP.

- Endpoiont - события с хостов с установленной компонентов EDR.
- Пусто - отображать алерты всех типов подсистем в выборке.

Фильтры дат и текста

По мимо данного типа фильтров доступен общий фильтр по датам с возможностью текстового запроса по всем полям алертов и событий. (рис. Фильтр по датам и полям событий)

6.3. Расследование

Данный раздел предоставляет информацию о всех обработанных письмах и файлах в MDP, подключенными к XDR, а также предоставляет информацию о хостах, на которых установлен EDRt. Раздел состоит из следующих подразделов:

- Письма
- Файлы
- Компьютеры

6.3.1. Письма

Раздел содержит всю информацию по почтовому трафику. В разделе отображаются все почтовые сообщения, прошедшие анализ в системе, в том числе и не имеющие вредоносных показателей. Раздел предоставляет возможность управлять карантином писем, в случае использования MTA-режима.

6.3.1.1. Общие данные по письмам

Раздел состоит из списка, каждый пункт которого представляет из себя почтовое сообщение. В списке предоставляются общие данные по письмам:

- Дата создания - время и дата письма, полученного на анализ.
- Сенсор - наименование сенсора через который происходит анализ письма. Рядом с именем сенсора указывает тег, указывающий на способ почтовой интеграции данного сенсора (BCC, MTA, MAILBOX, SPAN)
- От кого - источник письма.
- Кому - адрес назначения письма.
- Тема - Тема письма.

- Статус - атрибут, служащий для отображения информации о текущем статусе по анализу письма:
    - Безопасный - в ходе поведенческого анализа, признаки вредоносной активности не выявлены.
    - Проверяется - письмо находится в процессе анализа.
    - Вредоносный - в поведенческих маркерах письма были выявлены признаки вредоносного программного обеспечения.
    - Заблокированное - письмо заблокировано и находится в карантине (применяется при MTA интеграции)
    - Принудительное - письмо выведено из карантина администратором комплекса и отправлено оригинальному получателю (применяется при MTA интеграции)

Информация о письме

Раскрывая отдельный пункт списка писем, становится доступным детальная информация о почтовом сообщении. А также в правом верхнем углу находятся данные о проверке SPF, DKIM записей и возможность скачать почтовое сообщение в формате EML (кнопка скачать eml), в случае если письмо признано вредоносным.

- Проверенные объекты

Предоставляет список проверенных объектов, вложенных в почтовое сообщение. Данные по объектам:

    - Дата и время - время окончания проверки данного объекта системой поведенческого анализа.
    - SHA1 - хэш сумма объекта в формате SHA1.
    - Сведения об объекте - имя объекта и его размер. В случае если объект признан вредоносным, размер объекта становится активной ссылкой на сам объект. По нему можно получить файл для дополнительного анализа.
    - Статус - вредоносное или безопасное вложение.
- Заголовки письма

В данном подразделе описываются все технические SMTP заголовки почтового сообщения.

- Хронология событий

Предоставляет список важных событий, по почтовому сообщению, начиная с момента получения данного письма сенсором.

6.3.1.2. Управление карантином

При реализации MTA режима письма, заблокированные системой попадают в карантин XDR. Данные письма отображаются в настоящем разделе со статусом Заблокированное.

Для управления заблокированными письмами в карантине:

1. Выберите письма - разметив необходимое количество в крайней левой колонке.
2. Нажмите на кнопку **Принудительная отправка** в правом верхнем углу раздела.

После этого письма будут принудительно отправлены оригинальным получателям. Статус письма изменится с Вредоносное Заблокированное на Вредоносное Принудительное. О данном изменении так же будет запись в Хронологии событий.

6.3.1.3. Фильтры

Фильтры типов

По кнопке фильтров в левом верхнем углу веб-интерфейса открывается меню фильтрации.

Доступные фильтры для алертов:

- Вердикт по письму - выбор вердикта писем:
  - Вредоносный.
  - Безопасный.
  - Проверяется.
  - Пусто.
- SPF - статусы проверки записи SPF
  - Пройдена - отображать только письма, отправители которых прошли SPF.

    - Не пройдена - отображать только незаблокированные файлы.
    - Отсутствует - SPF запись у отправителя отсутствует.
    - Пусто - отображать все.
- DKIM - статусы проверки записи DKIM
    - Пройдена - отображать только письма, отправители которых прошли SPF.
    - Не пройдена - отображать только незаблокированные файлы.
    - Отсутствует - DKIM запись у отправителя отсутствует.
    - Пусто - отображать все.
- Наличие ссылок - отображение писем в которых есть ссылки.
    - Есть - ссылки в письме присутствуют.
    - Отсутствует - ссылки в письме отсутствуют.
    - Пусто - отображать все.
- Наличие вложений - отображение писем в которых есть вложения.
    - Есть - вложения в письме присутствуют.
    - Отсутствует - вложения в письме отсутствуют.
    - Пусто - отображать все.
- Размер файла - указать размер вложений:
    - От
    - До
- Статус письма
    - Получено - письмо получено сенсором.
    - Не обработано - письмо находится в очереди на обработку.
    - Обработано - письмо обработано и готово к отправке на анализ в песочницу.
    - Отправлено - файл отправлен в песочницу на анализ.
    - Проанализировано - файл проанализирован.
    - Байпасс - письмо слишком долго висело в системе(настройка “Таймаут проверки писем (мин.) и было отправлено адресату до завершения работы с ним.
    - Принуд. доставка - письмо было доставлено пользователю принудительно, с помощью на
    - Анализ завершен - работа с письмом в системе завершена. Событие Finished в ленте.

    - Белый список - письма не были проанализированы, т.к. отправитель находится в белом списке.
    - Ошибка - любая ошибка с письмом. В событии обозначена причина этой ошибки.
- Источник - фильтрация писем по способу почтовой интеграции
    - SPAN - попытки сбора почтовых сообщений из SPAN трафика
    - MAILBOX - интеграция системы через почтовый ящик по POP3/IMAP, на который предварительно перенаправляются копии почтовых сообщений для анализа
    - MTA - интеграция в inline-режиме
    - BCC - интеграция через приём SMTP копии входящего потока почтовых сообщений

Фильтры дат и текста

По мимо данного типа фильтров доступен общий фильтр по датам с возможностью текстового запроса по всем полям почтовых событий. (рис. Фильтр по датам и полям событий)

6.3.2. Файлы

Раздел содержит всю информацию о файлах, которые были переданы системе XDR для поведенческого анализа.

6.3.2.1. Общие данные по файлам

Раздел состоит из списка, каждый пункт которого представляет из себя объект поведенческого анализа (файл). В списке предоставляются общие данные по файлам:

- Дата создания - время и дата файла, полученного на анализ.
- Сенсор - наименование сенсора через который происходит анализ файла. Рядом с именем сенсора указывает тег, указывающий на способ почтовой интеграции данного сенсора (BCC, MTA, MAILBOX, SPAN)
- Источник файла - указывается тег, указывающий на способ получения файла (смотри Фильтры файла)
    - От - источник файла.
    - Кому - адрес назначения.

- Имя файла - имя объекта.
- SHA1 - хеш-сумма файла.
- Статус - атрибут, служащий для отображения информации о текущем статусе по анализу файла:
    - Безопасный - в ходе поведенческого анализа, признаки вредоносной активности не выявлены.
    - Обработка - файл находится в процессе анализа.
    - Вредоносный - в поведенческих маркерах письма были выявлены признаки вредоносного программного обеспечения.

6.3.2.2. Фильтр

По кнопке фильтров в левом верхнем углу веб-интерфейса открывается меню фильтрации.

Фильтры файлов

Доступные фильтры для файлов:

- Вердикт по файлу:
    - Безопасный
    - Вредоносный
    - Проверяется
- Размер файла
    - От
    - До
- Источник файла - фильтрация по типу используемого протокола при перехвате файла в сетевом потоке
    - BRO - используется BRO фильтр
    - HTTP
    - FTP
    - ICAP
    - MAIL - используется один из протоколов почтовой интеграции
    - SMB

6.3.3. Компьютеры

В данном разделе представлен список компьютеров, подключенных с помощью EDR к XDR. По каждому ПК предоставляются общие данные по системе и используемому оборудованию, а также алерты в чьих артефактах участвовал данный ПК.

6.3.3.1. Список компьютеров - общие сведения

Общая информация по компьютерам:

- Версия - версия EDR установленного на ПК
- Имя компьютера - сетевое / доменное имя ПК
- Пользователь - последний авторизованный пользователь ОС ПК
- ОС - используемая версия операционной системы ПК
- IP-адрес - первый адрес в списке сетевых адресов ПК
- Последняя активность - дата последней активности endpoint
- Статус
- Алерты - количество связанных с данным ПК алертов

6.3.3.2. Информация о компьютере

При открытии выбранного компьютера система предоставляет все данные собранные о системе.

6.3.3.2.1. О компьютере

Доступная информация:

- Имя - сетевое / доменное имя ПК
- Домен - домен ПК в Active Directory
- ОС - полная версия используемой операционной системы
- Статус - ON/OFF состояние ПК
- Первая активность - первый отстук EDR в систему XDR
- Последняя активность - последний зафиксированный отстук EDR
- MachineID - идентификатор ПК в системе XDR. Формируется EDR-ом.

6.3.3.2.2. Оборудование

Доступная информация:

- Процессор - полное техническое наименование используемого центрального процессора
- BIOS - наименование BIOS
- RAM - количество оперативной памяти

6.3.3.2.3. Сеть

- MAC-адрес
- IP-адрес
- Первая активность - первая сетевая активность интерфейса, зафиксированная с момента установки EDR
- Последняя активность - крайняя сетевая активность интерфейса, зафиксированная с момента установки EDR

6.3.3.2.4. Хранилище

Название	Емкость
ST2000DM001-1CH164	2000.4 GB
SanDisk SDSSDA120G	120.03 GB

Хранилище

Доступная информация: Предоставляет данные об установленных накопителях в системе

6.3.3.2.5. Пользователи

Список авторизованных, с момента установки Endpoint, пользователей.

Имя пользователя	Тип пользователя	Тип логина	Первая активность	Последняя активность
edrinstaller	n/a	local	2019-03-13 15:11	2019-03-18 16:37
rozhnov	n/a	local	2019-03-13 14:27	2019-03-18 15:19
dwm-1	n/a	local	2019-03-18 16:57	2019-03-18 16:57

Пользователи

Доступная информация:

- Имя пользователя

- Тип пользователя - Доменный/не доменный пользователь
- Тип логина - локальный или удалённый логин
- Первая активность
- Последняя активность

6.3.3.2.6. Алерты

Представляет список алертов в чьих событиях встречался MachineID данного ПК. (Полностью идентичен одноимённому разделу)

6.3.3.3. Фильтры

Фильтры типов

По кнопке фильтров в левом верхнем углу веб-интерфейса открывается меню фильтрации.

Доступные фильтры для компьютеров:

- Статус - статус работы endpoint на компьютере:
  - Online
  - Offline

Фильтры текста

По мимо данного типа фильтров доступен общий фильтр с возможностью текстового запроса по всем полям компьютеров. Например, по имени пользователя. (рис. Фильтр по полям)

6.4. Настройки

В данном разделе расположены настройки управления всех модулей ПО.

6.4.1. Устройства

Пункт Appliances служит для предоставления возможности настроек всех компонентов подключённых к XDR.

Доступные компоненты:

- NTA
- MDP

- XDR
- EDR

6.4.1.1 Общие данные по устройствам

Доступные данные:

- Версия - версия установленного ПО
- Имя
- Тип - определяется типом компоненты
- Модель - лицензия, заданная исходя из типа компоненты
- Дата создания - дата создания новой сущности в XDR
- Конец лицензии - дата окончания действия лицензии
- Свойства - теги определяющие активированные настройки компоненты

6.4.1.2. Фильтр

По кнопке фильтра в левом верхнем углу веб-интерфейса открывается меню фильтрации.

Параметры Статус и Свойства аддитивные - возможен выбор нескольких значений в рамках одного параметра. Доступные фильтры:

- Тип устройства
  - NTA
  - MDP
  - XDR
  - EDR
- Статус
  - Новый
  - Активен
  - В архиве
  - Выключен
  - Проблемы с подключением
  - Проблемы с производительностью
  - Проблемы с интеграцией
- Свойства

- MDP - указывает на интеграцию NTA с MDP для поведенческого анализа
- SPAN:FILES - указывает на попытку сенсора на сбор файлов из SPAN сессий для поведенческого анализа
- MAIL:SMTP - указывает на интеграция NTA с почтовым сервером по протоколу SMTP
- MAIL:SPAN - указывает на попытку сенсора на сбор почтовых сообщений из SPAN сессий
- MAIL:POP3 - указывает на интеграцию NTA с почтовым сервером по протоколу POP3
- MAIL:IMAP - указывает на интеграцию NTA с почтовым сервером по протоколу IMAP
- MAIL - указывает на включенный анализ почтовых сообщений в NTA

6.4.1.3. Добавить устройства

Для регистрации нового устройства нажмите кнопку **добавить устройство**

- Тип устройства - NTA / MDP
- Лицензия - от выбора типа лицензии зависит производительность зарегистрированного устройства
- Имя устройства
- Связанное железо(опционально) - связать с устройством из тех что ещё не зарегистрированы на XDR
- Комментарий

При нажатии на кнопку Создать Устройство диалоговое окно предложит ввести мастер пароль для получения уникального идентификатора(UID) создаваемого устройства.

Запросить Подписание подписывает UUID нового устройства мастер-паролем.

Таким образом после создания устройства в интерфейсе XDR становится доступным ряд настроек и параметров новой сущности. Главным параметром является UUID (или **Номер лицензии**). UUID используется для активации нового

устройства и его синхронизации с XDR. Остальные настройки и параметры описываются в разделе Редактирования настроек соответствующего модуля.

При регистрации нового устройства необходимо различать создание устройства и "активация и подключение" к XDR:

- Создание устройства - это процесс создания новой сущности внутри web-интерфейса XDR, а также подписания UID мастер-паролем
- Активация и подключение устройства к XDR - это процесс настройки на NTA/MDP - его активации и подключения к XDR.

6.4.2. Редактирование настроек XDR

Общая информация

- Номер лицензии - получен при покупке или тестировании решения
- Комментарий
- VPN IP - адрес VPN сервера для коммуникации XDR с подключаемыми модулями
- Внешний IP - адрес управляющего интерфейса

Состояние устройства

- Последний HeartBeat
- CPU / RAM / HDD

Графики состояния устройства

- CPU average (%)
- RAM maximum (%)
- HDD maximum (%)

Общие показатели XDR

По кнопке **Редактировать Настройки** доступны расширенные настройки:

- Обновления и потоки данных
- Прокси-сервер
- Сервер времени

- Сертификат web-сервера
- Настройки почтового сервера
- Сервер событий EDR

6.4.2.1. Обновления и потоки данных

Данная настройка предоставляет режимы работы XDR определяющие принцип взаимодействия с серверами и сервисами АО «Будущее». Настройка определяет типы данных которыми будут обмениваться инфраструктура клиента с инфраструктурой АО «Будущее». Возможно задать как полностью закрытую инсталляцию, так и полностью открытую.

Описание режимов:

- Не обновлять систему

Данный режим подразумевает полностью закрытую инсталляцию. XDR никак не взаимодействует с серверами АО «Будущее».

Обновление программного обеспечения, IOC и сетевых сигнатур не производится.

- Получать только обновление ПО и правил

Данный режим позволяет оборудованию получать обновления ПО для XDR и всех подключённых к нему устройств.

Обновление индикаторов и сигнатур не производится.

В данном режиме нет возможности загружать данные по инфраструктуре атакующих и отсутствует взаимодействие с SOC АО «Будущее» для получения поддержки по инцидентам в режиме 24/7.

Обновления доставляются с сервера АО «Будущее» - 92.53.76.98:443/tcp

- Обновления + одностороннее получение TI

Данный режим дополняет предыдущий и позволяет получать обновление индикаторов атак и сигнатур для подключённых к XDR устройств.

В данном режиме невозможно получать мониторинг и поддержку от CERT (SOC АО «Будущее»).

В данном режиме имеется возможность загружать данные по инфраструктуре атакующих вручную.

Для получения данных по инфраструктуре атакующих XDR необходим доступ до сервера - 443/tcp

- Обновление + Threat Hunting

Данный режим дополняет предыдущий и позволяет выгружать данные об обнаруженных инцидентах в сервера АО «Будущее».

Имеется возможность автоматически получать информацию по инфраструктуре атакующих.

В данном режиме имеется возможность мониторинга и поддержки от CERT АО «Будущее» в режиме 24/7.

Для получения данных по инфраструктуре преступников и связи с SOC АО «Будущее», а также для получения обновлений - 443/tcp

6.4.2.2. Прокси-сервер

Для работы XDR во всех режимах исключая первый (Не обновлять систему) системе необходима связь с серверами АО «Будущее». Данное подключение может осуществляться через прокси сервера. Доступные настройки:

- Адрес сервера - IP адрес прокси
- Порт
- Тип авторизации - поддерживается базовая и NTLM аутентификации. Так же возможно выбрать прокси без авторизации.
- Задайте логин и пароль при выборе базовой или NTLM аутентификации.

6.4.2.3. Сервер времени

В настройках сервера NTP возможно задать адрес сервера синхронизации времени для всех сенсоров, подключенных к данному XDR серверу. Все подключенные NTA и MDP синхронизируют своё время с XDR.

6.4.2.4. Сертификат web-сервера

Для доступа в веб-интерфейс возможно задать пользовательские SSL-сертификаты. Сертификат и ключ загружается в форматах .crt и .key

6.4.2.5. Настройки почтового сервера

Данная настройка задаёт почтовый сервер и аккаунт для рассылки сообщений для администраторов комплекса. Рассылка осуществляется индивидуально по сработанным инцидентам. Рассылка настраивается в соответствующих настройках аккаунта администратора в разделе Пользователи.

6.4.2.6. Сервер событий EDR

Сервер управления EDR.

Активирует сервер для агентов на конечных станциях с ОС Windows, следящих за системной активностью и отправляющих события на XDR для анализа и последующей реакции. Является решением типа endpoint detection and response.

6.4.3. Редактирование настроек NTA

На странице представлены общие показатели по работе подключенного NTA. Данные по каждому сенсору доступны при раскрытии карты сенсора в списке подключённых устройств.

Общая информация

- Номер лицензии - получен при покупке или тестировании решения
- Комментарий
- VPN IP - адрес внутри VPN туннеля, получаемый при подключении NTA к XDR для управляющих коммуникаций
- Внешний IP - адрес управляющего интерфейса, выданный на стороне клиента (через DHCP или статическими правилами)

Состояние устройства

- Последний HeartBeat - последний замеченный heartbeat с данного устройства

- Последняя активность - крайнее время активности VPN между сенсором и управляющим XDR
- Длительность - временной отрезок в течении, которого между сенсором и XDR был установлен управляющий VPN канал. Отчитывается с момента последней потери связи между устройствами
- CPU / RAM / HDD
- Загрузка канала
- Дропы в ядре / на интерфейсе

Графики состояния устройства

Предоставляют двумерный график на временном отрезке в 24 часа по следующим показателям:

- Производительность - задействованные ресурсы системы
  - CPU average (%)
  - RAM maximum (%)
  - HDD maximum (%)
- SPAN - средняя загрузка канала приёма копии трафика, аккумулированная по всем SPAN интерфейсам сенсора
- MSP - статистика по количеству принятых для анализа почтовых сообщений при наличии почтовой интеграции
  - Envelopers - статистика по принятым письмам
  - Files - статистика файлов, приложенных к данному количеству писем
  - MDP Queue - размер очереди на MDP к выбранному моменту времени
- DROPS - отбрасываемые пакеты на физическом интерфейсе приёма копии трафика

6.4.3.1. Интеграция с MDP

Данная настройка предлагает возможность интегрировать выбранный NTA с определенным MDP для осуществления функций поведенческого анализа.

- Интеграции

В меню задаётся запись в виде доменного имени или IP адреса MDP. Возможно задать больше чем одну запись, дабы обеспечить распределение

нагрузки по поведенческому анализу. Управление очередью производится на стороне сенсора. Сенсор делает опрос всех подключённых к нему MDP на предмет размера очереди поведенческого анализа и выбирает минимальную для следующего анализа.

- Язык анализа

Задаёт использование определённых образов операционных систем внутри подключённых MDP. Данные операционные системы будут настроены для поддержания защиты от актуальных угроз в регионах с выбранной языковой системой (По умолчанию поддерживаются Русский и Английский языки).

Использование облачного MDP

Для использования MDP Cloud (облачной версии MDP) используется следующая запись:

http://command-server.tds/MDP_cloud

6.4.3.2. Почтовый сервер

Настройка позволяет задать основной способ интеграции приёма почтовых сообщений.

Глубина хранения писем (дни)

Вне зависимости от выбора способа интеграции необходимо задать параметр глубины хранения.

Он определяет время в сутках в течении которого почтовые сообщения будут храниться на NTA для ретроспективного анализа почтовых сообщений и вложений в них.

6.4.3.2.1. Приём копии сообщений по SMTP

В данном режиме сенсор не будет являться точкой пересылки почтовых сообщений. И будет ожидать приёма копии почтовых сообщений от почтовых серверов клиента. Режим анализирует почтовый поток клиента, принимаемый по протоколу SMTP.

6.4.3.2.2. MTA режим

В данном режиме сенсор будет являться частью почтовой системы во внедряемой инфраструктуре. И будет анализировать реальный почтовый поток клиента.

Доступные настройки:

- Блокировать

При активации блокирует письма с подозрением на целевую атаку и отправляет их в карантин сенсора. Таким образом возможно интегрировать XDR в почтовую систему в режиме MTA как с блокировкой (для обеспечения превентивной защиты от целевых атак), так и без (для обеспечения бесперебойности бизнес-процессов в случае false-postivie срабатываний). Примечание: в случае использования режима работы с блокировкой, оповещения от SOC АО «Будущее» не будут производиться при успешном блокировании письма содержащего вредоносный контент. Управление карантином осуществляется в подразделе раздела Расследования - Письма -> Управление карантином

- Почтовые маршруты

Позволяет задать маршрутизацию почтового трафика для следующих MTA или почтовых серверов. Таким образом возможно обеспечить приоритизацию дальнейшей пересылки почтовых сообщений, в случае наличия более одного приёмщика почтовых сообщений (MTA, EDGE, CAS).

- Таймаут проверки писем

Время удержания почтовых сообщений на сенсоре до отправки его следующему MTA или почтовому серверу в соответствии с настроенными почтовыми маршрутами. По умолчанию NTA ограничивает передачу сообщений до получения вердикта от NTA и MDP. Таймаут ограничивает сверху время затрачиваемое на данный процесс. Таким образом, в случае если почтовое сообщение не было проверено по истечению заданного таймаута, оно будет отправлено по почтовому маршруту без решения по анализу и будет проанализировано в ретроспективе.

MTA интеграция

Требования к Inline интеграции

При реализации Inline-режима необходимо учитывать критерий отказоустойчивости, поэтому реализация выглядит следующим образом:

- Установка двух NTA, служащих для приема почты по протоколу SMTP.
- При помощи протокола VRRP NTAs делят один виртуальный адрес, на который поступает входящая почта.
- Один из NTA всегда находится в режиме Master (NTA, свободный от анализа сетевого трафика SPAN), второй NTA находится в режиме Backup (он же занят SPAN-трафиком).
- В случае выхода из строя основного NTA, резервный NTA в течении 2 секунд регистрирует проблему и переключается в MASTER-режим, забирая виртуальный IP-адрес себе и продолжая полноценную работу системы в части приёма почты.
- Выход из строя основного узла регистрируется в системном журнале, который передается в службу мониторинга команды CERT АО «БУДУЩЕЕ» и локально по сети через Syslog в систему учета логов заказчика.

Каждое устройство должно иметь доступ к XDR, для чего должен быть доступен следующий адрес:

IP_address _XDR:1443/udp

Система реализует гарантированную доставку писем в течении настраиваемого времени (по умолчанию 5 минут), жестко ограничивая время анализа сверху. Если из-за образовавшейся очереди на анализ проверка писем начинает занимать больше установленного порога времени, осуществляется прямая доставка писем. При этом анализ будет завершен в любом случае.

Перед переключением входящего почтового сервера на NTA необходимо проверить работу цепочки доставки писем. Для этого рекомендуется использовать скрипт, который предоставляют специалисты отдела внедрения АО «Будущее».

6.4.3.3. Почтовый клиент

Настройка почтового клиента позволяет NTA подключаться к почтовым серверам, хранящим клиентские письма и анализировать содержимое почтового ящика. Обратите внимание, сенсор подключается только к одному ящику почтового сервера - на данный ящик необходимо направлять копии почтовых сообщений для анализа (Организуется через внутренние BCC функции почтовых серверов или почтовых сервисов). Дополнительную информация по режиму работы возможно почерпнуть по ссылке Интеграция по POP3/IMAP.

Доступные настройки:

- Почтовый сервер

FQDN или сетевой адрес почтового сервера, к которому будет подключаться сенсор по протоколу POP3/IMAP.

- Порт

Задаётся в случае использования нестандартных портов на сервере клиента.

- Имя пользователя

Логин от почтового ящика, на котором агрегируется копии почтовых сообщений для анализа.

- Пароль

Пароль от почтового ящика

- Протокол

Внимание! задавая тип протоколов, необходимо иметь ввиду особенности работы данных протоколов относительно хранимой на почтовом ящике корреспонденции. Подробнее ниже.

Поддерживаемые протоколы:

- POP3

При использовании данного протокола, вся проанализированная почта будет автоматически удаляться сенсором после скачивания почтовых сообщений из ящика. Почта удаляется безвозвратно, только при наличии достаточных прав у используемого сенсором аккаунта.

- IMAP

При использовании протокола, используются стандартные команды протокола на удаление закаченных из ящика почтовых сообщений.

- Шифрование

Поддерживаемые версии протоколов шифрования SSLv2, SSLv3, TLS, TLSv1, TLSv1.1, TLSv1.2. Дополнительная информация по поддержке протоколов со стороны клиентов доступна по запросу к специалистам АО «Будущее».

- Пауза между подключениями

Таймаут между подключением к почтовому ящику для скачивания почтовых сообщений. По умолчанию NTA запрашивает с почтового сервера первые 100 доступных сообщений (вне зависимости от выбранного протокола). Таким образом, если почтовый сервер не корректно обрабатывает команды на удаление от сенсора, возникнет петля.

- Папка

Доступно при выборе протокола IMAP. Задаёт имя папки в подключаемом почтовом ящике для скачивания сообщений.

6.4.3.4. Стратегия работы со ссылками

При интеграции с почтовой системой сенсор будет осуществлять анализ почтовых сообщений на предмет содержания в нём ссылок на внешние ресурсы. При обнаружении ссылок NTA будет производить переходы по данным ссылкам. Переход по ссылке ограничивается только ресурсом, указанным в ссылке и не производит дальнейшее изучение ресурсы на предмет ссылок. Поэтому необходимо выбрать стратегию работы со ссылками.

Предлагаемые стратегии:

- Консервативная

Анализируются только ссылки, однозначно ведущие на потенциально-вредоносный контент, например, http://malwaresite.ru/a.exe. Ссылки, не имеющие таких явных признаков, пропускаются.

- Сбалансированная

Под анализ попадает значительно больше ссылок, выбираемых по специальному алгоритму. Не попадают на анализ ссылки на популярные домены и сервисы, потенциально изменяющие состояние ссылки. Этот режим работы требует настройки локального white-листа для ссылок.

- Агрессивная

Анализируются все ссылки, за вычетом локального white-листа. Режим может провоцировать изменение состояния определенных ссылок и повышенное число выполняемых анализов.

6.4.3.5. ICAP сервер

NTA может взаимодействовать по протоколу ICAP в качестве сервера с сетевым оборудованием поддерживающий данный протокол в качестве клиентов. Например: Web Proxy, UTM, NGFW, и т.п. При таком взаимодействии ICAP сервер в пассивном режиме ожидает подключение клиентов. ICAP-клиент передает файлы для проведения поведенческого анализа с ожиданием вердикта, либо без ожидания (в зависимости от настройки блокировки). Доступные настройки:

- TCP-порт

Порт для подключения ICAP-клиентов. На данном порту будет работать сервис ICAP-сервера.

- Блокировать скачиваемые вредоносные файлы

Позволяет активировать режим блокировки для ICAP-клиентов. В данном режиме ICAP-клиенты ожидают от NTA ответа по вердикту для файла по итогам поведенческого анализа на MDP. В случае, если файл вредоносный, NTA присылает ICAP-клиенту команду на блокировку проанализированного файла.

Примечание. В случае получения от ICAP-клиентов архивов или зашифрованных архивов, NTA разархивирует или попытается разархивировать шифрованный архив произведя подбор пароля по встроенному словарю. Дальнейший анализ будет производиться штатно.

6.4.3.6. Анализ файлов из трафика

При активации данной настройки сенсор будет пытаться получать файлы из анализируемой копии трафика и отправлять их на поведенческий анализ. При подобном способе интеграции необходимо учитывать следующие моменты:

- Дропы - если зеркалирующее устройство (с которого поступают SPAN сессии) будет дропать пакеты при формировании копии трафика, то высока вероятность невозможности собрать из SPAN сессий почтовых сообщений.

6.4.3.7. Анализ сетевого трафика

Важнейший раздел при настройке сигнатурного анализа. Данный раздел даёт системе понимание "инородного" трафика относительно легитимного. Позволяет указать локальные интерфейсы, а также интерфейсы для SPAN/RSAN/SPANinGR.

Укажите локальные адреса, принадлежащие сети, а также адреса локальных Proxy. Введите список локальных подсетей и исключите из них адреса Proxy-серверов (!proxy-ip). Это позволит отличить взаимодействие с внешними узлами.

6.4.3.8. Экспорт данных

По умолчанию логи работы NTA отправляются и хранятся в XDR и SOC АО «Будущее» (в зависимости от заданного режима работы XDR). Данная настройка позволяет дополнительно отправлять логи работы сенсора на внешние аналитические системы. Логи будут отправляться напрямую от NTA до указанных в настройке серверов. Для экспорта логов во внешние системы необходимо задать сетевой адрес, порт и протокол (UDP/TCP) сервера напротив выбранного формата. Возможно задать только один сервер для каждого доступного формата. Логи работы NTA формируются в формате syslog и затем упаковываются в указанные ниже форматы. Таким образом возможна интеграция с любой аналитической системой, которая может обрабатывать стандартный формат syslog. Доступные форматы:

- CEF

CEF (нативный для SIEM ArcSight), с уровнями угроз Low (1-2), Medium (3), High (4) и Very-High (5).

- JSON

json, с уровнем угрозы (severity) от 1 до 5.

6.4.3.9. Сервер времени NTA

По умолчанию каждый сенсор синхронизирует время с XDR, но это поведение можно изменить, указав произвольный NTP-сервер. Для того чтобы добавить новый произвольный NTP-сервер, необходимо нажать на кнопку **Добавить запись** и внести адрес NTP-сервера в формате FQDN или сетевой IP-адрес.

6.4.3.10. Белый список

Белые списки позволяют исключить из анализа внесенные в них объекты в компонентах NTA и MDP. Оптимизация работы решения с помощью данного инструмента - обязательное условие высоко качества обнаружения атак.

6.4.3.10.1. IP блоки

Позволяет исключать потоки данных на сетевом уровне в различных направлениях (от и/или к целевым,защищаемым, хостам).

В первую очередь необходимо задать направление для фильтрации:

- SRC - Источник.
- DST - Назначение.
- ANY - Источник и Назначение.

Далее необходимо ввести IP-адрес. Система поддерживает IPv4 и IPv6. В ближайшем будущем появится возможность вводить целые подсети.

6.4.3.10.2. Почты

Фильтрация почты может позволить значительно уменьшить нагрузку на MDP. В первую очередь необходимо задать направление для фильтрации:

- TO - адрес назначения.

- FROM - адрес отправителя.
- ANY - адрес назначения и отправителя.

Система поддерживает ввод, как единичных аккаунтов, так и целых доменов. Например, можно добавить в whitelist один аккаунт или все почтовые аккаунты в домене с помощью регулярных выражений.

6.4.3.10.3. Хеши файлов

Система поддерживает фильтрацию файлов в следующих форматах:

- MD5
- SHA1
- SHA256

Например, выбрав алгоритм хеширования: MD5 и хеш-сумму файла: d0b28c012c1276a92d787412bf2dd9dc данный файл будет включен в whitelist и не будет анализироваться песочницей.

6.4.3.10.4. Домены и URL-ы

Указанные в данном списке домены и URL будут опускаться при анализе сенсором подозрительных ссылок в почтовых сообщениях и сетевом трафике. В каждой записи необходимо задать:

- Domain - общий домен необходимого уровня
- URL mask - регулярное выражение для анализа ссылок из указанного домена

6.4.3.11. Настройки разрешения имён

Данный раздел активирует возможности сенсора по разрешению сетевых адресов в доменные и сетевые имена. Таким образом, аналитикам предоставляется удобный инструмент для быстрого определения принадлежности хостов к обнаруженным инцидентам и тем самым сокращается время реагирования.

DNS-сервера для PTR запросов

Настройка позволяет изменить стандартные маршруты по выполнению PTR (reverse DNS) запросов и позволяет задать статические маршруты для выполнения

подобных запросов. Чтобы настроить нестандартные маршруты PTR-запросов заполните записи в формате:

- Сеть

Подсеть/сеть/IP адрес. - Настройка задаёт подсеть/сеть/адрес для которых необходимо разрешать IP адреса в доменные имена.

- DNS-сервер

Настройка задаёт сервер, который будет отвечать за обслуживание PTR запросов для указанных подсетей/сетей/адресов.

Использование mDNS

Активирует на сенсоре протокол mDNS и позволяет осуществлять мультикаст DNS запросы для разрешения адресов в доменные/сетевые имена.

Использование Netbios

Активирует на сенсоре использование протокола Netbios для определения сетевых имён хостов.

6.4.4. PKI

В данном меню предоставляется список всех UUID (сертификатов) созданных с момента активации XDR.

6.4.4.1. Данные по сертификатам

По каждому сертификату доступна следующая информация:

- Серийный номер

UUID сертификата.

- Устройство

Имя, выданное при создании и генерации сертификата для нового устройства.

- Имя лицензии

Тип лицензии. Зависит от типа устройства.

- Статус
    - Reserved - сертификат создан, подписан. По нему зарегистрирован модуль. Сертификат используется в работе
    - Signed - сертификат создан (подписан), но ещё не используется. По нему возможно зарегистрировать новый модуль на XDR
    - Revoked - сертификат отозван. Связанное с ним устройство отсоединено от XDR без возможности дальнейшей работы
    - Requested - запрос на отзыв сертификат со стороны подключенных модулей. Модуль будет работать до те пор пока сертификат не будет отозван - перейдёт в статус revoked
- Подписан

Дата выпуска сертификата на XDR

- Последнее изменение

Дата последнего изменения статуса сертификата.

6.4.4.2. Изменение сертификатов

При выборе одного или нескольких сертификатов появляется возможность изменить статус сертификата:

- Подписать

Подписать зарезервированный сертификат

- Отозвать

Отозвать подписанный сертификат. Модуль, зарегистрированный на XDR по данному сертификату, будет отсоединён.

- Удалить

Удалить сертификат.

6.4.4.3. Фильтры

По кнопке фильтров в левом верхнем углу веб-интерфейса открывается меню фильтрации.

Доступные фильтры:

- Статус
    - Requested
    - Signed
    - Reserved
    - Revoked

6.4.5. Пользователи

Данная страница содержит информацию о пользователях, зарегистрированных в системе XDR, а также позволяет добавлять/удалять пользователей и вносить изменения в профили. В списке пользователей представлена общая информация по каждой записи. По каждому пользователю доступна полная информация.

6.4.5.1. Полная информация по пользователю

Информация о пользователе

- Имя - Имя и Фамилия пользователя.
- Роли - функция для определения прав доступа к ресурсам и управления этим доступом.
    - Owner - создатель проекта. Пользователь имеет права на выполнение любых действий.
    - Admin - привилегированный пользователь, имеющий права, включающие изменение прав доступа к продукту XDR для других пользователей, регистрация и удаление пользователей, изменение ролей пользователей. В одной организации может быть несколько администраторов.
    - Analyst - аналитик по реагированию и мониторингу на инциденты.

    - User - пользователь системы XDR обладающий правами доступа стандартного пользователя. Ему доступны: Dashboard, Алерты, Расследование.
    - Manager - имеет минимальные права доступа: Dashboard, Алерты.
- Почта - email-адрес пользователя. Используется как логин при аутентификации. Данный адрес будет использоваться для оповещений от SOC АО «Будущее» по инцидентам при наличии поддержки 24/7. А так же будет использоваться XDR для автоматической рассылкой сообщений о статусах алертов.
- Последняя активность - представлены крайние записи активности из пункта История событий.
- Белый список IP - В качестве более высокого уровня безопасности учетной записи, рекомендуется добавление белого списка IP адресов. Данный список позволит обеспечить доступ к учетной записи только по представленным IP адресам, для этого необходимо указать один IP адрес или его диапазон.
- Уведомления - используется два типа уведомлений:
    - Почта - оповещение пользователя о созданном тикете в системе XDR. Используется почта из соответствующего раздела
    - Телефон - при происшествии критических инцидентов специалисты SOC АО «Будущее» дополнительно оповестят пользователя телефонным звонком.

Компании

Наименование организации к которой относится пользователь. Компания определяет область видимости информации для аккаунта. Дополнительная информация содержится в разделе Компании.

История событий

Данный модуль позволяет вести логирование действий пользователя

6.4.5.2. Добавить пользователя

Для добавления нового пользователя в систему XDR необходимо провести регистрацию. Пользователю с ролью admin или owner требуется зайти на страницу "Настройки" и нажать на "Добавить пользователя". Следующие поля обязательны

к заполнению: Имя, Фамилия, Пароль, Повтор пароля, Компания, Почта, Язык интерфейса, Часовой пояс и Роль. Поля необязательные к заполнению: Телефон, Белый список IP и Уведомления.

Создание пользователя

6.4.5.3. Удаление пользователя

Для обеспечения более высокого уровня безопасности архитектуры клиента, при удалении пользователя учетная запись архивируется. Тем самым все внесенные записи, настройки сохраняются. Для удаления пользователя необходимо выбрать учетную запись и нажать "Удалить".

6.4.5.4. Фильтры

Для фильтрации данных на странице "Пользователи" существует два фильтра:

- Роль пользователя - позволяет сортировать информацию о пользователях исходя из выбранной роли.
- Состояние пользователя - сортирование информации об активных или удаленных пользователях.

6.4.6. Компании

XDR даёт возможность создавать несколько компаний в разрезе одной инсталляции, что позволяет разграничивать доступные данные среди пользователей, а также реализовывать более сложные иерархические структурные разграничения прав доступа. Все подключаемые модули (NTA, MDP, EDR) соотносятся с сущностью Компания из числа созданных в настоящем разделе. Таким образом, все события, формируемые данными модулями, будут разграничены по доступу в соответствии с принадлежностью модуля к Компании.

6.4.6.1. Общий список компаний

Предоставляет список компаний с описанием общих данных по ним.

Доступны следующие данные:

- Имя компании

- Менеджеры - список пользователей с ролью менеджер
- Устройства - количество прикрепленного к данной компании оборудования с разделением по типам
- Дата создания - дата создания компании
- Дата подписки - дата начала подписки

6.4.6.2. Информация о компании

При выборе компании доступной в списке открывается полная информация о компании. В левом верхнем углу будет отображаться заданный при создании компании логотип. Общие данные можно отредактировать по кнопке **Изменить** в правом верхнем углу.

Устройства

Предоставляет список устройств, привязанных к выбранной компании. Краткая информация:

- Название - имя устройства
- Тип - тип компоненты системы (NTA, MDP, EDR)
- UUID - идентификатор ключа активации
- Последняя активность - крайняя дата активности системы

Пользователи

Список пользователей, привязанных к компании. Предоставляется следующая информация по пользователям:

- Имя - имя пользователя в системе
- Роль - присвоенная пользователю роль
- Последняя активность - крайняя дата активности пользователя

6.4.6.3. Добавление новой компании

Для добавления новой компании нажмите на кнопку **Добавить компанию** и заполните следующие поля:

- Имя компании - уникальное название компании в рамках XDR (поле обязательное к заполнению)

- Язык - выберете язык интерфейса по умолчанию
- Часовой пояс - задайте часовой пояс по умолчанию
- Логотип - имеется возможность задать нестандартный логотип компании (Будет отображаться в правом верхнем углу)

6.4.6.4. Архивирование компании

При архивировании компании ... Для архивирования компании выберите её в списке компаний, раскройте полное описание и нажмите кнопку **Архивировать**.

6.4.6.5. Фильтры

Фильтры типов

По кнопке фильтров в левом верхнем углу веб-интерфейса открывается меню фильтрации.

Фильтры компании

Доступные фильтры компании:

- Состояние компании - выбор компаний в состоянии:
  - Активные - отображать только активные
  - Архивные - отображать только архивные
  - Пусто - отображать полный список компании
- Имя компании
- Имя пользователя