Программное обеспечение

«F.A.C.C.T. Storage»

Руководство по установке и эксплуатации

Оглавление

Аннотация

Настоящий документ содержит руководство администратора по встраиванию программного комплекса «MXDR» (далее – ПО) в защищаемую инфраструктуру.

1. Назначение ПО

ПО – комплексное решение предназначено для выявления современных высокотехнологичных атак на ранней стадии, обеспечения процесса threat hunting, оптимизации процессов реагирования на инциденты и их последующего расследования внутри как корпоративной, так и технологической инфраструктуры. Оно определяет заражения, которые пропускают стандартные средства защиты: антивирусы, межсетевые экраны, системы предотвращения вторжений. Применение MXDR существенно снижает риски организации, помогая вовремя выявить и предотвратить хищения, финансовые мошенничества, попытки шпионажа, утечку конфиденциальной информации и другие инциденты.

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. Программно-аппаратные среды функционирования ПО

ПО функционирует в следующих программно-аппаратных средах:

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

Таблица 2.1 – Технические требования для NTA

NTA (нагрузка Mbps)	250	1000	2000	5000	10000
CPU	3,8 GHz, 6 C (2 threads per core), 12 MB	3,8 GHz, 6 C (2 threads per core), 12 MB	2,1 GHz, 6 C (2 threads per core), 12 MB	2,1 GHz, 20 C (2 threads per core), 27.5 MB	2,1 GHz, 20 C (2 threads per core), 27.5 MB
RAM, GB	32 GB, DDR 4	32 GB, DDR 4	64 GB, RDIMM	64 GB, RDIMM	128 GB, RDIMM
HDD, GB	2 x 1200	2 x 1200	2 x 1200	2 x 1200	2 x 1200

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

Таблица 2.2 – Технические требования для Sensor Industrial

Sensor Industrial (нагрузка Mbps)	**500**	**1000**	**2000**
CPU	4 GHz, 6 C, (2 threads per core), 12 MB	4 GHz, 6 C, (2 threads per core), 12 MB	2.1 GHz, 20 C, (2 threads per core), 27.5 MB
RAM, GB	32 GB, DDR 4	32 GB, DDR 4	64 GB, RDIMM
HDD, GB	2 x 1200	2 x 1200	2 x 1200
Network			
mgmt Ethernet	1	1	1
Span	до 4 Ethernet	до 4 Ethernet or SFP	до 4 SFP/SFP+

Таблица 2.3 – Технические требования для XDR Console

XDR Console	**Enterprise**	**Performance**	**Storage**
CPU	2.1 GHz, 20 C (2 threads per core), 27.5 MB	2.1 GHz, 20 C (2 threads per core), 27.5 MB	3.8 GHz, 6 C (2 threads per core), 12 MB
RAM, GB	128 GB, RDIMM	256 GB, RDIMM	64 GB, RDIMM
HDD, GB**	4 x 1,2Тбайт, 10000 об/мин, SAS 12 Гбит/с	4 x 1,2Тбайт, 10000 об/мин, SAS 12 Гбит/с	4 x 1,2Тбайт, 10000 об/мин, SAS 12 Гбит/с
Network			
Mgmt Ethernet	1 Ethernet	1 Ethernet	1 Ethernet

Таблица 2.4 – Технические требования для MDP

MDP	**Standard**	**Enterprise**
CPU	2.1 GHz, 20 C (2 threads per core), 27.5 MB	2.1 GHz, 40 C (2 threads per core), 27.5 MB
RAM, GB	128 GB, RDIMM	256 GB, RDIMM

SSD, GB**	2 x 480	2 x 480
Mgmt Ethernet	1 Ethernet	1 Ethernet

Таблица 2.5 – Технические требования для EDR

Операционная система	**Windows 7**	**Windows 8/8.1**	**Windows 10**
CPU	Не ниже Inter Core i3 второго поколения или аналогичный	Не ниже Intel Core i3 второго поколения или аналогичный	Не ниже Intel Core i3 второго поколения или аналогичный
RAM, GB	не менее 4 GB	не менее 4 GB	не менее 4 GB
HDD, MB	100	100	100
Жесткий диск	Не менее 60Gb, со скоростью не ниже 7200RPM	Не менее 60Gb, со скоростью не ниже 7200RPM	Не менее 60Gb, со скоростью не ниже 7200RPM
Network			
	Связь с XDR Console	Связь с XDR Console	Связь с XDR Console

Таблица 2.6 – Технические требования для Storage

Storage	
CPU	3.8 GHz, 6 C (2 threads per core), 12 MB
RAM, GB	64 GB, RDIMM
HDD, GB**	4 x 1,2Тбайт, 10000 об/мин, SAS 12 Гбит/с
Network	
Mgmt Ethernet	1 Ethernet

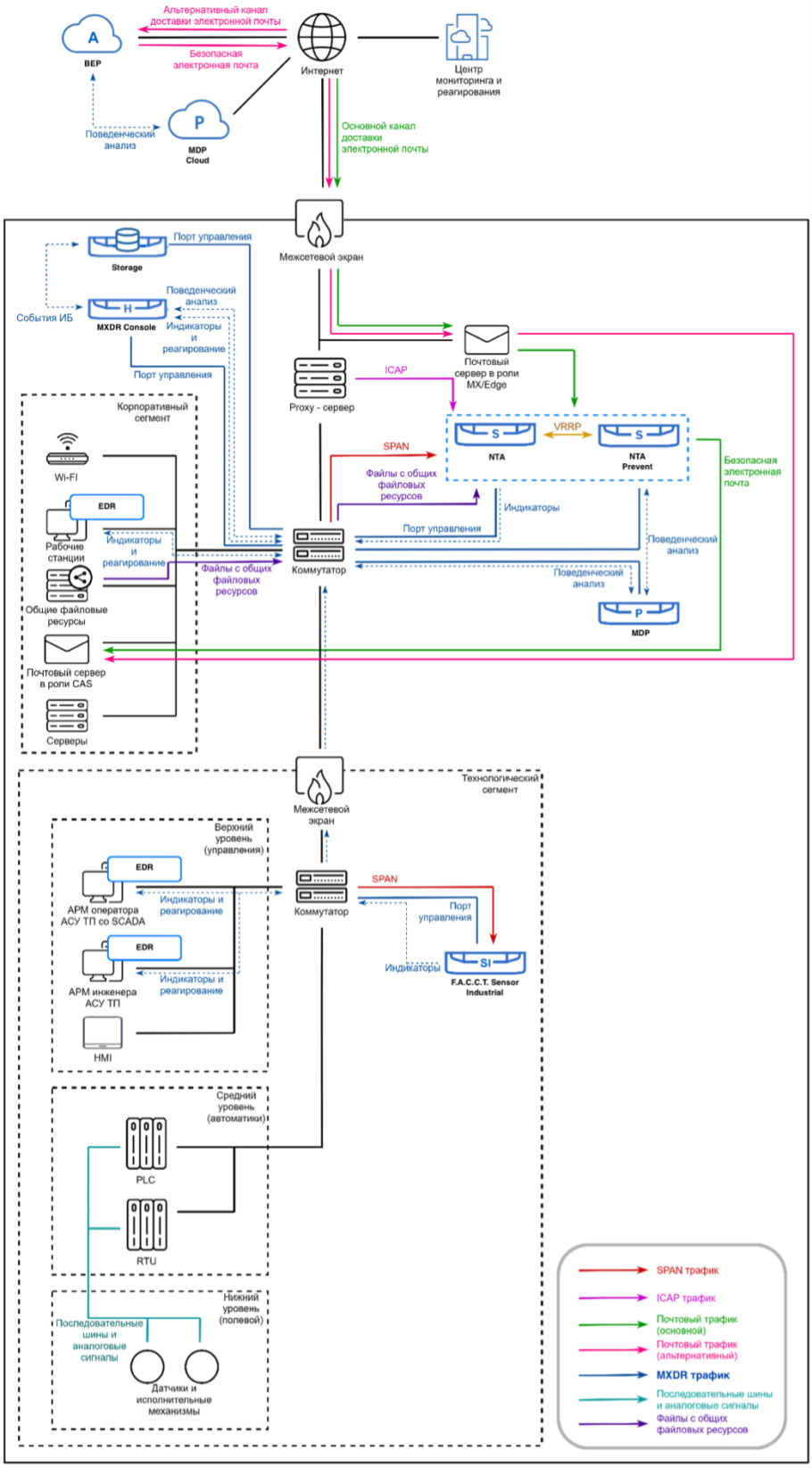
Таблица 2.7 – Технические требования для BEP

BEP	**Standard**	**Enterprise**
CPU	2.1 GHz, 20 C (2 threads per core), 27.5 MB	2.1 GHz, 40 C (2 threads per core), 27.5 MB
RAM, GB	128 GB, RDIMM	256 GB, RDIMM
SSD, GB**	2 x 480	2 x 480
Mgmt Ethernet	1 Ethernet	1 Ethernet

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.

4. Общие принципы функционирования ПО



XDR Console – набор инструментов, необходимых для команд мониторинга, реагирования на инциденты и проведения компьютерных расследований в защищаемой инфраструктуре. Является системой управления всеми модулями решения.

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.

Sensor Industrial – решение, предназначенное для детектирования атак на ранних стадиях в технологическом сегменте предприятия. Анализируя пакеты данных технологического трафика собственными сигнатурами и поведенческими правилами Sensor Industrial позволяет выявлять передачу нелегитимных команд управления между уровнями АСУ ТП, обнаруживать использование служебных команд АСУ ТП с целью перепрошивки ПЛК, подмены программы управления, остановки технологических процессов, и других нарушений.

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.

EDR– программное обеспечение для обнаружения угроз на хосте, фиксации полной хронологии событий на системе, блокировки аномального поведения, изоляции хоста, сбора криминалистически значимых данных.

Storage – модуль, предназначенный для хранения данных. Позволяет оптимизировать распределение хранящихся данных из имеющегося набора.

BEP – программное обеспечение, предназначенное для сбора электронной почты для дальнейшего поведенческого анализа, а также для фильтрации потенциально вредоносных писем. Является облачным решением, управление и настройка осуществляется на стороне АО «БУДУЩЕЕ».

ПО – это комплексное решение, предназначенное для выявления целенаправленных атак и неизвестных угроз, обеспечения процесса threat hunting как внутри защищаемого периметра, так и за его пределами, реагирования на инциденты и их последующего расследования как в корпоративном, так и в технологическом сегментах защищаемой инфраструктуры.

5. Обязанности и функции администратора заказчика

В обязанности администратора входит следующее:

- Произвести встраивание ПО в защищаемую инфраструктуру;
- Поддерживать функционирование ПО

6. Порядок получения экземпляров ПО

Для получения экземпляра ПО, необходимо скачать образы экземпляров ПО с информационных ресурсов АО «БУДУЩЕЕ». Пароль для скачивания предоставляется АО «БУДУЩЕЕ» по запросу Заказчика.

7. 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» (далее - 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 Console с выбранным режимом работы в инфраструктуру заказчика;
- Встраивание NTA с учётом точек съёма трафика, почтовой интеграции, интеграции с файловыми хранилищами и с учётом установки XDR Console;
- Встраивание Sensor Industrial с учётом точек съёма трафика, почтовой интеграции, интеграции с файловыми хранилищами и с учётом установки XDR Console;
- Установка EDR на защищаемых хостах заказчика;
- Встраивание MDP с учётом установки NTA, Sensor Industrial, EDR, XDR Console;
- Обеспечение связности всех модулей с XDR Console;
- Определить перечень IP-подсетей заказчика, которые будут определены как защищаемые и ввести эти данные в ПО;
- Интеграция почтовой системы;
- Интеграция файлового хранилища.

7.1. Выбор схемы встраивания в инфраструктуру

Существует следующие критерии встраивания в инфраструктуру:

1. Почтовая интеграция:
    a. Интеграция POP3/IMAP
    b. Интеграция по SMTP
    c. Inline (MTA)
2. Сетевая интеграция:
    a. TAP
    b. SPAN
    c. RSPAN
    d. RSPAN трафик в GRE-туннеле
3. Файловая интеграция:
    a. ICAP
    b. Файловые хранилища
    c. Интеграция внешних источников с API XDR для проверки файлов
    d. Анализ файлов из трафика

7.1.1. Почтовая интеграция

Поддерживаются несколько различных способов получения писем для поведенческого анализа:

1. Анализ копии писем
    a. Получение писем по POP3/IMAP
    b. Получение писем по SMTP
2. Inline – анализ оригинальных писем в режиме MTA (Mail Transfer Agent).

7.1.1.1. 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.

7.1.1.2. 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.

7.1.1.3. 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.

7.1.2. Сетевая интеграция

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

- TAP
- SPAN
- RSPAN трафик
- 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.

7.1.3. Файловая интеграция

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

a. ICAP
b. Файловые хранилища
c. Интеграция внешних источников с API XDR для проверки файлов

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

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.

7.2. 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**

Обновление программного обеспечения, IOC-ов и сетевых сигнатур не производится.
Отсутствует взаимодействие с инфраструктурой АО «БУДУЩЕЕ» SOC.

- **Получать только обновления ПО и правил**

Обновления сигнатур и IOC, а также обновление ПО комплекса загружаются в автоматическом режиме с сервера АО «БУДУЩЕЕ» по защищенному каналу. В этом режиме отсутствует взаимодействие с инфраструктурой АО «БУДУЩЕЕ» SOC. В данном режиме обновления инициируются XDR Console.

- **Обновления + одностороннее получение TI**

Обновления сигнатур и ПО загружаются в автоматическом режиме. У пользователя имеется возможность по выбранному индикатору (IP-адрес, доменное имя и т.п.) запросить и получить обогащенный контекст из системы АО «БУДУЩЕЕ» Threat Intelligence. Обмен информацией происходит по защищенным каналам. Для XDR необходим доступ до серверов – gateway.mxdr.ru :443/tcp.

События ИБ и уведомления по ним в АО «БУДУЩЕЕ» SOC не передаются.

Существует возможность активации аккаунта удаленной технической поддержки **АО «БУДУЩЕЕ»**.

- **Обновления + Threat Hunting**

Система работает в полнофункциональном режиме.

Автоматически загружаются обновления сигнатур и ПО. XDR автоматически получает информацию из системы АО «БУДУЩЕЕ» Threat Intelligence, поэтому имеется возможность осуществлять Threat Hunting. События ИБ передаются в АО «БУДУЩЕЕ» SOC и пользователь системы может получать поддержку от экспертов АО «БУДУЩЕЕ» CERT в режиме 24/7. Все данные передаются по защищенным каналам.

Для XDR необходим доступ до серверов – gateway.mxdr.ru :443/tcp.
Существует возможность активации аккаунта удаленной технической поддержки **АО «БУДУЩЕЕ»**.

7.3. Определение точек съема 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.

7.4. Определение способа интеграции с почтовыми серверами заказчика

Доступные способы интеграции:

- BCC по POP3/IMAP
- BCC по SMTP
- Inline режим по 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.

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

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

Поддерживаемые протоколы подключения:

- WebDav;
- SMB;
- FTP;
- NFS.

7.6. Встраивание XDR Console

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» – gateway.mxdr.ru :443/tcp.

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

Образ XDR Console можно установить на физический сервер.

7.6.1. Установка XDR Console

Варианты установки образа

- С помощью физических интерфейсов (iDRAC, iLO).
- С использованием USB-накопителя в ОС Linux. Запись образа на носитель следует производить с помощью утилиты **dd.**
- С использованием USB-накопителя в ОС Windows. Запись образа на носитель следует производить с помощью программы Rufus версии 2.x (в ней необходимо будет выбрать "Create a bootable disk" -> "DD image").

Далее рассматриваются пункты меню и шаги, возникающие во время установки XDR:

При загрузке установщика вас приветствует меню Пункты меню:

- Launch Installation – запускает процесс установки на виртуальной машине или сервере
- Hardware Information (HDT) – предоставляет данные по серверу или виртуальной машине, на которой запущен установщик
- Reboot – перезагружает сервер
- Power Off – выключает сервер

При выборе пункта **Launch Installation** загружается меню по дальнейшим шагам установки

Пункты:

- Install – запускает процесс установки
- Reboot – перезагружает сервер
- Poweroff – выключает сервер
- Shell – загружает командную строку

При выборе пункта **Install** пользователю предлагается прочитать лицензионное соглашение на русском или английском языках

Нажав **I Agree**, пользователь получает возможность продолжить установку и выбрать диск для установки.

Дождитесь окончания процесса установки и процесса настройки файловой системы.

После перезагрузки загрузится командная строка XDR Console. Появится возможность перейти к настройке и активации решения.

7.6.2. Активация XDR Console

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

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-адрес>_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
- Серийный номер – номер, выданный при покупке или тестировании XDR
- (Опционально) – прокси-сервер в формате http(s)://user:password@proxyFQDN:port
- Примечание: для синхронизации времени в момент активации необходимо иметь доступ к pool.ntp.org:123/udp.

Шаг 3: Создание удостоверяющего центра

Создать CA – запускает процесс генерации мастер-пароля для дальнейшей настройки и добавления оборудования.

Сохраните Ваш мастер-пароль в надёжном месте – он будет использоваться при подключении компонентов NTA, MDP, EDR.

При нажатии на кнопку **Начать Пользоваться** – завершится процесс активации XDR Console.

7.6.3. Подключение к консоли XDR Console

Консоль XDR Console 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 Console

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 Console.

Для входа в главное меню выберите Enter the Shell.

Не забудьте изменить пароль по умолчанию!

После нажатия **<Enter the shell>** откроется окно с выбором опций.

7.6.4. Главное меню XDR Console

Пункты главного меню:

1. Show current network settings – просмотр и изменение настройки сети
2. Configure network;
3. Configure proxy;
4. Configure management interface;
5. Reactivation;
6. Back: вывод основной информации о статусе сервера. Эта информация также выводится при входе в систему.

7.6.5. Настройка сети XDR Console

Для просмотра и изменения настроек сети необходимо перейти в пункт главного меню консоли XDR Console.

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 АО «БУДУЩЕЕ». XDR Console позволяет настроить использование прокси-сервера для доступа к обновлению базы сигнатур и правил анализа трафика для всех компонент MXDR. 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 Console интерфейсов управляющий. Управляющий интерфейс будет использоваться всеми компонентами для работы с XDR Console.

Reactivation

7.7. Встраивание NTA

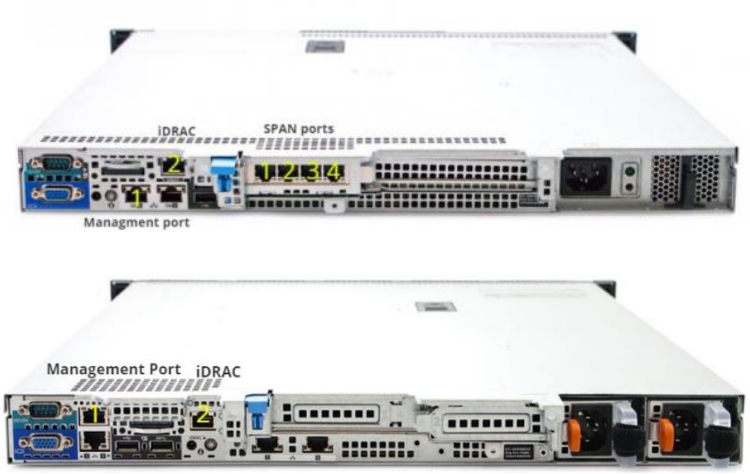
В базовой комплектации NTA имеет четыре сетевых интерфейса для приема трафика и один порт для подключения к сети и управления. Для обновления ПО и использования преимуществ облачного центра АО «БУДУЩЕЕ» SOC через порт управления NTA, в зависимости от выбранного типа инсталляции, должен быть доступен для подключения сетевой адрес:

- gateway.mxdr.ru :443/tcp – При использовании SOC АО «БУДУЩЕЕ»;
- IP адрес XDR Console:1443/udp – При использовании XDR Console.

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

7.7.1. Подключение к сети и захват трафика

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



Порт управления

Интерфейс №1 расположены на задней панели и используется для управления устройством и связи с АО «БУДУЩЕЕ» SOC / XDR Console, 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.

Захват трафика

Интерфейсы для захвата трафика расположены справа от порта управления и нумеруются от 1 до 4.

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.

MXDR захватывает зеркалированный трафик на уровне L2.

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

NTA 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.

iDRAC

На задних панелях серверов MXDR, правее от порта управления, расположены порты iDRAC. Данный интерфейс позволяет реализовать такие функции, как развертывание, обновление, мониторинг и обслуживание серверного оборудования.

7.7.2. Установка NTA

Для обновления ПО, проверки ссылок, отправки алертов и использования преимуществ XDR Console, необходимо обеспечить доступ к XDR Console через порт управления. При необходимости взаимодействие с XDR Console может осуществляться через прокси-сервер. В этом случае должен поддерживаться метод CONNECT для установления подключений на 443 порт.

Во время загрузки с образа будет предложено установить NTA. Здесь же можно просмотреть информацию об аппаратном обеспечении, перезапустить / выключить сервер или виртуальную машину.

В появившемся окне "Меню запуска установки" выберите **Install**.

На этом шаге можно выбрать один из двух языков, на котором выведется информация о лицензионном соглашении.

Чтобы ознакомиться с текстом лицензионного соглашения используйте клавиши **Page Up** и **Page Down**.

Далее необходимо выбрать устройство, на котором будет установлено ПО NTA.

Далее, начнется процесс установки NTA. В конце установки Вам будет предложено перезагрузить сервер или виртуальную машину.

Если все прошло успешно, откроется окно с приветственным экраном NTA.

7.7.3. Активация NTA и синхронизация с XDR Console

Активация NTA – включает функционал NTA.

Синхронизация NTA – привязывает NTA к XDR либо к XDR cloud, тем самым предоставляя возможность управления сенсором через обозначенные системы.

Перед активацией NTA на облачном или локальном XDR Console необходимо получение лицензионного ключа (UID). Воспользуйтесь одним из следующих вариантов:

1. При активации на XDR cloud обратитесь к менеджеру или технической поддержке АО «БУДУЩЕЕ»
2. При активации на локальном XDR используйте пункт меню "Добавить устройство".

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 NTA с BEP.

Активация и синхронизация осуществляется через консоль NTA.

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

После нажатия **<Enter the Shell>** пункт Activation в открывшемся меню 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:

- CA – on-cloud инсталляция. Оркестрация устройством осуществляется через SOC АО «БУДУЩЕЕ»;
- Private XDR Console – on-premise инсталляция. Оркестрация устройством осуществляется через XDR Console.

При выборе Private XDR Console необходимо задать доменное имя или IP-адрес XDR Console.

При выборе CA необходимо задать доменное имя или IP адрес SOC АО «БУДУЩЕЕ». (задано по умолчанию).

При работе с NTA 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 Console

При нажатии **OK** запускается процесс регистрации и синхронизации NTA с выбранным сервером.

Внимание: после данной операции мигрировать NTA с одной инфраструктуры на другую невозможно без вмешательства технической поддержки АО «БУДУЩЕЕ».

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

Панель инструментов в консоли NTA будет отображать XDR Connection со статусом OK.

Меню UI > Настройки > Устройства > *будет* отображать *в списке устройств информацию по состоянию подключенного устройства* NTA (

7.7.4. Подключение к консоли 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!

7.7.5. Главное меню 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.

При выборе кнопки **OK** откроется окно просмотра и изменения настройки сети.

7.7.6. Настройка сети NTA

Для просмотра и изменения настроек сети необходимо перейти в пункт главного меню консоли NTA.

Важно: если у Клиента используется локальный XDR (расположен непосредственно на площадке Клиента), то окно "Network menu" будет отображаться в следующем виде

Пункты меню настройки сети:

6. Show current network settings: вывод текущей настройки сетевого интерфейса управления.
1. Configure network: настройка сетевого интерфейса.
2. Configure proxy: настройки прокси для работы с SOC АО «БУДУЩЕЕ» / XDR Console.
3. Configure managment interface: настройки управляющего интерфейса.
4. Configure XDR connection
5. Traffic monitor Setup: меню для ввода пула адресов, принадлежащих внутренней сетевой инфраструктуре, а также для указания SPAN интерфейсов.
6. Reactivation
7. 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 АО «БУДУЩЕЕ» или локальному сервису XDR Console. NTA позволяет настроить использование прокси-сервера для доступа к обновлению базы сигнатур и правил анализа трафика, а также связи с облачным сервисом АО «БУДУЩЕЕ» или локальным сервисом XDR Console. 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 management interface

Предоставляет возможность задания управляющего интерфейса в NTA. Для задания выберите из списка интерфейсов нужный и нажмите "**Ок**".

Configure XDR connection

Позволяет задать IP адрес управляющего интерфейса XDR Console (в случаях использования локального XDR).

Traffic Monitor Setup

Позволяет указывать SPAN-интерфейсы.

Reactivation

Реактивация позволяет запустить процесс синхронизации с XDR (облачным или локальным) заново.

7.8. Встраивание Sensor Industrial

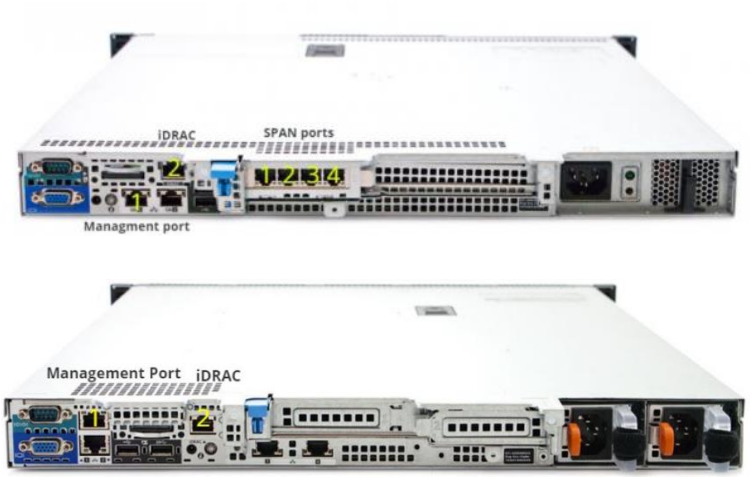
В базовой комплектации Sensor Industrial имеет четыре сетевых интерфейса для приема трафика и один порт для подключения к сети и управления. Для обновления ПО и использования преимуществ облачного центра АО «БУДУЩЕЕ» SOC через порт управления Sensor Industrial, в зависимости от выбранного типа инсталляции, должен быть доступен для подключения сетевой адрес:

- gateway.mxdr.ru :443/tcp – При использовании SOC АО «БУДУЩЕЕ»;
- IP адрес XDR Console:1443/udp – При использовании XDR Console.

При необходимости работа Sensor Industrial с АО «БУДУЩЕЕ» SOC / XDR Console может осуществляться через прокси-сервер. В этом случае должен поддерживаться метод CONNECT для установления подключений на 443 порт.

7.8.1. Подключение к сети и захват трафика

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



Порт управления

Интерфейс №1 расположены на задней панели и используется для управления устройством и связи с АО «БУДУЩЕЕ» SOC / XDR Console, 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.

Захват трафика

Интерфейсы для захвата трафика расположены справа от порта управления и нумеруются от 1 до 4.

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- трафиком.

MXDR захватывает зеркалированый трафик на уровне L2/

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

Sensor Industrial 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 MXDR 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.

iDRAC

На задних панелях серверов MXDR, правее от порта управления, расположены порты iDRAC. Данный интерфейс позволяет реализовать такие функции, как развертывание, обновление, мониторинг и обслуживание серверного оборудования.

7.8.2. Установка Sensor Industrial

Для обновления ПО, проверки ссылок, отправки алертов и использования преимуществ XDR Console, необходимо обеспечить доступ к XDR Console через порт управления. При необходимости взаимодействие с XDR Console может осуществляться через прокси-сервер. В этом случае должен поддерживаться метод CONNECT для установления подключений на 443 порт.

Во время загрузки с образа будет предложено установить Sensor Industrial. Здесь же можно просмотреть информацию об аппаратном обеспечении, перезапустить / выключить сервер или виртуальную машину.

В появившемся окне "Меню запуска установки" выберите **Install**.

На этом шаге можно выбрать один из двух языков, на котором выведется информация о лицензионном соглашении.

Чтобы ознакомиться с текстом лицензионного соглашения используйте клавиши **Page Up** и **Page Down**.

Далее необходимо выбрать устройство, на котором будет установлено ПО Sensor Industrial.

Далее, начнется процесс установки Sensor Industrial. В конце установки Вам будет предложено перезагрузить сервер или виртуальную машину.

Если все прошло успешно, откроется окно с приветственным экраном Sensor Industrial.

7.8.3. Активация Sensor Industrial и синхронизация с XDR Console

Активация Sensor Industrial – включает функционал Sensor Industrial.

Синхронизация Sensor Industrial – привязывает Sensor Industrial к XDR либо к XDR cloud, тем самым предоставляя возможность управления сенсором через обозначенные системы.

Перед активацией NTA на облачном или локальном XDR Console необходимо получение лицензионного ключа (UID). Воспользуйтесь одним из следующих вариантов:

3. При активации на XDR cloud обратитесь к менеджеру или технической поддержке АО «БУДУЩЕЕ».
4. При активации на локальном XDR используйте пункт меню "Добавить устройство".

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 Sensor Industrial с MDP.

Активация и синхронизация осуществляется через консоль NTA.

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

После нажатия **<Enter the Shell>** пункт Activation в открывшемся меню 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:

- CA – on-cloud инсталляция. Оркестрация устройством осуществляется через SOC АО «БУДУЩЕЕ»;
- Private XDR Console – on-premise инсталляция. Оркестрация устройством осуществляется через XDR Console.

При выборе Ptivate XDR Console необходимо задать доменное имя или IP-адрес XDR Console.

При выборе CA необходимо задать доменное имя или IP адрес SOC АО «БУДУЩЕЕ». (задано по умолчанию).

При работе с Sensor Industrial 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 Console.

При нажатии **OK** запускается процесс регистрации и синхронизации Sensor Industrial с выбранным сервером.

Внимание: после данной операции мигрировать Sensor Industrial с одной инфраструктуры на другую невозможно без вмешательства технической поддержки АО «БУДУЩЕЕ».

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

Панель инструментов в консоли Sensor Industrial будет отображать XDR Connection со статусом OK.

Меню UI > Настройки > Устройства > *будет* отображать *в списке устройств информацию по состоянию подключенного устройства* Sensor Industrial.

7.8.4. Подключение к консоли Sensor Industrial

Доступ к консоли Sensor Industrial 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!

7.8.5. Главное меню Sensor Industrial

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.

При выборе кнопки **OK** откроется окно просмотра и изменения настройки сети.

7.8.6. Настройка сети Sensor Industrial

Для просмотра и изменения настроек сети необходимо перейти в пункт главного меню консоли Sensor Industrial.

Важно: если у Клиента используется локальный XDR (расположен непосредственно на площадке Клиента), то окно "Network menu" будет отображаться в следующем виде

Пункты меню настройки сети:

1. Show current network settings: вывод текущей настройки сетевого интерфейса управления.
2. Configure network: настройка сетевого интерфейса.
3. Configure proxy: настройки прокси для работы с SOC АО «БУДУЩЕЕ» / XDR Console.
4. Configure managment interface: настройки управляющего интерфейса.
5. Configure XDR connection

6. Traffic monitor Setup: меню для ввода пула адресов, принадлежащих внутренней сетевой инфраструктуре, а также для указания SPAN интерфейсов.
7. Reactivation
8. 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 АО «БУДУЩЕЕ» или локальному сервису XDR Console. Sensor Industrial позволяет настроить использование прокси-сервера для доступа к обновлению базы сигнатур и правил анализа трафика, а также связи с облачным сервисом АО «БУДУЩЕЕ» или локальным сервисом XDR Console. 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 management interface

Предоставляет возможность задания управляющего интерфейса в Sensor Industrial. Для задания выберите из списка интерфейсов нужный и нажмите "**Ок**".

Configure XDR connection

Позволяет задать IP адрес управляющего интерфейса XDR Console (в случаях использования локального XDR Console).

Traffic Monitor Setup

Позволяет указывать SPAN-интерфейсы.

Reactivation

Реактивация позволяет запустить процесс синхронизации с XDR Console (облачным или локальным) заново.

7.9. Встраивание Storage

В базовой комплектации Storage поставляется в виде физического устройства. Стандартный Storage имеет формат 1U и монтируется в 19” стойку.

Storage это 1U сервер для хранения и корреляции событий и алертов в XDR, используется при увеличении объема и длительности хранения информации. Storage используется совместно с XDR.

Обновление ПО происходит через порт управления Storage, при этом должен быть доступен для подключения сетевой адрес:

- IP адрес XDR Console: 9200/tcp, 9300/tcp, 9220/tcp, 9320/tcp;
- gateway.mxdr.ru :443/tcp – При использовании 3,4-го режимов работы XDR.

7.9.1. Установка Storage

Варианты установки образа

- С помощью физических интерфейсов (iDRAC, iLO).
- С использованием USB-накопителя в ОС Linux. Запись образа на носитель следует производить с помощью утилиты **dd**
- С использованием USB-накопителя в ОС Windows. Запись образа на носитель следует производить с помощью программы Rufus версии 2.x (в ней необходимо будет выбрать "Create a bootable disk" -> "DD image").

Далее рассматриваются пункты меню и шаги, возникающие во время установки Storage:

.

Пункты меню:

- Launch Installation – запускает процесс установки на виртуальной машине или сервере
- Hardware Information (HDT) – предоставляет данные по серверу или виртуальной машине, на которой запущен установщик
- Reboot – перезагружает сервер
- Power Off – выключает сервер

При выборе пункта **Launch Installation** загружается меню по дальнейшим шагам установки.

Пункты:

- Install – запускает процесс установки
- Reboot – перезагружает сервер
- Poweroff – выключает сервер
- Shell – загружает командную строку

При выборе пункта **Install** пользователю предлагается прочитать лицензионное соглашение на русском или английском языках

Нажав **I Agree**, пользователь получает возможность продолжить установку и выбрать диск для установки.

Дождитесь окончания процесса установки и процесса настройки файловой системы

После перезагрузки загрузится командная строка Storage. Появится возможность перейти к настройке и активации решения.

7.9.2. Активация Storage и синхронизация с XDR Console

Синхронизация Storage – привязывает Storage к XDR, тем самым предоставляя возможность управления Storage через обозначенные системы.

Перед активацией Storage на локальном XDR Console необходимо получение лицензионного ключа (UID). Воспользуйтесь одним из следующих вариантов:

При активации на локальном XDR используйте пункт меню "Добавить устройство".

Для взаимодействия Storage с XDR необходимы следующие порты:

- 443/tcp – для первичной активации и привязки Storage (единоразово);
- 9200/tcp, 9300/tcp, 9220/tcp, 9320/tcp – для отправки данных с Storage к XDR Console.

Активация и синхронизация осуществляется через консоль Storage.

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

После нажатия **<Enter the Shell>** пункт Activation в открывшемся меню отвечает за активацию и синхронизацию.

Далее процесс активации Storage и синхронизация его с XDR Console будет аналогична процессу активации NTA и синхронизации его с XDR Console (см. пункт 5.7).

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

Панель инструментов в консоли Storage будет отображать License check со статусом **OK**.

Меню UI > Настройки > Устройства > *будет* отображать *в списке устройств информацию по состоянию подключенного устройства* Storage.

7.9.3. Подключение к консоли Storage

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 Storage. Для входа в главное меню выберите **<Enter the Shell>**.

Не забудьте изменить пароль по умолчанию!

7.9.4. Главное меню Storage

Пункты главного меню:

1. Show current network settings – просмотр и изменение настройки сети
2. Configure network
3. Configure proxy;
4. Configure management interface;
5. Reactivation;
6. Back: вывод основной информации о статусе сервера. Эта информация также выводится при входе в систему.

7.9.5. Настройка сети Storage

Для просмотра и изменения настроек сети необходимо перейти в пункт главного меню консоли Storage.

Важно: если у Клиента используется локальный XDR (расположен непосредственно на площадке Клиента), то окно "Network menu" будет отображаться в следующем виде

Пункты меню настройки сети:

1. Show current network settings: вывод текущей настройки сетевого интерфейса управления.
2. Configure network: настройка сетевого интерфейса.
3. Configure proxy: настройки прокси для работы с SOC АО «БУДУЩЕЕ» / XDR Console.
4. Configure managment interface: настройки управляющего интерфейса.
5. Configure XDR connection
6. Traffic monitor Setup: меню для ввода пула адресов, принадлежащих внутренней сетевой инфраструктуре, а также для указания SPAN интерфейсов.
7. Reactivation
8. 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 АО «БУДУЩЕЕ» или локальному сервису XDR Console. Storage позволяет настроить использование прокси-сервера для доступа к обновлению базы сигнатур и правил анализа трафика, а также связи с облачным сервисом АО «БУДУЩЕЕ» или локальным сервисом XDR Console. 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 management interface

Предоставляет возможность задания управляющего интерфейса в Storage. Для задания выберите из списка интерфейсов нужный и нажмите "**Ок**".

Configure XDR connection

Позволяет задать IP адрес управляющего интерфейса XDR Console (в случаях использования локального XDR).

Reactivation

Реактивация позволяет запустить процесс синхронизации с XDR заново.

7.10. Встраивание EDR

В данном разделе описаны способы установки агента EDR необходимого для фиксации хронологии поведения пользователя, выполнения программ на системе, а также сбора дополнительной контекстной информации для выявления вредоносного поведения на хосте.

Существуют три способа установки EDR:

- Установка и удаление EDR на OS Windows (вручную на хосте);
- Установка и удаление EDR (через GPO);
- Установка и удаление EDR (через EDR Installer).

7.10.1. Установка и удаление EDR на OS Windows (вручную на хосте)

Установка EDR

Перед началом установки EDR необходимо получить файл:

- gibep.msi

и конфигурационный файл с подписью:

- gibep_config.txt
- gibep_config.sign.txt

Эти файлы необходимо поместить в локальную директорию (например, в C:\EDR). Важно, что полный путь до директории не должен содержать кириллических символов и пробелов.

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

В случае возникновения проблем с установкой агента для анализа необходимо прислать лог, который создается командой выше.

Проверка установки EDR

Чтобы проверить наличие установленного EDR, необходимо запустить в командной строке cmd с правами Администратора:

"c:\Program Files\Group-IB\TDS Endpoint\gibepcli.exe" driver-version

sc queryex "gibtdsendpoint" | find "STATE"

TASKLIST | find "gibep"

При этом в реестре должны появиться ключи:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GIB*

Удаление EDR

Удаление EDR можно проводить через "Установка/ удаление программы".

Дополнительно

В случае возникновения проблем с деинсталляцией стандартным способом следует использовать утилиту:

- gibepremovaltool.msi.

Запускаем командную строку от Администратора и выполняем:

msiexec /i gibepremovaltool.msi /qn /L*V uninstall.log

Ожидайте завершения - должна вернуться ошибка. Перезагрузите хост. Ключи в реестре

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GIB* должны удалиться.

В случае возникновения проблем с удалением агента для анализа необходимо прислать лог, который создается командой выше и экспортированный ключ

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

Отладка EDR

В случае возникновения проблем с работой агента EDR на хосте необходимо прислать диагностические логи, которые находятся в директории:

C:\Program Files\Group-IB\TDS Endpoint\Logs.

Дополнительная диагностическая информация:

- При BSOD существует возможность включить на машине сборку дампов ядра https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/enabling-a-kernel-mode-dump-file, далее необходимо выбрать "Complete memory dump". Дамп соберется в C:\Windows\memory.dump, затем сожмите этот дамп в ZIP и пришлите его нам на анализ.
- При "жестких" зависаниях Windows существует возможность включить https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/forcing-a-system-crash-from-the-keyboard, чтобы генерировать BSOD нажатием "RightCtrl + Scroll" на клавиатуре. Тогда в момент зависания можно сгенерировать BSOD, после чего соберется дамп в C:\Windows\memory.dump, затем сожмите этот дамп в ZIP и пришлите его нам на анализ.
- При падениях сервиса EDR или других программ существует возможность включить сборку дампов юзер-спейс программ Windows https://docs.microsoft.com/en-us/windows/desktop/wer/collecting-user-mode-dumps, собранные дампы отправлять нам.
- Windows 10 уже содержит в себе WPR (Windows Performance Recorder) (C:\WINDOWS\System32\wpr.exe). Чтобы снять профиль производительности достаточно из командной строки cmd (от Администратора запустить):
  - WPR.exe -start CPU -start DiskIO -start FileIO -start Network;
  - Воспроизвести проблему с тормозами (вкладки, офис, сочетание Win+L);
  - WPR.exe -stop c:\Windows\Temp\perf.etl или другой путь (файл etl обычно несколько ГБайт);
  - Файл perf.etl отправить нам на анализ.
- Включить driver verifier для наших драйверов:
  verifier.exe /standard /driver gibepcore.sys gibepnetflt.sys gibepdevflt.sys.

7.10.2. Установка и удаление EDR (через GPO)

Установка EDR

Чтобы установить EDR через GPO необходимо выполнить следующие действия:

Шаг 1. Разместите установщик агента EDR, файл конфигурации и файл подписи в сетевой папке, доступной пользователю.

Шаг 2. Откройте консоль DPM, создайте политику на нужном уровне. В поле *Security filtering* уберите *Authenitificated Users* и добавьте у/з компьютеров или группы компьютеров, на которых требуется поставить агент. Нажмите **ПКМ** на политике и выберите **Edit**.

Шаг 3. По адресу Computer Configuration -> Polices -> Software settings найдите пункт *Software Installation*, нажмите на него **ПКМ** и выбираем **New** -> **Package**.

Шаг 4. В открывшемся окне откройте сетевую папку, в которую ранее положили установщик и выберите его.

Шаг 5. В открывшемся окне выберите **Assigned**

***Важно:** обратите внимание, что ветка политики *Computer Management* применяется только после перезагрузки операционной системы. Для того, чтобы принудительно запустить установку агента EDR на целевой машине, необходимо запустить командную строку от Администратора и выполнить: gpupdate /force.

7.10.3. Установка и удаление EDR (через EDR Installer)

Руководство по автоматической установке (EDR Installer)

Руководство АО «БУДУЩЕЕ» EDR Installer состоит из двух частей:

- 1. Windows service (Службы Windows)
- 2. GUI interface (графический интерфейс)

Все действия на удаленных хостах выполняются через протокол WMI. **Примечание:** необходимо разрешить входящее соединение WMI на всех целевых хостах.

Прежде чем приступить к установке, Вам необходимо подготовить следующее:

- Учетную запись Active Directory, у которой есть права на получение списка хостов AD (права на чтение).
- Учетную запись домена, которая имеет права на выполнение команд WMI и имеет доступ к общей папке с $ на всех целевых хостах и на ПК, на котором Вы устанавливаете EDR Installer.
- Локальную папку с файлами установщика EDR installer files (.msi), файлом конфигурации и файлом подписи.

Установка

Перед настройкой необходимо подготовить локальную или удаленную папку с установочными файлами агента EDR. Структура этой папки должна иметь следующий вид:

- ROOTFOLDER
- win7
    - x64
        - gibep.msi
        - gibepcheckclean.exe
        - gibepremovaltool.msi
    - x86

        - gibep.msi
        - gibepcheckclean.exe
        - gibepremovaltool.msi
- win8
    - x64
        - gibep.msi
        - gibepcheckclean.exe
        - gibepremovaltool.msi
    - x86
        - gibep.msi
        - gibepcheckclean.exe
        - gibepremovaltool.msi
- win81
    - x64
        - gibep.msi
        - gibepcheckclean.exe
        - gibepremovaltool.msi
    - x86
        - gibep.msi
        - gibepcheckclean.exe
        - gibepremovaltool.msi
- win10
    - x64
        - gibep.msi
        - gibepcheckclean.exe
        - gibepremovaltool.msi
    - x86
        - gibep.msi
        - gibepcheckclean.exe
        - gibepremovaltool.msi
- gibep_config.sign.txt
- gibep_config.txt

Конфигурационные файлы gibep_config.sign.txt и gibep_config.txt – файлы, которые будут использоваться по умолчанию. В дальнейшем Вы сможете выбрать другие конфигурационные файлы для отдельных хостов или OU в целом.

Для установки АО «БУДУЩЕЕ» EDR Installer Вам необходимо запустить файл *.msi file*. Это позволит установить как службу Windows, так и приложение пользовательского графического интерфейса (Graphical User Interface).

Путь установки C:\Program Files (x86)\Group-IB\EDRInstaller.

После установки графического интерфейса, ярлык приложения отобразится на рабочем столе ПК.

Руководство пользователя GUI

Чтобы открыть главное окно приложения с графическим интерфейсом, дважды щелкните на ярлык на рабочем столе.

Главное окно приложения GUI содержит три кнопки:

- 1. Кнопка Настройки;
- 2. Кнопка AD;
- 3. Кнопка Запуск.

Кнопка Настройки

При первом нажатии на кнопку **Настройки**, в открывшемся окне заполните поля данными, которые будут использоваться для получения информации об иерархии хостов из директории *Active Directory* (логин, пароль и IP-адрес контроллера домена).

После нажатия на кнопку **Check** заполненные учетные данные пройдут проверку и сохранятся в базе данных. Вам будет предложено заполнить следующие поля:

- **Use previous AD login and password** – При установке на АРМ, будут использоваться login и password, указанные выше ждя подключения к AD;
- **Installation only (no update)** – агент будет устанавливаться только на те хосты, на которых в данный момент не установлено никакой версии. В новых версиях XDR автоматически осуществляет обновления агентов, поэтому необходимо поставить галочку напротив данного пункта.
- **Set time to auto-update hosts** – установка времени для автоматического обновления хостов.

Здесь Вы должны выбрать путь к папке (локальной или удаленной) с установщиками агента EDR (описанной в разделе «Установка») и ввести логин и пароль, которые будут использоваться для установки агента (или установить флажок, чтобы использовать предыдущий).

Примечание: Путь к удаленной папке должен быть представлен в формате UNC, например,
\\share_name\path\to\folder.

При желании Вы можете установить таймер, чтобы начать автоматическое обновление в определённое время с указанным интервалом между попытками установки.

Кнопка AD

При нажатии на кнопку **AD** откроется новое окно, в котором можно выбрать на какие хосты необходимо установить EDR агент. Вы можете выбрать как отдельный хост, так и весь OU (во втором случае все новые хосты, добавленные в выбранный OU, будут рассматриваться как целевые хосты для дальнейшей автоматической установки).

Зелёное поле помечает хост как целевой, красное запрещает установку на данный хост.

Примечание: красное поле имеет больший приоритет, чем зелёное. При выборе обоих полей хост будет отображаться в главном окне графического интерфейса, но установка на него производиться не будет.

При нажатии на хост или OU правой кнопкой мыши появится контекстное меню с возможностью выбора конфигурационных файлов.

Процесс установки

Если в процессе настройки Вы выбрали опцию автоматической установки по таймеру, установка начнётся в заданное время. Также Вы можете вручную запустить процесс установки на все выбранные хосты нажатием на кнопку **Запуск** (если в базе данных есть информация об установленной на хосте версии агента, то установка на хост будет произведена только при установке более новой версии).

На время процесса установки кнопки приложения становятся недоступными. По завершении установки поля таблицы в главном окне приложения будут заполнены соответствующими данными.

При нажатии на хост правой кнопкой мыши будет отображено контекстное меню со следующими возможностями:

1. View logs для отображения логов последней установки (также логи можно отобразить двойным нажатием мыши на данный хост).

2. Force installation для принудительной установки агента на хост (в данном случае установщик не обращает внимания на версию агента в локальной базе данных, а производит установку в любом случае).

3. Remove agent используется для удаления агента с хоста. При успешном удалении агента информация о хосте будет также удалена из базы данных.

Важно: закрытие главного окна приложения не остановит его. Приложение будет отображаться в трее. Если Вы хотите полностью остановить приложение GUI, Вам необходимо щелкнуть правой кнопкой мыши на значок приложения в трее и выбрать опцию *«Exit»*.

4. Start collecting perflogs инициирует на хосте процесс сбора перфлогов.

5. Stop collecting perflogs завершает на хосте процесс собра перфлогов и копирует файл с собранными перфлогами в корневую директорию EDRInstaller (C:\Program Files (x86)\Group-IB\EDRInstaller).

Установочные логи

Процесс установки можно посмотреть, дважды щелкнув левой кнопкой мыши по хосту. В таком случает будет открыто окно Log Viewer.

Предпоследняя строка данного лога показывает конечный статус установки:

MainEngineThread is returning *

значение 0 – установка прошла успешно и без ошибок;

значение 1603 – в процессе установке произошла ошибка, в следствии которой агент не был установлен на хост.

Служба Windows

Всё взаимодействие с хостами и базой данных производится через службу EDRInstallerService (Вы можете найти эту службу в списке служб Windows – services.msc).

Логи службы пишутся в Event Viewer (Журналы приложений и служб -> EDRInstallerService).

Event Viewer и взаимодействие с ним

Основная информация во время установки агентов на хосты, будет записываться службой EDRInstallerService в Event Viewer (Просмотр событий).

Найти события, записанные данным сервисом можно по пути:

Event Viewer (local) > Applications and Services Logs > EDR Installer

Просмотр событий (локальный) > Журналы приложений и служб > EDR Installer

Примечание:

Основная и самая частая ошибка, которая может возникать при установке агента на хосты:

RPC is unavailable – Удаленный хост выключен или недоступен. Если в параметрах HP Installer вы установили какой-либо интервал установки, то на выключенные хосты рано или поздно агент установится автоматически, как только целевой хост станет доступным.

Другие ошибки при работе с Event Viewer

Если в ходе работы у вас возникли ошибки иного рода, тогда выполните следующие действия.

Выделите события процесса установки на проблемный хост, начиная с события *“Starting for *HOSTNAME*“* и до конечной ошибки, где указан тот же **HOSTNAME** затем нажмите на них правой кнопкой мыши и выберите опцию “сохранить выделенные события”.

7.11. Встраивание MDP

7.11.1. Установка MDP

Для обновления ПО, проверки ссылок, отправки алертов и использования преимуществ XDR Console, необходимо обеспечить доступ к XDR Console через порт управления.

При необходимости взаимодействие с XDR Console может осуществляться через прокси-сервер. В этом случае должен поддерживаться метод CONNECT для установления подключений на 443 порт.

Во время загрузки с образа будет предложено установить MDP. Здесь же можно просмотреть информацию об аппаратном обеспечении, перезапустить / выключить сервер или виртуальную машину.

В появившемся окне "Меню запуска установки" выберите **Install**.

На этом шаге можно выбрать один из двух языков, на котором выведется информация о лицензионном соглашении.

7.11.2. Активация MDP и синхронизация с XDR Console

Активация MDP – включает функционал NTA.

Синхронизация MDP – привязывает MDP к XDR либо к XDR cloud, тем самым предоставляя возможность управления сенсором через обозначенные системы.

Перед активацией NTA на облачном или локальном XDR Console необходимо получение лицензионного ключа (UID). Воспользуйтесь одним из следующих вариантов:

1. При активации на XDR cloud обратитесь к менеджеру или технической поддержке АО «БУДУЩЕЕ».
2. При активации на локальном XDR используйте пункт меню "Добавить устройство".

Для взаимодействия сенсора с XDR необходимы следующие порты:

- 443/tcp – для первичной активации и привязки MDP (единоразово) – вне зависимости от выбора типа XDR
- 1443/udp – для дальнейшего взаимодействия MDP с XDR – только для локальной версии
- 3000/tcp – для взаимодействия MDP с NTA

Активация и синхронизация осуществляется через консоль MDP.

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

После нажатия **<Enter the Shell>** пункт Activation в открывшемся меню 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:

- CA – on-cloud инсталляция. Оркестрация устройством осуществляется через SOC АО «БУДУЩЕЕ»;
- Private XDR Console – on-premise инсталляция. Оркестрация устройством осуществляется через XDR Console.

При выборе Ptivate XDR Console необходимо задать доменное имя или IP-адрес XDR Console.

При выборе CA необходимо задать доменное имя или IP адрес SOC АО «БУДУЩЕЕ». (задано по умолчанию).

При работе с MDP 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 Console

При нажатии **OK** запускается процесс регистрации и синхронизации MDP с выбранным сервером.

Внимание: после данной операции мигрировать NTA с одной инфраструктуры на другую невозможно без вмешательства технической поддержки АО «БУДУЩЕЕ».

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

Панель инструментов в консоли MDP будет отображать XDR Connection со статусом OK.

Меню UI > Настройки > Устройства > *будет* отображать *в списке устройств информацию по состоянию подключенного устройства* MDP.

7.11.3. Подключение к консоли MDP

Доступ к консоли MDP 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!

7.11.4. Главное меню MDP

Пункты главного меню:

1. Network menu: просмотр и изменение настроек сетевых интерфейсов.

2. Change Password: изменение пользовательского пароля от Shell.
3. Debug shell: режим отладки.
4. Power management: меню управления питанием.

При выборе кнопки **OK** откроется окно просмотра и изменения настройки сети.

7.11.5. Настройка сети MDP

Для работы с сетевыми настройками необходимо подключиться к MDP используя любой удобный SSH-клиент.

Важно: если у Клиента используется локальный XDR (расположен непосредственно на площадке Клиента), то окно "Network menu" будет отображаться в следующем виде:

Примечание: Пункт меню "Configure XDR connection" будет отображаться только после активации NTA за локальным XDR

Пункты меню настройки сети:

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

Для настройки сети необходимо проделать следующее:

- Перейдите в меню "Configure network"
- Network menu -> Configure network

Выберите необходимый способ получения сетевых настроек

- DHCP: позволяет автоматически получить и сохранить необходимые сетевые настройки;
- STATIC: переходит в разделы для статической конфигурации сетевого интерфейса.

Вводить IP-адреса DNS необходимо через пробел.

- Проверьте информацию о настроенном сетевом интерфейсе:
  Network menu -> Show current network settings

7.12. Обеспечение связности всех модулей с XDR Console

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

XDR Console

- Для доступа к инфраструктуре АО «БУДУЩЕЕ»:
  - gateway.mxdr.ru :443/tcp – режим "TI Feed", т.е. с туннелем

- repo.mxdr.ru (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
- Для отправки файлов на анализ в MDP:
  - 3000/tcp на ip-адрес MDP

Sensor Industrial

- Для связи с XDR:
  - 1443/udp на ip-адрес XDR
- Для отправки файлов на анализ в MDP:
  - 3000/tcp на ip-адрес MDP

MDP

- Для связи с XDR:
  - 1443/udp на ip-адрес XDR
- Для отправки отчетов об анализе в NTA
  - 3000/tcp на ip-адрес NTA

Storage

- Для связи с XDR:
  - 9200/tcp, 9300/tcp, 9220/tcp, 9320/tcp на ip-адрес XDR

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

Настройка находится по адресу WUI -> Администрирование -> Настройка модуля NTA -> Блок «Сетевой трафик» –> 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.
Позволяет указать локальные интерфейсы, а также интерфейсы для SPAN/RSAN/SPANinGRE.
Разделён на два подраздела.

Анализ сетевого трафика
Позволяет явно указать локальные адреса, сети / подсети, а также адреса локальных Proxy. Данный список определяет так называемую домашнюю сеть (Homenet) для сигнатурного анализа трафика. Выбор Homenet важен для группировки событий по подразделениям
Введите список локальных подсетей и исключите из них адреса Proxy-серверов (используйте знак отрицания – пример: !proxy-ip/32).
Это позволит различать взаимодействия целевых хостов, сетей / подсетей с открытой сетью Интернет.

Интерфейсы для анализа трафика

- Интерфейс – имена интерфейсов.
- Текущая нагрузка – это поток трафика, который подается на конкретный интерфейс – без учёта того анализируется данный трафик или нет.
- BPF – фильтр BPF для анализа трафика по сигнатурным правилам.
- On/Off
- Число тредов – установленное число потоков для каждого процесса сигнатурного анализа SPAN трафика на выбранном интерфейсе. (по умолчанию задано рекомендуемое значение. Изменение значения может повлиять на производительность системы!).

7.14. 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

8. Интерфейс администратора

Управление настройками модулей MXDR производится через Web-интерфейс XDR Console.

При открытии в браузере страницы https://ip_addr_TDS_XDR Пользователю будет предложена форма аутентификации. Для входа в систему используйте логин/пароль созданный в процессе активации XDR Console или выданный вам вашим администратором.

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

8.1. Панель управления

Панель управления предоставляет возможность наблюдения за общими показателями всех модулей системы в графическом виде. Каждый виджет предоставляет возможность наблюдать различные показатели подсистем и настраивается под нужды Пользователя. Для заполнения панели управления необходимо нажать «**Добавить виджет»**.

- **Имя виджета** – задаёт уникальное наименование виджета
- **Фильтр данных** – частный фильтр данных. Типы фильтров в данном разделе зависят от выбранного виджета и полностью повторяют их в соответствующих разделах интерфейса XDR (Например, "Алерты", "Устройства", "Почта" и т.п.)
- **Время** – выбранный период выборки. Присутствует в зависимости от типа виджета.

В таблице представлена краткая информация по каждому виджету.

Название виджета	Описание
Состояние устройств	Виджет предоставляет данные о CPU, RAM, HDD по всем подключенным к XDR Console устройствам
Последние алерты	Виджет предоставляет список крайних по дате алертов возникших в системе
Алерты по классификатору и критичности	Виджет предоставляет диаграмму с количеством алертов за выбранный период по выбранному сенсору
Статистика событий по классификатору	Предоставляет данные по количеству событий сразу по всем классификаторам за выбранный временной период в виде диаграммы
График событий по классификатору	Представляет график количества событий по каждому классификатору за выбранный период времени
График SPAN интеграции	График зависимости общей нагрузки на всех SPAN интерфейсах выбранного сенсора к выбранному периоду времени
Статистика SPAN интеграции	Предоставляет диаграмму с данными по нагрузке на SPAN интерфейсы выбранного сенсора в режиме онлайн
График проанализированных файлов и почты	График отображает статистику по принятым почтовым сообщениям и проанализированным вложениям у выбранного сенсора на указанном отчётном периоде, а также явно указывает число уникальных файлов, проанализированных за выбранный период в почтовом трафике
Статистика электронной почты	Предоставляет диаграмму с данными по количеству принятых письменных сообщений и письменных сообщений с вложениями на выбранном сенсоре
График числа online-хостов с EDR	График отображает количество ПК с установленными на них EDR со статусом онлайн на временной шкале
График системных событий EDR	График отображает статистику по числу событий на всех EDR обнаруженных за указанный отчётный период
Состояние интеграций	Виджет решает проблему информирования о недостатках в работе интеграций решения, таких как, например, ошибки подключения к интернету виртуальных машин MDP, недоступность почтовых серверов клиента для передачи им писем, ошибки в запросах ICAP-серверу и т.д.

Статистика сетевых соединений	В данном поле отображается статистика сетевых соединений, сформированная за выбранный промежуток времени
Время обработки электронных писем	Виджет предоставляет информацию по количеству обработанных электронных писем в разрезе времени обработки за выбранный период

8.1.1. Состояние устройств

Виджет предоставляет данные о CPU, RAM, HDD по всем подключенным к XDR Console устройствам. Данные по нагрузке предоставляются в режиме онлайн. По отключенным / несинхронизированным устройствам отображаются крайние рабочие даты.

По каждому устройству доступно:

- **Тип устройства**

Тип модуля MXDR

- **Имя устройства**

Наименование, заданное при создании нового устройства в разделе "Добавить устройство" в настройках графического интерфейса XDR.

По клику на имени возможен переход к настройкам данного устройства в разделе "Устройства"

- **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 и датой крайнего статуса "онлайн"*

Цветовые индикаторы:

- зеленый – Активное устройство;
- розовый – Ограничение производительности;
- синий – Ограничение лицензии

8.1.2. Последние алерты

Виджет предоставляет список крайних по дате алертов возникших в системе. По щелчку на алерте происходит переход к полному описанию в разделе "Алерты".

Чтобы перейти к списку всех алертов нажмите "**Показать все"** 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**

8.1.3. Алерты по классификатору

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

В правом верхнем углу виджета находится меню выбора отчётного периода.

8.1.4. Структура событий по классификатору

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

8.1.5. График событий по классификатору

График, отображающий количество событий по каждому классификатору за выбранный период времени. Каждая кривая описывает статистику одного классификатора по всем подключенным к XDR модулям данного типа (классификатора).

Существует возможность отображать на графике отдельные кривые, характеризующие модули. По умолчанию все фильтры отключены. При выборе одного из фильтров кривая, соответствующая названию фильтра перестаёт отображаться (вычёркивается).

Доступные фильтры:

- MDP – Количество событий от всех MDP, подключенных к XDR.
- NTA – Количество событий от всех NTA подключенных к XDR.
- EDR – Количество событий от всех EDR подключенных к XDR.

8.1.6. График SPAN интеграции

График зависимости общей нагрузки на всех SPAN интерфейсах выбранного сенсора за определенный период времени. Предоставляет данные по дропам ядра в том же масштабе. Для отображения данных задайте сенсор через меню выбора сенсора.

Существует возможность отображать на графике 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.

8.1.7. 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 загрузка**

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

- **Максимальная загрузка**

Максимальная загрузка 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.

8.1.8. График проанализированных файлов и почты

График отображает статистику по принятым почтовым сообщениям и проанализированным вложениям у выбранного сенсора на указанном отчётном периоде, а также явно указывает число уникальных файлов, проанализированных за выбранный период в почтовом трафике. По меню выбора сенсора доступны подключенные к XDR сенсоры:

Существует возможность отображать на графике отдельные кривые. По умолчанию все фильтры отключены. При выборе одного из фильтров кривая, соответствующая названию фильтра перестаёт отображаться (вычёркивается). Доступные фильтры:

- **Письма**
  Количество входящих (принятых) письменных сообщений.
- **Вложения**
  Количество вложений в письмах принятых к обработке
- **Файлы (уникальные)**
  Количество уникальных файлов за выбранный период в почтовом трафике.

8.1.9. Статистика электронной почты

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

Для отображения данных задайте сенсор через меню выбора сенсора. А также выберите требуемый промежуток времени.

Доступная информация:

- **Писем на проверке**

Количество писем в состоянии обработки. По щелчку на количестве производит переход в раздел "Письма" с соответствующими фильтрами сенсора и датам.

- **Ошибок доставки писем**

Ошибки доставки писем. По щелчку на количестве производит переход в раздел "Письма" с соответствующими фильтрами сенсора и датам

8.1.10. 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.

8.1.11. График системных событий EDR

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

8.1.12. Состояние интеграций

Виджет решает проблему информирования о недостатках в работе интеграций решения, таких как, например, ошибки подключения к интернету виртуальных машин MDP, недоступность почтовых серверов клиента для передачи им писем, ошибки в запросах ICAP-серверу и т.д. Ошибки не всегда говорят об аварийной ситуации, но должны контролироваться Клиентом.

Полный список ошибок доступен в разделе "Системные журналы».

К данному списку также можно перейти, нажав на количественное обозначение возникших проблем в виджете. При этом автоматически будет задействован фильтр выбранного типа ошибки.

8.1.13. Статистика сетевых соединений

В данном поле отображается статистика сетевых соединений, сформированная за выбранный промежуток времени. Более подробная информация содержится в одноименном разделе.

8.1.14. Время обработки электронных писем

Виджет предоставляет информацию по количеству обработанных электронных писем в разрезе времени обработки за выбранный период.

Для inline-писем считается время между получением письма и отправкой следующему серверу;

Для не-inline писем – время между получением письма и завершением его полного анализа

По умолчанию статистика предоставляется по всем контролируемым устройствам за выбранный период. Для задания конкретного набора используйте поисковую строку в настройках виджета или при его создании. (тег поиска: appliance_name).

По щелчку на времени обработки будет произведен переход пользователя в раздел "Письма" с автоматически указанными фильтрами по диапазону обработки.

9. Алерт

Данный раздел, отображаемый в графическом интерфейсе XDR, предоставляет информацию о всех потенциальных инцидентах, детектируемых установленными модулями MXDR: NTA, Sensor Industrial, MDP, BEP и EDR.

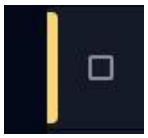
Алерт – уведомление о потенциальной вредоносной активности.

Уровни опасности алерта

Рядом с каждым алертом расположены цветовые индикаторы, которые обозначают уровень опасности алерта.

Высокий (Красный) – события с критическим уровнем угрозы. Такие события, как правило, указывают на критические заражения устройств в сети (целевые трояны, дропперы, бэкдоры, и т.д.), либо на подтвержденную эксплуатацию критических уязвимостей

Средний (Оранжевый) – события со средним уровнем угрозы, указывающие на попытки эксплуатации уязвимостей в ПО, сетевом оборудовании или сетевых сервисах



Низкий (Желтый) – события, указывающие на нежелательную, но в целом, некритическую активность. Например, ПО класса Adware или другое нежелательное ПО, нарушающее политику безопасности, принятую в организации

Информация по алертам

По каждому инциденту предоставляется основная краткая информация, содержащаяся в полях:

- **Уровень опасности** – цветовая индикация, которая визуально классифицирует алерт по степени угрозы.
- **Создан** – дата и время создания алерта. Подразумевается формальная дата обозначения набора событий потенциально вредоносными. Формальная дата может быть позже даты цепочки событий, породивших данный алерт. Содержит в себе время последнего обновления алерта (изменения состава по событиям)
- **Статус** – атрибут, служащий для отображения информации о текущем статусе работ по решению заявки.

	**Обнаружен** – выявлена потенциально вредоносная активность, требуется реакция
	**Заблокирован** – вредоносная активность была заблокирована системой XDR Console
	**Закрыт** – отметка аналитика о решенной проблеме
	**Ложный** – отметка аналитика о ложноположительном срабатывании
	**Инцидент** – отметка о принадлежности к группе алертов в рамках одного инцидента
	**Приостановленный** – отслеживание системой приостановлено на выбранный период

- **Причина** – Наименование алерта. Содержит в себе теги событий, породившие данный алерт.
- **Устройство** – наименование модуля MXDR, на котором была выявлена подозрительная активность
- **Свойства**
  - **События** – количество атомарных событий в составе выбранного алерта
  - **Комментарии** – количество комментариев по выбранному алерту
  - **Связан с** – ссылка на цепочку алертов, связанных с одним инцидентом *(ссылка на раздел Инциденты)*
- **Цель** – целевой объект (хост, пользователь и т.п.), на который на направлена атака злоумышленника. На него необходимо обратить внимание.

Описание алерта

Алерт может состоять из нескольких групп однотипных событий. В таком случае события собираются в цепочку и отображаются при раскрытии алерта в поле "Информация об алерте". Чтобы получить подробную информацию по алерту необходимо нажать на него.

При раскрытии алерта предоставляется расширенная информация по нему, включающая:

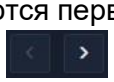
- События – собранные в цепочку группы событий, связанных с данным алертом. Также приведено описание контекста.

Подробное описание событий приведено на страницах соответствующих классификаторов.

Классификатор событий

- DGA аномалии
- Нарушение политик технологических протоколов
- Изменение топологии
- EDR
- MDP
- Сигнатурный анализ трафика
- Скрытые каналы
- Lateral Movement

Фильтрация событий

1. События выстроены в виде убывающего по времени списка (крайние по времени события отображаются первыми).
2. С помощью кнопок  в левом нижнем углу существует возможность листать события.
3. Помимо этого, имеется возможность фильтрации событий следующими инструментами:

- Поиск – текстовый поиск по всем полям событий
- Уровень угрозы – отображает только события заданного уровня угроз.
    - Низкий (желтый)
    - Средний (оранжевый)
    - Критический (красный)

Не путайте уровень угроз события и уровень угроз алерта – это разные показатели!

- Классификатор событий – отображает только события, полученные из выбранной компоненты.
    - Сигнатурный анализ трафика
    - DGA аномалии
    - MDP
    - EDR
    - Неизвестное сетевое взаимодействие

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. При реагировании на алерт, рекомендуется оставлять комментарии.

Для добавления вложений необходимо нажать на кнопку	

Для отправки комментария нажмите	

Обработка и реагирование на алерты

Аналитику необходимо своевременно реагировать и обрабатывать алерты.

Чтобы отреагировать и присвоить статус алерту необходимо нажать на кнопку	
Чтобы скачать отчет в формате csv необходимо нажать на кнопку	
Чтобы перейти на страницу с информацией о выбранном алерте, а также скопировать ссылку на эту страницу в буфер обмена необходимо нажать	

Алерту можно присвоить один из следующих статусов:

- Решенный – отметка аналитика о решенной проблеме (*закрыт*)
- Ложный – отметка аналитика о ложноположительном срабатывании
- Приостановлен – отслеживание системой приостановлено на выбранный период

Сортировка алертов

Для сортировки алертов используйте кнопку  в правом верхнем углу экрана. Доступные поля для сортировки:

- Дата создания
- Дата обновления
- Уровень опасности

Фильтр алертов

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

Доступные фильтры для алертов:

- **Актуальные** – алерты, которые требуют внимания аналитика (т.е. не ложные, не решенные и не приостановленные алерты)
  - Да
  - Нет
- **Уровень угрозы** – выбор алертов с выбранным уровнем угроз:
  - Низкий (Желтый цвет индикатора).
  - Средний (Оранжевый цвет индикатора).
  - Высокий (Красный цвет индикатора).
- **Заблокировано** – статус файлов:
  - Да – отображать только заблокированные файлы.
  - Нет – отображать только незаблокированные файлы.
- **Ложный** – 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.
- **Решенный** – отображение разрешенных алертов:
    - Да – отображать только решённые.
    - Нет – убрать все решенные из общей выборки алертов.
    - Пусто – отображать решенные алерты в общей выборке.
- **Приостановленный**
    - Да – отображать приостановленные
    - Нет – отображать все кроме приостановленных
    - Пусто – без фильтров
- **Система интеграции** – выбор алертов, содержащих в себе события выбранного способа интеграции:
    - EDR – события с ПК с установленной компонентой EDR.
    - Сетевой трафик – события из анализируемого SPAN трафика.
    - 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
    - Общие ресурсы – события, полученные при анализе файлов файловых хранилищ
    - Пусто – отображать алерты всех типов событий в выборке.
- **Классификатор** – выбор алертов, содержащих события от выбранной подсистемы(компоненты) MXDR:
    - DGA аномалии
    - Нарушение политик технологических протоколов
    - Изменение топологии
    - EDR
    - MDP
    - Сигнатурный анализ трафика
    - Скрытые каналы
    - Lateral Movement

Фильтры дат и текста

По мимо данного типа фильтров доступен общий фильтр по датам с возможностью текстового запроса по всем полям алертов и событий. Подробнее о форматах запросов смотри в разделе "Расширенный поиск внутри алертов и событий".

9.1. События «DGA аномалии»

В данном разделе отображаются события типа "DGA коммуникации", выявленные при взаимодействии с управляющими серверами через DGA.

9.2. События «Сигнатурный анализ трафика»

События, зарегистрированные системой сигнатурного анализа – это случаи совпадения содержимого сетевых сессий с известными шаблонами вредоносного трафика

(рис. Сигнатурные события). 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;
  - 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 (если присутствуют)
  - SID – уникальный номер сигнатуры (может быть несколько). Подробнее в статье "Атрибуция"
  - Удаленные хосты – хосты использовавшиеся для проведения атаки. При переходе по домену / IP адресу, система использует его для графового анализа.
  - Описание угрозы – атрибуция события известному ВПО или техникам (если присутствует). Подробнее в статье "Атрибуция"
- **Исходные данные**

Предоставляет заголовок коммуникаций, относящихся к данному событию в различных форматах (рис. Исходные данные). Состав доступных форматов зависит от конкретного события.

9.3. События «MDP»

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
  - 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 (если присутствует). При переходе по домену / IP адресу, система использует его для графового анализа
  - URI – полная ссылка на ресурс, из-за обращения на которую был получен объект анализа (если присутствует)
  - Тема – Тема письма, из которого был получен объект анализа (если присутствует)

- Имя файла
- MD5/SHA1/SHA256 – Значение хешей объекта анализа
- Вердикт – вывод по проведенному анализу
- Отчёты – ссылка на подробный описание анализа
- SID – уникальный номер сигнатуры (может быть несколько), сработавшей на трафике ВПО. Подробнее в статье "Атрибуция"
- Описание угрозы – атрибуция события известному ВПО или техникам (если присутствует). Подробнее в статье "Атрибуция"

- **Исходные данные**
  - Исходные данные – это часть полезной нагрузки, относящейся к передаче анализируемого объекта. Например: почтовые заголовки письма, HTTP хедер и ICAP сессии и т.п.

Отчёты

При клике на **отчёте** страница перенаправляет пользователя на итоги детального анализ семпла в MDP.

Общие сведения

В блоке 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.

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
- Наличие интернет-соединения – явно указывает на присутствие / отсутствие доступа в сеть Интернет при проведении анализа

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 (рис. Детали файловой структуры).

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

Матрица MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge)

Отчеты MDP по вредоносным файлам предоставляются в соответствии с матрицей MITRE ATT&CK (Тактики, техники и общеизвестные знания о злоумышленниках).

Каждое поведенческое правило связано с одной или несколькими ячейками матрицы, что позволяет более точно визуализировать вредоносную активность файла. Матрица ATT&CK позволяет стандартизировано описывать поведение злоумышленников. Акторы могут отслеживаться с помощью ассоциаций с методами и тактиками в ATT&CK, используемыми ими.

База знаний ATT&CK также доступна в виде фида STIX / TAXII 2.0, который позволяет легко интегрировать ее в любые инструменты, поддерживающие эту технологию.

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 зависимости от присутствующей активности информация может содержать: DNS, HTTP, TCP, UDP и иные протоколы.

По кнопке "Скачать PCAP" доступна возможность скачивания PCAP-файла с полным дампом выявленных запросов.

Дерево процессов

В блоке содержится дерево процессов в состоянии после запуска объекта анализа.

Применяется цветовая легенда:

- Красный цвет - процессы исследуемого объекта
- Желтый цвет - процессы созданных (дропнутых) файлов.
- Синий цвет - остальные процессы.

При клике на любой из процессов можно получить детали по активности процесса и вносимых системных изменениях.

7.3.1 Приоритет поведенческого анализа на MDP

При использовании различных подсистем для анализа файлов решением сформирован следующий приоритет анализа (в порядке убывания):

1. Файлы, полученные из почты в режиме inline (MTA) анализируется в первую очередь.
2. Файлы из полученные из почтового трафика в режиме мониторинга

3. Файлы, полученные со всех остальных типов интеграции, анализируются в последнюю очередь

- При этом приоритет устанавливает NTA для всех файлов кроме EDR.
- Файлы от EDR автоматически попадают в 3-й тип приоритетов (см. список выше).
- MDP, получая файл, использует установленный приоритет в своей очереди.

9.4. События «Выявление скрытых туннелей»

В данном разделе отображаются события типа "Скрытые туннели", выявленные при взаимодействии с управляющими серверами.

При нажатии на событие откроется подробная информация по нему, включающее в себя:

- **Сведения об источнике**
  - ID сенсора - уникальный номер оборудования NTA;
  - Интеграция - указывает на способ интеграции и протокол реализации;
  - Время - время и дата сработки;
  - От кого - источник, инициировавший коммуникацию;
  - Кому - адрес назначения;
- **Сведения об угрозе**
  - Удаленные хосты - управляющий сервер для установления выявленного туннеля. При переходе по домену / IP адресу, система использует его для графового анализа
- **Исходные данные**
  - Предоставляет заголовок коммуникаций, относящихся к данному событию в различных форматах (рис. Исходные данные). Состав доступных форматов зависит от конкретного события.

9.5. События «EDR»

События, зарегистрированные на конечных станциях.

В событиях описываются все производимые на конечном устройстве изменения связанные с данным алертом.

По клику на любое из событий открывается более подробная информация о каждом из событий.

Состав подробного описания событий варьируется от типа действий, зафиксированных на конечных станциях.

Изолировать хост

Данная функция доступна только при наличии EDR установленного на ПК. После активации блокирует все входящие и исходящие сетевые соединения ПК за исключением общения с XDR Console.

9.6. События «Lateral Movement»

События данного типа представляют реакцию ML классификатора на возможные неавторизованные использования административных ресурсов в защищаемой сети. Анализируемые протоколы:

- SMB
- NTLM
- DCE-RPC (WMI и т.п.)
- Kerberos (update)

В тегах под названием алерта описываются выявленные признаки потенциально неавторизованных действий. (В данном случае Brute Forse через NTLM).

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;
  - Интеграция - указывает на способ интеграции и протокол реализации;
  - Время - время и дата сработки;
  - От кого - источник, инициировавший коммуникацию;
  - Кому - адрес назначения;
- **Сведения об угрозе**
  - Удаленные хосты - хосты использовавшиеся для проведения атаки. При переходе по домену / IP адресу, система использует его для графового анализа.
- **Исходные данные**
  - Предоставляет исходные данные коммуникаций вызвавшие сработок у классификатора (рис. Исходные данные). Состав доступных форматов зависит от конкретного события.

9.7. События «Изменение топологии»

События данного типа представляют информацию о сетевых соединениях, получаемую в результате анализа трафика с помощью решения Sensor Industrial.

Настройка правил фильтрации сети трафика для обеспечения контроля целостности среды Заказчика осуществляется в разделе "Реагирование на неизвестные сетевые взаимодействия".

Детальное описание событий "Изменение топологии"

Чтобы получить подробное описание по определенному неизвестному сетевому взаимодействию, необходимо нажать на него.

При нажатии на событие откроется подробная информация по нему, включающее в себя:

- **Сведения об источнике**
  - ID сенсора - уникальный номер оборудования NTA;
  - Интеграция - указывает на способ интеграции и протокол реализации;
  - Время - дата и время обнаружения соединения;
  - От кого - информация о инициирующем оборудовании. Производитель и MAC- адрес (опционально), а также IP-адрес;

- Кому - информация о принимающем оборудовании. Производитель и MAC-адрес (опционально), а также IP-адрес.

- **Сведения об угрозе**
  - Удаленные хосты - найденные запросы при анализе трафика. При переходе по домену, система использует его для графового анализа.

9.8. События «Нарушение политик технологических протоколов»

В данном разделе представлены события, формирующиеся в процессе контроля технологических протоколов.

Детальное описание событий "Прикладные протоколы"

Чтобы получить подробное описание по определенной сессии, необходимо нажать на неё.

При нажатии на событие откроется подробная информация по нему, включающее в себя:

- **Сведения об источнике**
  - ID сенсора - уникальный номер оборудования NTA;
  - Интеграция - указывает на способ интеграции и протокол реализации;
  - Время - дата и время обнаружения соединения;
  - От кого - информация о инициирующем оборудовании. Производитель и MAC-адрес (опционально), а также IP-адрес;
  - Кому - информация о принимающем оборудовании. Производитель и MAC-адрес (опционально), а также IP-адрес.
- **Сведения об угрозе**
  - Удаленные хосты - найденные запросы при анализе трафика. При переходе по домену, система использует его для графового анализа

9.9. Расширенный поиск внутри алертов и событий

Система позволяет производить поиск по всем показателям, определяемыми модулями (NTA, MDP, EDR). Таким образом возможно осуществлять сквозной поиск по всем индикаторам во всех событиях и алертах системы!

Поиск по общим маркерам

Общие маркеры

Служебные маркеры	Краткое описание	Формат запроса
action	-	-
alert_id	номер алерта в базе	ID
created_at	timestamp. дата появления алерта в базе	-
event_classifier	Фильтр классификатора событий	MDP

Служебные маркеры	Краткое описание	Формат запроса
		suricata eclipse
event_type	Фильтр по типу событий	exploit_activity network_anomaly EDR_activity malicious_file cnc_callback
events_count	Фильтр по количеству событий в алерте	Число
false_positive	статусы алерта	true/false
first_event	timestamp, дата появления первого события	
host	uuid хоста, на котором зафиксирован алерт/событие	UUID
integration_system	система интеграции	edr polycephal-server suricata EDR bro-ids telescope
last_event	дата последнего события в базе, timestamp	Текст ячейки
malware_families	Семейство ВПО	Выберите из списка предлагаемых семейств
matching_hashes	Текст ячейки	Текст ячейки
message	Поиск по имени события	Имя события
resolved	статусы алерта	True/False
severity	Фильтр по уровню опасности алерта	Значение от 1 до 5. 1 - зеленый уровень 5 - красный уровень
timestamp	Текст ячейки	Текст ячейки
updated_at	дата последнего изменения чего-либо в событии/алерте	Текст ячейки

Служебные маркеры	Краткое описание	Формат запроса
appliance_name	Фильтр имени сенсора	имя сенсора (выбрать из списка)
company_name	Фильтр по компаниям	Выбрать компанию из списка
ip	Поиск по всем IP адресам алертов	"111.111.111.111"
hosts	Фильтр по DNS / IP обнаруженном в сетевом трафике	
md5	MD5 файла	Hash
sha1	SHA1 файла	Hash
sha256	SHA256 файла	Hash
url	Фильтр по URI запросам в сетевом трафике	
malware	Фильтр по классификатору ВПО	Имя ВПО

Маркеры атакуемого

Подкласс **target** позволяет осуществлять поиск по атакуемым сущностям (IP, domainname, emails, файловые хранилища, имена пользователей).

Маркеры атакуемого

Служебные маркеры	Краткое описание	Формат запроса
target	-	-
target.emails	Фильтр по целевым почтовым адресам	электронный адрес (полный или частично)
target.hosts	Фильтр по доменным именам целевых хостов	доменное имя
target.ip_addresses	Фильтр по IP адресам целевых хостов	IP адрес
target.shares	Фильтр по подключенным файловым хранилищам	-

Служебные маркеры	Краткое описание	Формат запроса
target.usernames	Фильтр по менам пользователям жертвам	имя пользователя

Маркеры атакующего

Служебные маркеры	Краткое описание	Формат запроса
attribution.malware.reliability		
attribution.malware.ti_malware_id	Идентификатор ВПО или угрозы в системе киберразведки.	идентификатор
attribution.malware.ti_malware_name	Наименование ВПО или угрозы в системе киберразведки.	Строка. Выбрать из списка
attribution.threatactor.ti_threatactor_id	Идентификатор злоумышленников (threat actor) в системе киберравздки.	идентификатор
attribution.threatactor.ti_threatactor_name	Наименование злоумышленников (threat actor) в системе киберравздки.	Строка. Выбрать из списка
attribution.tool.ti_tool_id	Идентификатор технических инстру ментариев.	идентификатор
attribution.tool.ti_tool_name	Наименование технических инструментариев.	Строка. Выбрать из списка
attribution.threatactor		
attribution.malware		
attribution		

Поиск по индикаторам компрометации

Подкласс **ioc** позволяет осуществлять поиск по индикаторам внутри отчётов MDP, активности EDR, сетевой активности, выявленной NTA.
В рамках подкласса различают следующие индикаторы:

- **Индикаторы верхнего уровня (ioc.event)**

Индикаторы верхнего уровня позволяют осуществлять поиск по данным присущим самому артефакту анализа, исключая порождаемые этим артефактом данные (например: его сетевая активность, дропнутые файлы, затронутые ветки реестра и т.п.)

Индикаторы верхнего уровня (ioc.event)

Служебные маркеры	Краткое описание	Формат запроса
ioc	-	-
ioc.event	-	-
ioc.event.domains	Доменные адреса участников потенциальной атаки. Сюда подпадают, как управляющие хосты, так и целевые хосты, а также иные хосты, замеченные в трафике	DNS addresses
ioc.event.emails	Текст ячейки	Текст ячейки
ioc.event.filenames	Поиск по имени анализируемого файла	Имя файла
ioc.event.headers	Текст ячейки	Текст ячейки
ioc.event.ip_addresses	Сетевые адреса участников потенциальной атаки. Сюда подпадают, как управляющие хосты, так и целевые хосты, а также иные хосты, замеченные в трафике	IP addresses
ioc.event.md5	MD5	Hash
ioc.event.sha1	SHA1	Hash
ioc.event.sha256	SHA256	Hash
ioc.event.subjects	Текст ячейки	Текст ячейки
ioc.event.urls	Запросы URI выявленные в трафике	Полный или частичный URL запрос
ioc.event.usernames	Текст ячейки	Текст ячейки

- **Индикаторы внутренних уровней (ioc.extended)**

Индикаторы внутренних уровней (или расширенные индикаторы) позволяют осуществлять поиск по данным порождаемым анализируемым артефактом - дропнутые файлы, затронутые ветки реестра, процессы системы, регистры и т.п.

Индикаторы внутренних уровней (ioc.extended)		
Служебные маркеры	**Краткое описание**	**Формат запроса**
ioc.extended	-	-

Индикаторы внутренних уровней (ioc.extended)		
Служебные маркеры	**Краткое описание**	**Формат запроса**
ioc.extended.domains	Домены, к которым обращалось ВПО в процессе поведенческого анализа	DNS адрес
ioc.extended.families	Семейство ВПО	Выберите из списка предлагаемых семейств
ioc.extended.files	Поиск по файловой структуре артефакта анализа. При поведенческом анализе.	Имя файла
ioc.extended.ip_addresses	IP адреса, к которым обращалось ВПО в процессе поведенческого анализа	IP адрес
ioc.extended.md5	MD5	Hash
ioc.extended.mutexes	Мьютексы используемые анализируемым артефактов при поведенческом анализе	Имя мьютекса
ioc.extended.probabilities	Поиск по вероятностной оценке степени вредоносности файла при поведенческом анализе	Численное значение
ioc.extended.processes	Процессы, используемые артефактом анализа при проведении поведенческого анализа	Имя процесса
ioc.extended.registry	Поиск по затронутым ключам реестра при поведенческом анализе	Текст ячейки
ioc.extended.scores	оценка вредоносности файла из MDP	
ioc.extended.sha1	SHA1	Hash
ioc.extended.sha256	SHA256	Hash
ioc.extended.sids	Поиск по идентификатору сработавшей сигнатуры	"1002804"
ioc.extended.suricata_rules	Название SID-а	Название сигнатуры

Индикаторы внутренних уровней (ioc.extended)		
Служебные маркеры	**Краткое описание**	**Формат запроса**
ioc.extended.urls	Производимые URL запросы в процессе проведения поведенческого анализа артефакта	Полный или частичный URL

Сложные запросы

Для формирования гибких сложных запросов используются логические операции:

- **И**

  Используйте символы **&&**
- **ИЛИ**

  Используйте символы **||**
- **НЕ**

  Используйте символы **!**

Помимо данных операндов, возможно формировать запросы с использованием lucene-синтаксиса.

Важные примеры формирования сложных запросов

Отражение специальных символов

Обратите внимание на используемые спец символы при формировании запросов! Используйте операнд **/** для их отражения.

Список специальных символов:

- **&&**
- **||**
- **!**
- **( )**
- **{ }**
- **[ ]**
- **^**
- **"**
- *****
- **?**
- **:**
- ****

Группировка и использование операндов И, ИЛИ, НЕ

Для формирования запросов с операндами И, ИЛИ, НЕ необходимо обращать внимание на группировку вашего запроса. Ввиду того что система различает запросы типа:

- marker: запрос1 или запрос2

В данном запросе будет осуществлён поиск по marker-у со значением "запрос1", к которому будет добавлен поиск строки "запрос2".

- marker: (запрос1 или запрос2)

В данном запросе будет осуществлён поиск по marker-у со значением "запрос1" или "запрос2"

Пример из системы

- ioc.extended.mutexes: Local\\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511 OR Local\\WininetConnectionMutex

Найдёт мьютекс *Local\\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511* в отчётах поведенческого анализа. А также найдёт строку со значением *Local\\WininetConnectionMutex* в событиях системы.

- ioc.extended.mutexes: (Local\\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511 OR Local\\WininetConnectionMutex)

Найдёт мьютекс *Local\\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511* или *Local\\WininetConnectionMutex* в отчётах поведенческого анализа.

Поиск в пределах численных или строковых значений

- Включая границы

При формировании запроса используйте квадратные скобки **[ ]**, внутри которых используйте граничные значения с ключевым словом **TO**. Пример:

events_count: [0 TO 10] - выводит все алерты с количеством событий от 0 до 10 включительно

- Исключая границы

При формировании запроса используйте фигурные скобки **{ }**, внутри которых используйте граничные значения с ключевым словом **TO**. Пример:

malware: {Anunak TO Cron} - выводит все алерты с обнаруженными ВПО от Anunak до Cron (исключая граничные значения) - поиск осуществляется в лексикографическом порядке

Wildcards в тексте запроса

При использовании специальных символов в численных значениях кавычки опускаются, а в текстовых - ставятся.

- Одно вхождение любого символа

Используйте специальный символ **?**. Пример:

target.ip_addresses: 10.9.2.14? - выведет все алерты с IP адресами вида 10.9.2.14(0-9 или любой символ)

- Множественное вхождение любых символов

10. Расследование

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

- Письма
- Файлы
- Компьютеры
- События EDR
- Сетевые соединения
- Отчеты
- Контроллеры

10.1. 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.

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)
- Доставлено - указывает на соотношение полученных и доставленных писем. Различие типа интеграции меняет смысл соотношения:
    - BCC - указывает лишь на количество полученных писем. Количество отправленных всегда будет равно нулю.
    - MTA с безопасными письмами - указывает на соотношение количества получателей к количеству реально отправленных писем до получателей.
    - MTA с вредоносными письмами - указывает на соотношение количества получателей к количеству отправленных уведомлений о факте блокировки.

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, возможность скачать почтовое сообщение в формате *EML* (кнопка **скачать eml**), в случае если письмо признано вредоносным и возможность поделиться данным событием (в буфере обмена сохраняется ссылка с уникальным ID на данное событие).

- **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.

  Управление карантином

  При реализации MTA режима письма, заблокированные системой, попадают в карантин XDR Console. 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 

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

Фильтры

Фильтры типов

По кнопке фильтра  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.

- **Статус доставки -** фильтрация писем, используемая в случае установки MDP "в разрыв".
  - Доставлено - письмо доставлено до конечного получателя
  - Не доставлено - не доставлено по причине ошибок
- **Статус письма**
  - Получено - письмо получено сенсором.
  - Не обработано - письмо находится в очереди на обработку.
  - Обработано - письмо обработано и данные письма готовы к отправке в MDP на анализ.
  - Отправлено - файл отправлен в MDP 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 письма** - 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

Помимо данного типа фильтров доступен общий фильтр по датам с возможностью текстового запроса по всем полям почтовых событий

10.2. Файлы

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

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.
- Устройство - наименование устройства через который файл был получен для анализа.
- Источник файла - указывается тег, указывающий на способ получения файла (смотри Фильтры файла).

    - От - источник файла.
    - Кому - адрес назначения.
- Имя файла - имя объекта. При клике по размеру файла происходит скачивание файла. (Доступно только для вредоносных файлов)
- 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.

При клике по статусу файла производится открытие подробного отчёта поведенческого анализа. Подробнее см. статью по классификаторам событий.

Мультиверсионные отчёты

В случае, если анализ в MDP потребовал использование различных версий ОС Windows для анализа объекта, имеется возможность просмотреть отчёты всех задействованных.

Для просмотра используйте знак троеточия рядом с вердиктом и в появившемся меню выберите необходимую версию отчёта. (см. рис. Мультиверсионный анализ)

Фильтры типов

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

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
    - HTTP
    - FTP
    - ICAP
    - MAIL - используется один из протоколов почтовой интеграции
    - SMB
    - DIR
    - MANUAL
    - ENDPOINT
- Получатель
- Отправитель

Переход к разделу "Сетевые соединения"

При нажатии на тег источника файлов, осуществляется переход в раздел "Сетевые соединения" с автоматической фильтрацией по потоку, связанному с передачей данного файла.

Переход к разделу "Компьютеры"

При нажатии на имя хоста в поле **Источник файла**, осуществляется переход в раздел "Компьютеры" с автоматической фильтрацией по выбранному компьютеру.

Восстановление файлов

Для восстановления файлов из карантина используйте кнопку **Восстановить** после выделения нужных файлов.

Восстановление производится по оригинальным метаданным. Файл не помещается в белые списки.

10.2.1. Ручная загрузка файлов для поведенческого анализа

Добавление задачи на анализ файлов доступно по кнопке 

Все задачи по анализу будут напрямую направляться в MDP. Статус анализа и отчёты доступны на той же странице в разделе "Файлы"

Поля к заполнению:

- Файлы
  Выбрать файл для загрузки.
- Язык
  Выберите язык ОС для поведенческого анализа объекта.
- Пароль архива
  Задайте пароль в случае, если объектом является запароленный архив.
  Примечание:
  Необходима интеграция XDR с MDP.

10.3. Компьютеры

В данном разделе представлен список компьютеров (хостов), на которых установлен или был установлен EDR. По каждому ПК предоставляются общие данные по системе и используемому оборудованию, а также алерты в чьих артефактах участвовал данный ПК.

Список компьютеров - общие сведения

В списке представлены все когда-либо подключавшиеся ПК к XDR.

Общая информация по компьютерам:

- **Версия** - версия EDR установленного на ПК
- **Имя компьютера** - сетевое / доменное имя ПК
- **Домен** - домен ПК в Active Directory
- **Компания -** подразделение ПК
- **Описание** - (опционально)
- **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 EDR

- **Алерты** - количество связанных с данным ПК алертов

Информация о компьютере

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

О компьютере

Доступная информация:

- **Имя** - сетевое / доменное имя ПК
- **Домен** - домен ПК в Active Directory
- **Описание хоста** - (опционально)
- **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.

Оборудование

Доступная информация:

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

Сеть

Информация о сетевом оборудовании ПК.

Доступная информация:

- **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.

Хранилище

Доступная информация: предоставляет данные об установленных накопителях в системе.

Пользователи

Список авторизованных, с момента установки EDR, пользователей.

Доступная информация:

- **Имя пользователя -** сетевое / доменное имя ПК
- **Первая активность** - первая сетевая активность интерфейса, зафиксированная с момента установки EDR
- **Последняя активность** - последняя сетевая активность интерфейса, зафиксированная с момента установки EDR

При нажатии на строку с информацией о пользователе откроется поле "Информация о логинах":

- **Дата**
- **Тип логина** - локальный или удалённый логин

- **Домен** - домен ПК
- **IP адрес** - первый адрес в списке сетевых адресов ПК

Алерты

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

Управление версиями

Для ручной загрузки пакетов с новыми версиями EDR, необходимо нажать на кнопку **Управление версиями**. В появившемся поле прикрепите файл.

Обновление компьютеров до новых версий EDR

Чтобы обновить компьютеры вручную до новых версий XDR, необходимо выбрать один или несколько компьютеров, после чего выбрать версию обновления.

Фильтры

По кнопке фильтра  расположенной в строке поиска веб-интерфейса открывается меню фильтрации.

Доступные фильтры для компьютеров:

- **Статус** - статус работы EDR на компьютере:
  - Online
  - Offline
- **Актуальные** - актуальные подключения
  - Да
  - Нет
- **Разрядность системы** - разрядность ОС ПК
  - 32
  - 64

10.4. События EDR

Система позволяет производить поиск по всем событиям, зафиксированным EDR. События формируются в таблицу, которая состоит за следующих полей.

Общая информация	
Тип поля	**Описание**
Дата	Дата обнаружения первого алерта
Имя домена	Домен, с которого пришел алерт
Имя хоста	Хост, с которого выявлен алерт
Пользователь	Имя пользователя в системе
Тип события	Возможные варианты событий приведены в таблице "Event type"

Детали	Подробная информация о событиях

Подробная информация по событию

При нажатии на строку откроется дополнительная информация по событию:

Возможные типы событий

При осуществлении поиска можно выбрать событие определенного типа, задав в поисковой строке следующий запрос: Header.Type: "№", где в качестве № указать один из возможных типов из следующей таблицы.

Типы событий с АРМ

№	Событие	Описание
1	ProcessCreate	создание процесса
2	ProcessExit	завершение процесса
3	ImageLoad	загрузка исполняемого кода (image) в процесс
4	Heartbeat	внутреннее периодическое событие, показатель работоспособности агента с отправкой информации о Windows системе, на которой находится данный агент
5	Flush	внутреннее событие цель которого протолкнуть (гарантировано отправить) все предыдущие события на сервер
6	ThreadCreate	создание потока
9	FileCreate	создание файла
10	FileWrite	модификация содержимого файла
11	FileRename	переименование файла
12	FileDelete	удаление файла
13	FileSetEa	изменение extended attributes файла
14	FileSetBasicInfo	изменение базовой информации о файле
17	FileSetLink	создание ссылки на файл
18	ProcessHandleCreate	создание Windows handle на процесс
19	ProcessHandleDuplicate	создание копии Windows handle на процесс
20	ThreadHandleCreate	создание Windows handle на поток (thread)

№	Событие	Описание
21	ThreadHandleDuplicate	создание копии Windows handle на поток (thread)
22	DesktopHandleCreate	создание Windows handle на рабочий стол Windows (desktop)
23	DesktopHandleDuplicate	создание копии Windows handle на рабочий стол Windows (desktop)
25	NetConnection	NetConnection
26	NetDnsQuery	посылка dns запроса
27	RegCreateKey	создание ключа реестра
28	RegDeleteKey	удаление ключа реестра
29	RegRenameKey	переименование ключа реестра
30	RegSetValueKey	создание или изменение значения ключа реестра
31	RegDeleteValueKey	удаление значения ключа реестра
32	Shutdown	событие о завершении работы системы
33	AvFileDelete	событие об удалении файла антивирусом
34	SessionChange	событие об изменении состояния сессии Windows
35	LogonSessionNew	событие о создании новой logon сессии Windows
36	VolumeChange	событие об изменении состояния file-system volume Windows (например, mount/unmount)
37	DeviceChange	событие об изменении состояния Pnp устройства (device) (arrival/removal)
38	CrashDump	событие о наличии нового дампа ядра на диске (возможно был BSOD)
39	NamedObject	событие о наличии новых именованных (глобальных) events, mutex на системе
40	ProcessExist	событие о наличии процесса, который был запущен раньше EDR
41	FileClose	событие о закрытии файла, соответствует более раннему событию FileCreate или FileWrite (можно связать по EventHeader.ParentEventId)

№	Событие	Описание
42	FILE_OPEN_BLOCKED	событие о попытке открытия заблокированного файла
43	REG_QUERY_VALUE_KEY	
44	REG_OPEN_KEY	
45	FILE_OPEN	событие на открытие и чтение избранных файлов и директорий (регулярки)
46	GET_FILE_INFO	событие на получение информации о файле
47	LOG	логи агента
48	NET_PROCESS_PORT	событие о появлении в системе открытого сетевого порта (bind)

Возможные запросы

В поисковой строке можно использовать следующие типы запросов. В скобках указаны номера type id.

Теги данных с APM

Тип поля	Описание
Заголовки	
Header.AuthenticationId	Идентификатор входа (Logon id)
Header.BootTime	Время с загрузки ОС в 100 наносекундах
Header.DomainName	Название домена
Header.EventId	Идентификатор события в формате Microsoft GUID
Header.HostName	Имя компьютера
Header.ImageFileName	Расположение файла, относящемуся к событию
Header.MachineId	Идентификатор машины
Header.ProcessId	Идентификатор процесса
Header.ProcessUniqueId	UUID процесса - уникальный идентификатор процесса
Header.RequestId	UUID запроса - уникальный идентификатор запроса

Тип поля	**Описание**
Header.SenderIP	IP-адрес отправителя
Header.SessionId	Идентификатор сеанса службы терминалов для связанного процесса
Header.Sid	Идентификатор безопасности (уникальное значение переменной длины, используемое в операционных системах Windows для идентификации участника безопасности или группы безопасности)
Header.ThreadId	Идентификатор потока
Header.ThreadUniqueId	UUID потока - уникальный идентификатор потока
Header.Type	Тип события
Header.UserName	Имя пользователя
Полезная нагрузка	
Payload.AddressFamily	Тип интернет-адреса (IPv4 или IPv6)
Payload.Architecture	Архитектура процессора (CPU): 86 - x86, 64 - x64
Payload.BootTime	Время с загрузки ОС в миллисекундах
Payload.ClientAddress (34)	Адрес (IP) клиента удаленной RDP сессии
Payload.CommandLine (18)	Используемая команда
Payload.Component (47)	Компонент, вызвавший диагностическое сообщение
Payload.CpuNumber (47)	Количество CPU
Payload.DataString (30)	Значение ключа реестра
Payload.DriverVersionVersion (4)	Версия EDR агента
Payload.DstFileName (11)	Конечное расположение файла при переименовании
Payload.FileHash.Sha1	SHA 1 - хеш файла

Тип поля	Описание
Payload.FileId	UUID файла - уникальный идентификатор файла
Payload.FileName	Путь к файлу (его название)
Payload.Function (47)	Системная функция, вызвавшая диагностическое сообщение
Payload.ImageFileHash.Sha1 (1,3,40)	SHA 1 - хеш файла, запустившего службу
Payload.ImageFileName (1,3,6,18)	расположение файла, запустившему службу
Payload.Irql (47)	Уровень запроса прерывания
Payload.KeyName (27,28)	Путь ветки создаваемого, удаляемого либо изменяемого ключа реестра
Payload.LocalAddress (25,26,48)	IP-адрес сетевого интерфейса
Payload.LocalPort (25,26,48)	Порт
Payload.Message (47)	Диагностическое сообщение
Payload.ObjectType (39)	Тип объекта, создавшего Mutex
Payload.ParentImageFileName (1,40)	Расположение файла родительского процесса
Payload.ParentProcessUniqueId (1,40)	UUID родительского процесса - уникальный идентификатор родительского процесса
Payload.ProcessId (1,2,6,18)	идентификатор процесса
Payload.ProcessUniqueId (1,6,18)	UUID процесса - уникальный идентификатор процесса
Payload.Remote (6,34)	В событиях по созданию потока - обозначает, что поток был создан из другого потока. В событиях по сессиям Windows - обозначает локальная это или удаленная сессия
Payload.RemoteAddress (25,26)	IP-адрес машины, на которую происходит обращение

Тип поля	Описание
Payload.RemoteHost (25,26)	Название удаленной машины/ сервера, на которое происходит обращение
Payload.RemotePort (25,26)	Порт, на который происходит обращение
Payload.SrcFileName (11)	Начальное расположение файла, которое мы переименовываем.
Payload.SystemInfo.BiosInfo.BIOSVersion	информация о версии BIOS ПК
Payload.SystemInfo.BiosInfo.Manufacturer	производитель BIOS ПК
Payload.SystemInfo.CpuInfo.CpuList.Name	производитель материнской платы ПК
Payload.SystemInfo.DiskInfo.DiskList.DeviceID	Идентификатор жесткого диска
Payload.SystemInfo.NetInfo.NetworkList.IPAddress	IP-адрес сетевого адаптера
Payload.SystemInfo.NetInfo.NetworkList.Name	Название сетевого адаптера
Payload.ThreadId	ID потока
Payload.Timestamp	Дата и время события
Payload.UserName	Имя пользователя
Payload.Value (30, 31)	Название ключа реестра
Payload.VolumeName	Логическое расположение раздела жесткого диска
company_name	Имя компании. Например, ООО АО «БУДУЩЕЕ»
computer_name	Имя компьютера
event_type	Тип события. Возможные варианты событий приведены в таблице "Event type"
timestamp:	Метка времени

Фильтрацию можно проводить с помощью кнопок: 

Сложные запросы

Для формирования гибких сложных запросов используются логические операции:

- **И**

Используйте символы **&&**

- **ИЛИ**

  Используйте символы **||**

- **НЕ**

  Используйте символы **!**

Помимо данных операндов, возможно формировать запросы с использованием lucene-синтаксиса.

Важные примеры формирования сложных запросов

Отражение специальных символов

Обратите внимание на используемые спец символы при формировании запросов!

Используйте операнд **/** для их отражения.

Список специальных символов:

- **&&**
- **||**
- **!**
- **( )**
- **{ }**
- **[ ]**
- **^**
- **"**
- *****
- **?**
- **:**
- ****

Группировка и использование операндов И, ИЛИ, НЕ

Для формирования запросов с операндами И, ИЛИ, НЕ необходимо обращать внимание на группировку вашего запроса. Ввиду того что система различает запросы типа:

- marker: запрос1 или запрос2

В данном запросе будет осуществлён поиск по marker-у со значением "запрос1", к которому будет добавлен поиск строки "запрос2".

- marker: (запрос1 или запрос2)

В данном запросе будет осуществлён поиск по marker-у со значением "запрос1" или "запрос2".

10.5. Сетевые соединения

В результате анализа трафика, получаемого по SPAN с помощью модуля NTA, существует возможность получить описание всех сетевых сессий - функциональность Threat Hunting. В разделе "Сетевые соединения" приведено описание и результаты сквозного поиска по различным индикаторам анализируемого трафика.

Общие данные

Главное окно интерфейса "Сетевые соединения" содержит в себе следующую информацию (см. изображение Список сетевых соединений).

Информация о поисковой строке содержится в разделе "Управление поисковыми запросами".

Общая информация по сетевым соединениям:

- **Время** - точное время инициации сессии источником;

- **Сенсор** - имя сенсора, задаваемое при создании;
- **Источник** - инициатор сессии;
- **Получатель** - получатель сессии;
- **Протокол** - протокол уровня OSI, за исключением прикладного, используемый в сессии;
- **Получено байт** - количество байт полученных получателем сессии;
- **Отправлено байт** - количество байт отправленных инициатором сессии;
- **Продолжительность** - продолжительность сессии;
- **Сервис** - протоколы прикладного уровня (приложения / сервисы).

Детальное описание сессии

Для отображения детальной информации по определенной сессии, необходимо нажать на нее.

В зависимости от прикладного протокола сессии информация в поле **"Информация о сетевом подключении"** будет различна.

Информация о сетевом подключении (пример для протокола TCP):

- **Источник** - информация о инициирующем оборудовании. Производитель, MAC-адрес, IP-адрес (опционально);
- **Получатель** - информация о принимающем оборудовании. Производитель, MAC-адрес, IP-адрес (опционально);
- **Статус** - статус сессии коротко. При наведении курсора на знак ***i*** отобразится полное описание состояния;
- **Начало** - временная метка инициации сессии;
- **Байты** - суммарное количество переданных байт в обе стороны.

Чтобы поделиться полученной информацией о сетевом соединении, необходимо нажать на кнопку  , после чего ссылка будет скопирована в буфер обмена.

Поле **"Статистика использования функций"** содержит в себе графическую визуализацию используемых функций в пределах одной сессии в процентном соотношении.

- SECURITY - функция из группы security, в данном случае используется для аутентификации на ПЛК
- SETUP_COMMUNICATION - установка соединения протокола s7

используются в 50% соотношении.

Поле **"Запросы"** содержит в себе следующую информацию:

- **Время** - дата и время обнаружения соединения;
- **Функция** - функция, присущая определенному протоколу;
- **Направление** - в данном поле стрелками указано направление запроса:
  - **->** запрос;
  - **<-** ответ;
  - **<->** запрос-ответ

В зависимости от типа сообщения в сетевом соединении, информация предоставляется пользователю в трех основных блоках (в зависимости от соединения некоторые блоки могут отсутствовать):

- Общие данные;

- Заголовки запроса;
- Заголовки ответа.

Переход к разделу "Файлы"

При нажатии на прикрепленный файл в поле **Связанные файлы**, будет осуществлен переход в раздел "Файлы". В данном разделе будет содержаться информация о файле, который передан по данному потоку.

Протоколы

Протоколы, содержащиеся в блоке "Сетевой трафик"

Протокол	Описание
DNS	компьютерная распределённая система для получения информации о доменах. Фильтр позволяет рассмотреть выявленные коммуникации с DNS серверами
FTP	протокол, с помощью которого осуществляется передача файлов по сети
HTTP	протокол прикладного уровня, предназначенный для реализации передачи гипертекста между распределёнными системами
RDP	проприетарный протокол прикладного уровня, использующийся для обеспечения удаленной работы пользователя с сервером, на котором запущен сервис терминальных подключений
SMB	сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
SMTP	простой протокол прикладного уровня, предназначенный для передачи электронной почты — широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP
SSH	сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов)
ICMP	сервисный протокол транспортного уровня, предназначенный для диагностики сетевых устройств
TCP	один из основных протоколов транспортного уровня, предназначенный для управления передачей данных
UDP	простой, ориентированный на дейтаграммы протокол транспортного уровня, предназначенный для передачи данных без организации соединения, предоставляющий быстрое, но необязательно надежное транспортное обслуживание

Протоколы, содержащиеся в блоке "Технологический сегмент"

Протокол	Описание
CIP	общий промышленный протокол, позволяющий создавать единую коммуникационную систему в масштабах как отдельного производственного процесса, так и предприятия в целом. Изначально был представлен ассоциацией ODVA (Open DeviceNet Vendors Association)
DELTAV	промышленный протокол, широко используемый промышленным оборудованием автоматизации производства компании Emerson для реализации коммуникаций в сегменте АСУ ТП
DNP3	промышленный протокол, используемый для передачи данных между компонентами АСУ ТП. Разработан для удобного взаимодействия между различными типами устройств и систем управления. Может применяться на различных уровнях АСУ ТП
IEC104	промышленный протокол передачи данных, реализующий прикладной уровень TCP/IP, широко используемый в технологических сетях объектов электроэнергетики для организации передачи данных между распределительными устройствами, контроллерами телемеханики, РЗА, АИСКУЭ и АРМ оператора
MODBUS	открытый коммуникационный промышленный протокол для машинного взаимодействия, основанный на архитектуре "ведущий — ведомый" (master-slave). Является стандартом де-факто и поддерживается почти всеми производителями промышленного оборудования
OPCDA	фильтр позволяет рассмотреть выявленные коммуникации с устройствами (ПЛК, РСУ, ЧМИ, ЧПУ), реализованные в соответствии со стандартом OPC Data Access
OPCUA	фильтр позволяет рассмотреть выявленные коммуникации, реализованные в соответствии с спецификацией OPC Unified Architecture
S7COMM	промышленный протокол, разработанный компанией Siemens для реализации передачи данных между контроллерами автоматизации, устройствами полевого уровня, периферийными модулями, серверами и АРМ оператора со SCADA
S7COMMPlus	промышленный протокол, являющийся развитием S7COMM и предназначенный для работы нового поколения устройств автоматизации производства компании Siemens
UMAS	промышленный протокол, широко используемый промышленным оборудованием автоматизации производства компании Schneider Electric для реализации коммуникаций в сегменте АСУ ТП. Часто используется для обмена данными по монтажной шине между процессорным модулем контроллера автоматизации и модулями периферии.

Поле	Описание
type:	тип соединения
ts:	время создания запроса
duration:	время ожидания обработки запроса
uid:	идентификатор соединения
id.orig_h:	отправитель
id.orig_p:	порт отправителя
id.resp_h:	получатель
Id.resp_p:	порт получателя
proto:	название протокола
sequence:	идентификатор запрос-ответ
func:	функция
bytes:	количество байтов при передаче

10.6. Отчеты

Раздел предоставляет доступ к результатам формирования отчётов по логам работы системы.

В раздел попадают отчёты, сформированные во всех сопутствующих разделах - содержащих информацию о работе системы.

К таким разделам относятся:

- Алерты
- Письма
- Файлы
- Компьютеры
- События EDR
- Сетевые соединения

Формирование отчётов возможно двумя способами:

1. Прямое формирование отчётов из интересующего раздела
2. Формирование отчётов через раздел "Сохранённые поиски".

Прямое формирование отчетов

Описание

1. Пользователь находится в интересующем его разделе (например, Алерты). Он хочет сформировать отчет по своим алертам, в рамках какого-то критерия (диапазон дат и поисковый запрос).

2. Пользователь определяет критерий: выбирает в календаре диапазон времени и устанавливает поисковый запрос. Например, он выбирает весь период с начала года и запрос `severity > 3`.

3. Получив отфильтрованные алерты, пользователь либо выбирает конкретные алерты, либо выбирает весь поисковый критерий (а не только первой страницы). На панели массовых действий у пользователя появляется кнопка "Сформировать отчет" с выбором формата:

- CSV;
- PDF.

4. Нажав кнопку, пользователь получает уведомление: "Запрос на генерацию отчета отправлен. По готовности он будет доступен в разделе Расследование -> Отчеты" / "The report has been requested. It will be available in Investigation -> Reports section"

5. Если пользователь перейдет в раздел Расследование -> Отчеты, он увидит новую строчку с задачей и ее статусом: Pending, Processing, Done

6. Название репорта составлять так: %КОМПАНИЯ_Раздел_Начало_Конец%, например, "Альфа_Штанг_alerts_2020-03-01_2020-06-01". Если компанией в скоупе несколько, имя компании пропускается. Если диапазон дат не выбран, вместо диапазона вставлять время генерации отчета.

7. По готовности отчета пользователь получит стандартное уведомление на почту о готовности запрошенного отчета.

- При нажатии на кнопку **Проверить количество**, будет реализован автоматический подсчет.
- При нажатии на кнопку **Перейти к результатам**, будет совершен автоматический переход в раздел Алерты.

10.7. Контроллеры

В данном разделе содержится информация по используемым программируемым логическим контроллерам (ПЛК) в инфраструктуре Клиента.

- Имя сенсора - название оборудования;
- MAC - MAC-адрес устройства (ПЛК);
- Вендор - Производитель устройства (ПЛК);
- IP - IP-адрес устройства (ПЛК);
- Модель - Модель устройства (ПЛК)
- Версия - Версия прошивки, установленный в данный момент на устройстве (ПЛК);
- Последнее обновление - Последнее время обнаружения;
- Последняя контрольная сумма - Последнее обнаруженная контрольная сумма программы управления, разработанный на TIA Portal.

При нажатии на строку с интересующим ПЛК, откроется подробная информация по нему.

Пассивное обнаружение

- Время - время обнаружения;
- Исходный IP - источник, от которого пришел запрос;
- Артикул - Идентификатор устройства (Product ID);
- Модель - Модель устройства (ПЛК);
- Версия - версия прошивки, обнаруженный на ПЛК;

- Контрольная сумма - контрольная сумма программы управления, разработанный на TIA Portal.

Настройки активного опроса

Драйвер - выбор протокола:

- s7comm;
- s7commplus;
- modbus;
- umas.

Преиод опроса - интервал времени, через который необходимо опрашивать устройство:

- 10 минут;
- 30 минут;
- 1 час;
- 4 часа;
- 8 часов;
- 24 часа.

Результаты активного сканирования

Данные пункт позволяет отслеживать изменения о контроллерах в сети:

- Время - время обнаружения;
- Исходный IP - источник, от которого пришел запрос;
- Контрольная сумма - контрольная сумма программы управления, разработанный на TIA Portal.

11. Настройки

В данном пункте описан интерфейс XDR Console с функциями по администрированию комплекса. Основные возможные действия при администрировании XDR Console:

- Настройка всех модулей MXDR, подключенных к XDR Console
  При этом информация по настройке конкретных модулей приведена на соответствующих страницах:
  - Настройка модуля XDR
  - Настройка модуля NTA
  - Настройка модуля Sensor Industrial
  - Настройка модуля MDP
  - Настройка модуля EDR
- Определение принадлежности модулей MXDR к одной общей сущности Компания
- Предоставление информации о пользователях MXDR
- Оценка статистики использования лицензий по каждому из модулей MXDR

11.1. Устройства

Пункт **Устройства** служит для предоставления возможности настроек всех компонентов MXDR подключённых к XDR Console.

Доступные компоненты:

- NTA
- Sensor Industrial

- MDP
- XDR Console
- Storage
- EDR
- BEP

Общие данные по устройствам

Доступные данные:

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

Фильтры

Фильтры типов данных

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
  - Sensor Industrial
  - MDP
  - XDR
  - Storage
  - EDR
  - BEP

- **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 - указывает на включенный анализ почтовых сообщений в NTA

- **Компания**
  Фильтрует устройства по привязке к выбранным компаниям.

Строка поиска

Фильтр позволяет производить поиск по частым полям в описании устройств.

11.1.1. Добавить устройство

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

- Тип устройства
  Определяет тип регистрируемого устройства (NTA /Sensor Industrial/ MDP/ BEP).
- Лицензия
  Доступные лицензии зависят от выбранного типа устройства. От типа лицензии зависит производительность зарегистрированного устройства.
- Имя устройства
- Связанное железо(опционально)
  Связывает UID с устройством из тех, что ещё не зарегистрированы на XDR.
- Компания
  Определяет маркировку всех событий от данного устройства к выбранной компании. Позволяет разграничивать выявленные события в разрезе нескольких инсталляций устройств, зарегистрированных на одном XDR Console. (Смотри также разделы "Подразделения" и "Группировка событий по подразделениям")
- Комментарий

При нажатии на кнопку **Создать Устройство** диалоговое окно предложит ввести *мастер пароль* для получения уникального идентификатора (UID) создаваемого устройства (рис.9.1.1.2)

Запросить Подписание подписывает UID 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/Sensor Industrial/ BEP/ MDP - его активации и подключения к XDR.
  Ссылки на активацию по полученному UID:
- Активация сенсора и синхронизация с XDR.

11.2. Компании

XDR Console 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/Sensor Industrial/ BEP/ 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*. Также в разрезе созданной компании может существовать множество Подразделений. Каждое подразделение реализует возможность иерархического разделения данных внутри одной компании. Подробнее см. Подразделения

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
- Пользователи - количество созданных пользователей
- Подразделения - количество подразделений компании

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 

в правом верхнем углу.

Устройства

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

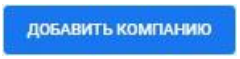
- Название - имя устройства
- Тип - тип компоненты системы (NTA/Sensor Industrial/ BEP/ MDP)
- UUID - идентификатор ключа активации
- Последняя активность - крайняя дата активности системы

Пользователи

Список пользователей, привязанных к компании. Имеется возможность удаления пользователей по клику на кнопку удаления в правом краю строки пользователя. Предоставляется следующая информация по пользователям:

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

Добавление новой компании

Для добавления новой компании нажмите на кнопку 

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)

Архивирование компании

Для архивирования компании выберите её в списке компаний, раскройте полное описание и нажмите кнопку 

Фильтры

Фильтры типов

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

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**
- **Компании / Подразделения**

Фильтры дат и текста

В верхней части списка компаний доступна строка поиска по содержанию полей с дополнительными тегами.

11.3. Пользователи

Данная страница содержит информацию о пользователях, зарегистрированных в системе MXDR, 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 (см. разделы ниже).

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 (просмотр списка пользователей; заведение новых пользователей;

редактирование информации о пользователях, в т.ч. удаление пользователей).
    - Admin - привилегированный пользователь, имеющий права на просмотр списка пользователей только тех компаний, к которым он привязан. А также обладает правами на выполнение любых действий по отношению к пользователям более слабой роли, включающих изменение прав доступа к продукту MXDR, регистрацию и удаление пользователей. В одной организации может быть несколько администраторов.
    - CERT - аналитик, обладает правами просмотра списка всех пользователей. Для пользователей более слабой роли имеет возможность заведения новых пользователей, редактирования информации, а также удаления пользователей.
    - Analyst - аналитик по реагированию и мониторингу на инциденты в пределах закрепленной за ним компании. Доступны действия по изменению информации, заведению и удалению пользователей более слабой роли.
    - User - пользователь системы MXDR, обладающий правами доступа стандартного пользователя. Ему доступны: *Панель управления*, *Алерты*, *Расследование*.
    - Manager - имеет минимальные права доступа: *Панель управления*, *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 также будет использоваться XDR-ом для автоматической рассылки сообщений о статусах алертов.
- Компании - принадлежность пользователя к компании
- Последняя активность - представлены крайние записи активности из пункта **История событий**.

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.

Добавить пользователя

Для добавления нового пользователя в систему MXDR 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.

- 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 MXDR. Используется почта из соответствующего раздела

- Телефон - при происшествии критических инцидентов специалисты SOC АО «БУДУЩЕЕ» дополнительно оповестят пользователя телефонным звонком.

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".

Фильтры

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

- Роль пользователя - позволяет сортировать информацию о пользователях исходя из выбранной роли.
- Состояние пользователя - сортирование информации об активных или удаленных пользователях.
- Компания - позволяет фильтровать пользователей, относящихся к определенной компании.

Роль пользователя:

- owner
- admin
- analyst
- user
- manager
- cert

Состояние пользователя:

- архивные
- активные

Например, данный фильтр позволяет выбрать только активных пользователей с ролью Администратора.

Фильтры дат и текста

В верхней части списка компаний доступна строка поиска по содержанию полей с дополнительными тегами.

11.4. Лицензии

В разделе "Лицензии" после поля "Управление поисковыми запросами" представлена статистика использования лицензий по каждому из продуктов решения MXDR.

Примечание:

За каждым устройством закреплен серийный номер, при этом лицензии выдаются на ПО.

Ниже предоставляется список всех UUID (устройств и используемых лицензий), созданных с момента активации XDR.

Данные по лицензиям

По каждой лицензии доступна следующая информация:

- **Серийный номер**

UUID лицензии. Используется для регистрации и синхронизации новых устройств и ПО (в случае EDR) с XDR.

- **Устройство**

Имя заданное при создании нового устройства.

- **Имя лицензии**

Тип лицензии. Зависит от типа устройства.

- **Статус**
  - Reserved - лицензия создана, подписана. По ней зарегистрировано устройство. Лицензия используется в работе
  - Signed - лицензия создана (подписана), но ещё не используется. По ней возможно зарегистрировать новое устройство на XDR
  - Revoked - лицензия отозвана. Связанное с ней устройство отсоединено от XDR без возможности дальнейшей работы
  - Requested - запрос на отзыв лицензии со стороны подключенных устройств. Устройство будет работать до тех пор, пока лицензия не будет отозвана - перейдёт в статус *revoked*
  - Removed - лицензия удалена
- **Подписан**

Дата выпуска лицензии на XDR

- **Последнее изменение**

Дата последнего изменения статуса лицензия.

При нажатии на конкретное устройства в списке выданных лицензий откроется информация, отображающая:

- Тип лицензии - тип лицензии, используемой для данного устройства;
- Дата окончании - дата истечения срока действия лицензии

Изменение статуса лицензии

Для изменения статуса лицензии необходимо выбрать серийный номер устройства, из имеющегося списка. Для этого необходимо выделить элемент, расположенный слева от серийного номера устройства.

При выборе одного или нескольких устройств появляется возможность изменить статус лицензии, которая будет отображена в верхнем правом углу окна интерфейса XDR:

- **Подписать**

Подписать зарезервированную лицензию. Доступно для лицензий со статусом *Requested*.

- **Отозвать**

Отозвать подписанную лицензию. Устройство, зарегистрированное на XDR по данной лицензии, будет отсоединено.

- **Снятие резервирования**

Снять лицензию с резервирования.

- **Удалить**

Удалить запрос на лицензию. Доступно для лицензий со статусом *Requested*.

Фильтры

По кнопке фильтра  в строке поиска открывается меню фильтрации.

Доступные фильтры:

- **Статус**
  - Requested
  - Signed
  - Reserved
  - Revoked
  - Removed

Фильтры дат и текста

В верхней части списка компаний доступна строка поиска по содержанию полей.

11.4.1. Управление лицензиями подчиненных устройств

В пункте "Лицензии" Вы сможете увидеть выданные Вам лицензии на различные типы устройств, а также статистику по их использованию срокам окончания.

Так, например, у Клиента для использования имеются в распоряжении:

NTA_250 - 10 лицензий;

NTA_1000 - 10 лицензий, одна из которых использована;

MDP_STANDARD - 5 лицензий;

MDP_ENTERPRISE - 5 лицензий, одна из которых также использована.

Чтобы воспользоваться оставшимися в наличии лицензиями, необходимо перейти в раздел "Устройства" и добавить устройство

В появившейся форме необходимо заполнить поля, помеченные *****.

В поле **Лицензии** в выпадающем списке будут представлены доступные для выбранного типа устройства лицензии.

Например, как изображено на - NTA_1000.

В Поле **Дата окончания лицензии** указывается срок действия лицензии, который не может превышать дату окончания лицензии XDR.

Для сохранения настроек необходимо ввести PKI, присвоенный XDR, с которого выполняются настройки

После сохранения настроек данная лицензия будет доступна для активации на устройстве, для которого создавалась лицензия (например, для NTA_1000), при этом счетчик используемых лицензий NTA_1000 увеличится на 1

Продление срока действия лицензии

Если Вам необходимо продлить лицензию на XDR и одно (или несколько) устройств, Вам необходимо обратиться в службу поддержки АО «БУДУЩЕЕ» для продления лицензии XDR.

Важно:

Служба поддержки АО «БУДУЩЕЕ» продлевает лицензию только на XDR. Лицензии на остальные устройства Клиент присваивает и продлевает самостоятельно.

Важно:

Следует заметить, что продлевать лицензию для подчиненных устройств можно на срок, не превышающий дату окончания лицензии XDR.

Изменение типа лицензии

Если Вам потребовалось изменить тип лицензии, например, с NTA_1000 на NTA_250, то Вам не обходимо зайти в раздел "Лицензии" и в списке используемых лицензий выбрать ту, которую необходимо изменить

Нажмите на кнопку редактирования  и в поле **Тип лицензии** выберите доступную. (Например, NTA_250).

Для сохранения настроек необходимо ввести PKI XDR, с которого выполняются настройки.

12. Редактирование настроек модуля XDR Console

На странице представлены общие показатели по работе XDR Console:

Общая информация

- Имя - заданный идентификатор может быть любым
- Номер лицензии - получен при покупке или тестировании решения
- Серийный номер - серийный номер оборудования
- Комментарий
- VPN IP - адрес VPN сервера для коммуникации XDR с подключаемыми модулями
- Внешний IP - адрес управляющего интерфейса
- Компания - задается при создании нового устройства из списка Настройки -> Компании

Состояние устройства

- Последний HeartBeat
- Последнее обновление
- CPU / RAM / HDD
- Дропы в ядре / на интерфейсе
- Последняя активность
- Длительность
- Загрузка канала

Графики состояния устройства

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

Кнопка редактирования базовых свойств  - доступны для редактирования:

- Имя
- Комментарий

Примечание: данная кнопка доступна только для пользователей с типом аккаунта ***owner***.

По кнопке **Редактировать Основные Настройки** доступны расширенные настройки XDR Console.

12.1. Обновления и потоки данных

Данная настройка определяет способ и типы данных, которыми будет обмениваться XDR с инфраструктурой АО «БУДУЩЕЕ».

- **Не обновлять систему**

  Обновление программного обеспечения, IOC-ов и сетевых сигнатур не производится.

  Отсутствует взаимодействие с инфраструктурой АО «БУДУЩЕЕ» SOC.

- **Получать только обновления ПО и правил**

  Обновления сигнатур и IOC, а также обновление ПО комплекса загружаются в автоматическом режиме с сервера АО «БУДУЩЕЕ» по защищенному каналу. В этом режиме отсутствует взаимодействие с инфраструктурой АО «БУДУЩЕЕ» SOC. В данном режиме обновления инициируются XDR Console.

- **Обновления + одностороннее получение TI**

  Обновления сигнатур и ПО загружаются в автоматическом режиме. У пользователя имеется возможность по выбранному индикатору (IP-адрес, доменное имя и т.п.) запросить и получить обогащенный контекст из системы АО «БУДУЩЕЕ» Threat Intelligence. Обмен информацией происходит по защищенным каналам.

  Для XDR необходим доступ до серверов - gateway.mxdr.ru :443/tcp.

  События ИБ и уведомления по ним в АО «БУДУЩЕЕ» SOC не передаются.

  Имеется возможность активации аккаунта удаленной технической поддержки **АО «БУДУЩЕЕ»**.

- **Обновления + Threat Hunting**

  Система работает в полнофункциональном режиме. Автоматически загружаются обновления сигнатур и ПО. XDR автоматически получает информацию из системы АО «БУДУЩЕЕ» Threat Intelligence, поэтому имеется возможность осуществлять Threat Hunting. События ИБ передаются в АО «БУДУЩЕЕ» SOC и пользователь системы может получать поддержку от экспертов АО «БУДУЩЕЕ» CERT в режиме 24/7. Все данные передаются по защищенным каналам.

  Для XDR необходим доступ до серверов - gateway.mxdr.ru :443/tcp. Существует возможность активации аккаунта удаленной технической поддержки **АО «БУДУЩЕЕ»**.

12.2. Интеграция XDR Console с MDP

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

Интеграции

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

Использование облачного MDP

Для использования MDP Cloud (облачной версии MDP) используется одна из следующих записей:

http://command-server.tds/MDP_cloud

10.144.178.1:3000

12.3. Управление интеграцией с LDAP

В данном пункте осуществляется настройка управления интеграции с LDAP.

В настоящей настройке производится упрощённая интеграция со службой внешних каталогов. Может быть задействована любая служба, поддерживающая LDAP протокол. После интеграции при попытках входа пользователей в систему XDR будет осуществлять запрос в службу каталогов на предмет существования данного клиента в базе. Вход будет осуществлён только в случае наличия, указанного при аутентификации пользователя в базе LDAP.

При этом проверяется пароль и логин. Пароль должен быть от учетной записи в LDAP.

Для настройки интеграции достаточно указать адреса LDAP серверов, чтобы использовать их в качестве источника аутентификации.

Для добавления адреса LDAP сервера нажмите на кнопку	
Для сохранения данных нажмите	
Для отмены ранее введенных данных нажмите	
Для сохранения настроек функции "Управление интеграцией с LDAP" нажмите на кнопку	
Для удаления настроек функции "Управление интеграцией с LDAP" нажмите на кнопку	

12.4. 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. Также возможно выбрать прокси без авторизации.

- Задайте логин и пароль при выборе базовой или NTLM аутентификации.

12.5. 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.

12.6. Сертификат web-сервера

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

Имя Домена Определяет полное DNS имя сервера XDR Console для домена которого выписан сертификат.

12.7. Настройки почтового сервера

Данная настройка задаёт почтовый сервер и аккаунт для рассылки сообщений для аналитиков комплекса.

Рассылка осуществляется индивидуально по сработанным инцидентам. Рассылка настраивается в соответствующих настройках аккаунта пользователей в разделе "Пользователи"

12.8. SNMP-мониторинг XDR

Настройка позволяет обеспечивать мониторинг состояния оборудования, а также мониторинг статистических данных используемых модулей в XDR Console. Поддерживаемые версии протокола SNMP:

- SNMPv1
- SNMPv2
- SNMPv3

При выборе версии протокола появляется возможность задать дополнительные параметры, специфичные для выбранного протокола.

SNMPv1

Доступные настройки:

- Адрес сервера
- Порт
- Временной период
- Версия протокола
- Community Data

SNMPv2

Доступные настройки:

- Адрес сервера
- Порт
- Временной период
- Версия протокола
- Имя пользователя
- Протокол авторизации:

    - None
    - MD5
    - SHA
    - SHA224
    - SHA256
    - SHA384
    - SHA512
- Ключ авторизации

SNMPv3

Доступные настройки:

- Адрес сервера
- Порт
- Имя пользователя
- Протокол авторизации:
    - None
    - MD5
    - SHA
    - SHA224
    - SHA256
    - SHA384
    - SHA512
- Ключ авторизации
- Протокол шифрования:
    - None
    - DES
    - 3DES
    - AES128
    - AES192
    - AES256
- Ключ шифрования

12.9. 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 *Behaviour Inspection & Host Forensics*

12.10. Сброс мастер-пароля

При утере мастер пароля возможно сбросить главный ключ и запустить процесс генерации PKI заново. Для этого нажмите на кнопку **Сбросить PKI**.

13. Редактирование настроек модуля NTA

Расположение: UI -> Настройки -> Устройства -> *в списке устройств выбрать необходимый* 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

- Имя - заданный идентификатор может быть любым
- Номер лицензии - получен при покупке или тестировании решения
- Серийный номер - серийный номер оборудования
- Комментарий
- VPN IP - адрес внутри VPN туннеля получаемый при подключении NTA к XDR Console для управляющих коммуникаций
- Внешний IP - адрес управляющего интерфейса, выданный на стороне клиента (через DHCP или статическими правилами)
- Компания - задаются при создании нового устройства из списка Настройки -> Компании
- Скрыть от CERT -свойство сенсора, скрывающее его события из выдачи для мониторинга пользователям с ролью CERT

Состояние устройства

- Последний HeartBeat - последний замеченный heartbeat с данного устройства
- Последнее обновление - дата последнего обновления
- CPU / RAM / HDD
- Дропы в ядре / на интерфейсе
- Последняя активность - крайнее время активности VPN между сенсором и управляющим XDR
- Длительность - временной отрезок, в течение которого между сенсором и XDR был установлен управляющий VPN канал. Отчитывается с момента последней потери связи между устройствами
- Загрузка канала

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

Кнопка редактирования базовых свойств  - доступны для редактирования:

- Имя
- Комментарий
- Скрыть от CERT

Примечание: данная кнопка доступна только для пользователей с типом аккаунта ***owner***.

Кнопка **Редактировать настройки** открывает раздел конфигурации устройства, который разделен на следующие разделы:

При нажатии на кнопку **Управление лицензией** (позволяет изменить лицензию для выбранного устройства) происходит автоматический переход в раздел Лицензии.

13.1. Блок «Общие настройки»

Данный блок содержит в себе набор функций, позволяющих: связывать NTA с устройствами поведенческого анализа (MDP, MDP Cloud), создавать белые списки индикаторов для исключения из анализа, создавать правила по разрешению сетевых адресов в доменные и сетевые имена, передавать регистрируемые события во внешние системы через Syslog, изменять синхронизацию времени устройства с XDR, настраивать функции для мониторинга работы и состояния устройства.

13.1.1. Группировка событий по подразделениям

Данная настройка позволяет разделить события и алерты внутри одной инсталляции, в разрезе одной Компании. Таким образом возможно разделять обработку инцидентов внутри одной компании между аналитиками ответственными за различные подразделения.

Из меню **Подразделение** возможно выбрать как подразделение, так и саму компанию. Видимость компаний XDR Console зависит от привязки выбранного сенсора к Компании на стадии регистрации (создания) устройства (см. Добавить Устройство).

После выбора подразделения станет доступно меню группировки данных по сетевым адресам и почтовым адресам (см рис. "Разделение данных по подразделению).

- **IP-адреса**

Позволяет ввести сетевые адреса в форматах CIDR. В данном разделе необходимо вводить адреса из диапазона Homenet адресов. Homenet диапазон задаётся в процессе настройки сигнатурного анализа трафика в разделе "Анализ сетевого трафика"

- **Почтовый адрес**

Позволяет ввести адреса или домены почтовых адресов. В данном разделе необходимо вводить адреса целевых получателей, то есть внутренние для клиента.
Изменения вступают в силу сразу после сохранения. События, предшествующие по датам данным изменениям, не будут промаркированы новым подразделением.

13.1.2. 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 одна из следующих записей:

10.144.178.1:3000

13.1.3. 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 высокого качества обнаружения атак.

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.

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 .*

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.

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

13.1.4. Настройки управления Mediator /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.

13.1.5. Экспорт данных

При установке MXDR важно организовывать обновления эксплуатируемых устройств и сбор регистрируемых событий.

При необходимости функция мониторинга состояния систем может быть возложена на Пользователя. Для этого реализована возможность интеграции с различными SIEM-системами. Данная процедура осуществляется с помощью передачи хартбитов через syslog.

По умолчанию логи работы NTA отправляются и хранятся в XDR Console и SOC АО «БУДУЩЕЕ» (***в зависимости от заданного режима работы XDR Console***). 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 возможно интегрировать MXDR 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.

Система MXDR может детектировать события четырех различных категорий:

- Сигнатурные события (на основе анализа трафика)
- Сетевые аномалии
- События о вредоносных файлах (полученные от модуля MDP)
- Сообщения самодиагностики (хартбиты)

События в формате JSON

Сигнатурные события в формате JSON

Описание возможных полей при получении сигнатурных событий в формате JSON представлено в таблице ниже.

Поле	**Описание**
timestamp	*Дата и время события*
flow_id	*Идентификатор потока данных*
event_type	*Тип события*
src_ip	*IP источника*
src_port	*Порт источника*
dest_ip	*IP назначения*
dest_port	*Порт назначения*
proto	*Протокол*
gid	*ID генератора сигнатуры*
signature_id	*Идентификатор сигнатуры*
rev	*Номер ревизии сигнатуры*
signature	*Название сигнатуры*
category	*Категория угрозы*
severity	*Уровень угрозы*
hostname	*Доменное имя*
url	*Адрес страницы*
http_user_agent	*Приложение*
http_content_type	*Тип контента*
http_refer	*URL источника запроса*
http_method	*Метод запроса*
protocol	*Протокол*
status	*Статус*
length	*Длина*

Пример сообщения с сигнатурным событием в формате JSON:

```
{
  "timestamp":"2016-06-30T13:51:28.033623+0300",
  "flow_id":2065914546,
  "event_type":"alert",
  "src_ip":"10.5.0.157",
  "src_port":64464,
  "dest_ip":"136.243.81.198",
  "dest_port":80,
  "proto":"TCP",
  "tx_id":0,
  "alert":{
    "action":"allowed",
    "gid":1,
    "signature_id":2808364,
"rev":3,
    "signature":"MALWARE CheatEngine.AF Variant Checkin",
    "category":"unwanted-software",
    "severity":1
  },
  "http":{
    "hostname":"mobred.net",
    "url":"\/red.php?s=1623677220",
    "http_user_agent":"Mozilla\/5.0 (Windows NT 6.3; WOW64) AppleWebKit\/537.36
(KHTML, like Gecko) Chrome\/51.0.2704.103 Safari\/537.36",
    "http_content_type":"text\/javascript",
    "http_refer":"http:\/\/kinofilmi-online.net\/ekipazh\/",
    "http_method":"GET",
    "protocol":"HTTP\/1.1",
    "status":200,
    "length":50
  },
"payload":"R0VUIC9yZWQucGhwP3M9MTYyMzY3NzIyMCBIVFRQLzEuMQ0KSG9zdD
ogbW9icmVkLm5ldA0KQ29ubmVjdGlvbjoga2VlcC1hbGl2ZQ0KVXNlci1BZ2VudDogTW96aWxs
YS81LjAgKFdpbmRvd3MgTlQgNi4zOyBXT1c2NCkgQXBwbGVXZWJLaXQvNTM3LjM2IChLSF
RNTCwgbGlrZSBHZWNrbykgQ2hyb21lLzUxLjAuMjcwNC4xMDMgU2FmYXJpLzUzNy4zNg0K
QWNjZXB0OiAqLyoNClJlZmVyZXI6IGh0dHA6Ly9raW5vZmlsbWktb25saW5lLm5ldC9la2lwYXp
oLw0KQWNjZXB0LUVuY29kaW5nOiBnemlwLCBkZWZsYXRlLCBzZGNoDQpBY2NlcHQtTGFu
Z3VhZ2U6IHJ1LVJVLHJ1O3E9MC44LGVuLVVTO3E9MC42LGVuO3E9MC40DQpDb29raWU6
IFBIUFNFU1NJRD1ja3JsMzJtaWplbjl2bWNtYTRzbGNiMTl1Nw0KDQo=",
  "payload_printable":"GET \/red.php?s=1623677220 HTTP\/1.1\r\nHost:
mobred.net\r\nConnection: keep-alive\r\nUser-Agent: Mozilla\/5.0 (Windows NT 6.3; WOW64)
AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/51.0.2704.103 Safari\/537.36\r\nAccept:
*\/*\r\nReferer: http:\/\/kinofilmi-online.net\/ekipazh\/\r\nAccept-Encoding: gzip, deflate,
sdch\r\nAccept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4\r\nCookie:
PHPSESSID=ckrl32mijen9vmcma4slcb19u7\r\n\r\n",
  "stream":1,
  "packet":"uK9nHtAHrPLFETTqCABFAAAozTpFAAAoCjqI81EGCgUKBQCdiPNRxvvQ
AFAAAAAAcO9SJgAAAAAAAAAA"
}
```

Сетевые аномалии в формате JSON

Описание возможных полей при получении сообщения в формате JSON о сетевых аномалиях представлено в таблице ниже.

Поле	Описание
confidence	*Вероятность вредоносности*
src_port	*Порт источника*
classifier_version	*Версия классификатора*
domain_len	*Длина домена*
ts	*Дата и время события*
src_ip	*IP источника*
domain_idn	*Идентификатор домена*
dst_port	*Порт назначения*
dst_ip	*IP назначения*
msg	*Сообщение*
query	*Web-запрос*
domain_lvl	*Уровень домена*

Пример сообщения о сетевой аномалии в формате JSON:


```
{
   "confidence": "93.57",
   "src_port": "56147/udp",
   "classifier_version": "cf18209f902e244f44a7b510c25b5241b178673a-764c6c-2424",
   "domain_len": 9,
   "ts": 1486386430.751216,
   "src_ip": "10.0.0.2",
   "domain_idn": false,
   "dst_port": "53/udp",
   "dst_ip": "77.88.8.8",
   "msg": "DGA detected by XGB",
   "query": "ruwufluhg.top",
   "domain_lvl": 2
}
```


События о вредоносных файлах в формате JSON

Описание возможных полей при получении сообщения в формате JSON о вредоносных файлах представлено в таблице ниже.

Поле	Описание
sha256	*Контрольная сумма sha25*
sha1	*Контрольная сумма sha1*
filename	*Имя файла*
from	*Отправитель*
event_type	*Тип события*
timestamp	*Дата и время события*
md5	*Контрольная сумма MD5*
to	*Получатель*
probability	*Вероятность вредоносности*

Пример сообщения о вредоносном файле в формате JSON:


```
{
    "sha256":"c90c7c55be28436302c037a1215cb161dc6ff7eff029117122dd48cc833b8ce
6",
   "sha1":"16b1fc6af3901de3802af9643defb06e1d4f9de1",
   "filename":"VM576507_20170802.zip",
   "from":"MSVoice@irk.rshb.ru",
   "event_type":"MDP_alert",
   "timestamp":"2017-08-02T08:24:31.925799",
   "md5":"beefcca95f9b774a27c75d77c6897790",
   "to":[
      "director@irk.rshb.ru"
   ],
   "probability":67.60000000000001
}
```


Сообщения самодиагностики в формате JSON

Описание возможных полей при получении хартбитов в формате JSON представлено в таблице ниже.

Поле	Описание
host	*Идентификатор сенсора*
timestamp	*Время в UTC*
time_delta	*Время в секундах после последнего измерения*
ifaces_packets_delta	*Увеличение счетчика поступивших на интерфейс пакетов*

krnl_packets_delta	*Увеличение счетчика пакетов в kernel space*
ifaces_bytes_delta	*Увеличения счетчика RX-байт на интерфейсе*
vmmem_used	*Выделено виртуальной памяти (в байтах)*
vmmem_free	*Свободно виртуальной памяти (в байтах)*
swapm_free	*Свободно в свопе (в байтах)*
swapm_used	*Выделено в свопе (в байтах)*
disk_free	*Свободно в дисковой системе*
disk_used	*Занято в дисковой системе*
cpu_percent	*Средняя загрузка CPU по ядрам*
kernel_version	*Версия ядра*
bios_version	*Версия BIOS*
uptime	*Uptime устройства*

Пример хартбитов в формате JSON:


```
{
  "host":"kpx37lnychxz7lhw",
  "timestamp":"2017-10-04T16:13:40.158688",
  "time_delta":301.177393,
  "ifaces_packets_delta":4646238,
  "krnl_packets_delta":4660719,
  "ifaces_bytes_delta":3489196566,
  "vmmem_used":8569155584,
  "vmmem_free":24991760384,
  "swapm_free":4198846464,
  "swapm_used":83533824,
  "disk_free":816764354560,
  "disk_used":113368637440,
  "cpu_percent":8.4,
  "kernel_version":"4.4.0-45-generic",
  "bios_version":"2.0.8",
  "uptime":"16 weeks, 51 minutes"
}
```


События в формате CEF

Сигнатурные события в формате CEF

Описание возможных полей при получении сигнатурных событий в формате CEF представлено в таблице ниже.

Поле	Описание
proto	*Протокол*
start	*Дата и время события*
src	*IP источника*
spt	*Порт источника*
dst	*IP назначения*
dpt	*Порт назначения*
cat	*Категория угрозы*
dhost	*Доменное имя*
request	*Адрес страницы*
requestMethod	*Метод запроса*
app	*Протокол*
reason	*Статус*

Пример сообщения с сигнатурным событием в формате CEF:

CEF:0|Group-ib|Bot-Trek TDS|1.0|2808364|MALWARE CheatEngine.AF Variant Checkin|Low|proto=TCP start=Jun 30 2016 13:51:28 src=10.5.0.157 spt=64464 dst=136.243.81.198 dpt=80 cat=unwanted-software dhost=mobred.net request=/red.php?s=1623677220 requestMethod=GET app=HTTP/1.1 reason=200 requestClientApplication=Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36

Сетевые аномалии в формате CEF

Описание возможных полей при получении сообщения в формате CEF о сетевых аномалиях представлено в таблице ниже.

Поле	Описание
src	*IP-адрес источника файла для события, связанного с протоколами HTTP, FTP*
dst	*IP-адрес получателя файла для события, связанного с протоколами HTTP, FTP*
destinationDnsDomain	*Web-запрос*
rt	*Время события в UTC*

Пример сообщения о сетевой аномалии в формате CEF:

CEF:0|Group-IB|TDS|1.0|0|DGA Alert|3|src=10.3.0.214 dst=10.0.0.2 destinationDnsDomain=ruwufluhg.top rt=2017-08-22T13:20:18

События о вредоносных файлах в формате CEF

Описание возможных полей при получении сообщения в формате CEF о вредоносных файлах представлено в таблице ниже.

Поле	Описание
duser	*Получатель письма для события, связанного с электронной почтой*
suser	*Отправитель письма для события, связанного с электронной почтой*
src	*IP-адрес источника файла для события, связанного с протоколами HTTP, FTP*
dst	*IP-адрес получателя файла для события, связанного с протоколами HTTP, FTP*
fileHash	*SHA 1 -хеш файла*
rt	*Время события в UTC*
fname	*Имя файла*

Сообщения самодиагностики в формате CEF

Описание возможных полей при получении хартбитов в формате CEF представлено в таблице ниже.

Поле	Описание
duser	*Получатель письма для события, связанного с электронной почтой*
suser	*Отправитель письма для события, связанного с электронной почтой*
src	*IP-адрес источника файла для события, связанного с протоколами HTTP, FTP*
dst	*IP-адрес получателя файла для события, связанного с протоколами HTTP, FTP*
fileHash	*SHA 1 -хеш файла*
rt	*Время события в UTC*
fname	*Имя файла*

13.1.6. Сервер времени

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.

13.1.7. SNMP-мониторинг

Настройка позволяет обеспечивать мониторинг состояния оборудования, а также мониторинг статистических данных используемых модулей в MXDR.

Поддерживаемые версии протокола SNMP:

- SNMPv1
- SNMPv2
- SNMPv3

При выборе версии протокола появляется возможность задать дополнительные параметры - специфичные для выбранного протокола.

SNMPv1

Доступные настройки:

- Адрес сервера
- Порт
- Community Data

SNMPv2

Доступные настройки:

- Адрес сервера
- Порт
- Имя пользователя
- Протокол авторизации:
  - None
  - MD5
  - SHA
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Ключ авторизации

SNMPv3

Доступные настройки:

- Адрес сервера
- Порт
- Имя пользователя
- Протокол авторизации:
  - None
  - MD5
  - SHA
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Ключ авторизации
- Протокол шифрования:
  - None
  - DES
  - 3DES
  - AES128
  - AES192
  - AES256
- Ключ шифрования

13.2. Блок «Сетевой трафик»

Данный блок содержит в себе набор функций, позволяющих: собирать метаинформацию о сетевых соединениях по протоколам уровня L7 (за исключением технологических протоколов); анализировать web-трафик, получаемый от прокси-серверов компании через ICAP; настраивать модуль сигнатурного анализа трафика; управлять загружаемыми файлами с сигнатурами на сетевой трафик; загружать специфичные для NTA правила анализа сетевого трафика.

13.2.1. Сбор метаинформации о сетевых соединениях

Для обеспечения безопасности работы коммерческих сетей необходимо осуществлять контроль данных, передаваемых посредством протоколов передачи данных. Изначально переключатель для каждого модуля включен.

Протоколы L7

При включении L7 протокола система будет производить запись метаинформации о сессиях с использованием данного протокола. Таким образом возможно восстанавливать данные сессии, анализировать и ассоциировать их с файлами, передаваемыми в данных сессиях.

Подробная информация будет отображена в пункте "Сетевые соединения"

Логирование неизвестных соединений

Для логирования сессий с использованием нестандартных портов и протоколов необходимо активировать требуемые протоколы UDP, TCP или ICMP. Таким образом все сессии, не попадающие под стандартно используемые протоколы седьмого уровня модели OSI будут логироваться и размещаться в разделе Сетевые соединения".

13.2.2. 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.

13.2.3. Анализ сетевого трафика

Важнейший раздел при настройке сигнатурного анализа.

Настройки раздела позволяют системе дифференцировать зловредный трафик относительно легитимного. Позволяет указать локальные интерфейсы, а также интерфейсы для SPAN/RSAN/SPANinGRE.

Разделён на два подраздела.

Анализ сетевого трафика

Позволяет явно указать локальные адреса, сети / подсети, а также адреса локальных Proxy. Данный список определяет так называемую домашнюю сеть (Homenet) для сигнатурного анализа трафика. Выбор Homenet важен для группировки событий по подразделениям

Введите список локальных подсетей и исключите из них адреса Proxy-серверов (используйте знак отрицания - пример:!proxy-ip/32).
Это позволит различать взаимодействия целевых хостов, сетей / подсетей с открытой сетью Интернет.

Интерфейсы для анализа трафика

- **Интерфейс**
  Имена интерфейсов
- **Текущая нагрузка**

Это поток трафика, который подается на конкретный интерфейс - без учёта того анализируется данный трафик или нет.

- **BPF**
  Фильтр BPF для анализа трафика по сигнатурным правилам.
- **On/Off**
- **Число тредов**

Установленное число потоков для каждого процесса сигнатурного анализа SPAN трафика на выбранном интерфейсе. (по умолчанию задано рекомендуемое значение. *Изменение значения может повлиять на производительность системы!*)

13.2.4. Сетевые сигнатуры

В настройке представлен список подклассов сигнатур, с возможностью выборочного отключения или включения определенных подклассов.

Примечание:
Включение новых правил, как и загрузка новых пользовательских правил анализа трафика, может приводить к снижению работоспособности устройства. Меняя перечень активных правил и загружая новые пользовательские правила, всегда взвешивайте работоспособность устройства в части параметра "Дропы в ядре".Сенсоры протестированы на поддержку номинальной полосы пропускания только при условии использования конфига по умолчанию.

Ниже приведен список возможных сигнатур.

- Целевые атаки ;
- Уязвимости в серверном ПО;
- Уязвимости прикладного ПО;
- Бэкдоры и нелегальные средства удаленного управления;
- Банковские трояны;
- Мобильные трояны;
- Неспецифичная активность троянов;
- Drive-by атаки;
- Подозрительные события;
- Фишинговые ресурсы;
- Нарушение политик;
- Нежелательное ПО;
- Троян-вымогатель;
- Исследование сетевого периметра;
- Шпионское ПО.

13.2.5. Пользовательские сетевые сигнатуры

Загрузка пользовательских сигнатур в формате Suricata.

Примечание: ID пользовательских сигнатур должны быть в пределах 1300001 - 1500000.

13.3. Блок «Почта»

Данный блок содержит в себе набор функций, позволяющих: осуществлять настройку почтового клиента для скачивания писем на анализ по протоколам POP3/IMAP; управлять функцией SMTP-сервера в части получения и роутинга почты; определять поведение системы (из предлагаемого списка) в отношении работы со ссылками в письмах; настраивать параметры уведомления о заблокированных сообщениях.

13.3.1. 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 течение которого почтовые сообщения будут храниться на NTA для ретроспективного анализа почтовых сообщений и вложений в них.

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.

Для анализа почтовых сообщений по протоколу POP3/IMAP перейдите в раздел настройки "Почтовый клиент"

Дополнительная информация по режиму работы представлена в разделе "Интеграция по SMTP"

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 MXDR 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.

Более подробно об инфраструктурных требованиях можно почерпнуть в разделе "Интеграция inline (MTA)"

13.3.2. 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.

13.3.3. 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.

- **Прокси сервер**

Позволяет задать прокси сервер для обеспечения web доступа сенсора при анализе ссылок в почтовых сообщениях и вложенных в них документах.

Примечание!

Для использования прямого взаимодействия сенсора через интерфейс управления с Интернет оставьте данное поле пустым.

После выбранной стратегии необходимо сохранить настройки.

13.3.4. Уведомления о заблокированных письмах

Настройка позволяет задать собственный шаблон отсылаемых информационных сообщений о факте блокировки письма.

13.4. Блок «Файлы»

Данный блок содержит в себе набор функций, позволяющих: управлять анализом и извлечением файлов из трафика, подключать общие папки для анализа файлов, а также настраивать общие ресурсы для сбора и анализа файлов.

13.4.1. 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 файлов или почтовых сообщений.

BPF для захвата трафика

BPF фильтр - это open-source проект позволяющий задавать фильтры извлечения данных из анализируемого трафика.

Фильтры действуют по принципу **white list** списка.

Протоколы

Переключатели активируют предустановленные BPF фильтры для анализа файлов из указанных протоколов.

- **SMTP/POP3**

  Данный переключатель активирует функциональность по анализу почтовых сообщений в отсутствие возможности полноценной почтовой интеграции. *Обратите внимание: при реализации полноценной почтовой интеграции данную функцию необходимо отключить*
- **HTTP**

  Восстанавливает из SPAN сессий файлы, передаваемые протоколом http (обычно при скачивании из сети Интернет)
- **FTP/SMB**

  Восстанавливает из SPAN сессий файлы, передаваемые при работе с файловыми хранилищами.

13.4.2. Монтирование и анализ общих ресурсов

Настройка анализа файлов в сетевых папках осуществляется в два этапа:

- Монтирование общих ресурсов
- Анализ общих ресурсов

Монтирование общих ресурсов

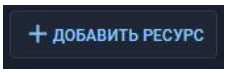
Расположение: UI -> Настройки -> Устройства -> *в списке устройств выбрать необходимый* NTA -> Блок "Файлы" -> Монтирование общих ресурсов.

В разделе "Монтирование общих ресурсов" выполняется только подключение папок для дальнейшего анализа.

Чтобы добавить папки для подключения к общей сетевой папке NTA необходимо нажать на кнопку **Добавить ресурс** и заполнить следующие поля:

- Название - наименование папки, присвоенное пользователем, которое будет отображаться разделе "Анализ общих ресурсов"

- Тип ресурса - протокол, по которому будет проходить соединение с ресурсом (SMB, WebDAV, NFS, FTP)
- Адрес - расположение ресурса
- Логин - логин для подключения к выбранному ресурсу
- Пароль - пароль для подключения к выбранному ресурсу
- Статус - состояние подключения к выбранному ресурсу

Для добавления нового ресурса нажмите кнопку	
Для редактирования существующей записи нажмите кнопку	
Для удаления существующего ресурса нажмите кнопку	
После этого проверьте введённые данные и нажмите кнопку **Сохранить**	
В случае успешного подключения ресурса, в колонке Статус появится значок	

Анализ общих ресурсов

Расположение: UI -> Настройки -> Устройства -> *в списке устройств выбрать необходимый* NTA > Блок "Файлы" > Анализ общих ресурсов

В разделе "Анализ общих ресурсов" осуществляется настройка режима обработки уже подключенных в разделе "Монтирование общих ресурсов" файловых ресурсов для сбора и анализа файлов.

Чтобы начать анализ ресурсов, необходимо нажать на кнопку **Добавить ресурс** и заполнить следующие поля:

- Имя - наименование ресурса из списка смонтированных
- Путь анализа - указываем путь относительно указанного в разделе "Монтирование общих ресурсов" (путь до дополнительного элемента в папке)
- Время анализа - временная метка создания или модификации файла, начиная с которой будет производиться анализ
- Период анализа - периодичность, с которой производится проверка ресурса на появление новых файлов
- Игнорировать скрытые - не проверять скрытые файлы
- Первичный анализ - проверить все существующие на момент включения анализа файлы
- Режим - режим работы:
    - *Анализ* - режим мониторинга, при котором только выдаётся алерт на вредоносные файлы. Файл остаётся в папке неизменным.
    - *Удаление* - режим мониторинга с блокировкой. Вредоносные файлы помещаются в карантин.

- *Перемещение* - режим работы с двумя папками. Вредоносные файлы помещаются в карантин. Проверенные безопасные файлы перемещаются в указанную папку.

При выборе режима работы *"Перемещение"* будут доступны следующие поля:

- Место назначения - наименование папки, созданной в разделе "Монтирование общих ресурсов", в которую будут перемещаться проанализированные безопасные файлы
- Путь назначения - относительный путь внутри папки, в которую будут перемещаться проанализированные безопасные файлы.

После того, как все необходимые параметры заданы, нажмите кнопку **Сохранить**

13.5. Блок «Интеллектуальный анализ трафика»

Данный блок содержит в себе набор функций, позволяющих: выявлять взаимодействия с управляющими серверами через DGA, а также управлять модулем выявления туннелей в верхнеуровневых протоколах.

13.5.1. Модуль выявления DGA-коммуникаций

Настройка позволяет выявлять взаимодействия с управляющими серверами через DGA.

Для того чтобы запустить процесс, необходимо заполнить поля:

- **Порог обращений**

Количество DGA запросов для порождения одного события безопасности.

- **Порог секунд**

Время, за которое учитываются DGA запросы в количестве, заданном в пороге обращений.

После того как поля будут заполнены, нажмите на кнопку **Сохранить.**

13.5.2. Выявление туннелей

Переключатель «Выявление туннелей» предназначен для управления верхнеуровневыми протоколами:

- UDP
- TCP
- DNS
- SSL
- HTTP

При обнаружении в сети соединений, создаваемых разными фреймворками (meterpreter, dnscat, assitsov и т.п.) автоматически создается алерт, который будет отображен в пункте "Алерты"

Для настройки управления модулем выявления туннелей в верхнеуровневых протоколах необходимо включить/выключить переключатель, затем нажать кнопку **Сохранить**.

13.5.3. Выявление скрытых каналов и горизонтального перемещения

В блоке "Интеллектуальный анализ трафика" настройка "Выявление скрытых каналов и горизонтального перемещения" представляет собой модуль для выявления распространения угроз во внутренней инфраструктуре.

Логика обработки

Используются ML классификаторы.

NTA анализирует kerberos(update), smb, ntlm, dce-rpc протоколы на предмет обращения к файловым хранилищам администратора, записи на них файлов, использования wmi и т.п.

В зависимости от выбранной чувствительности алгоритм на основе совокупности индикаторов, описанных выше, создаёт события и алерты.

По умолчанию весь трафик, настроенный на обработку в пункте "Анализ сетевого трафика" подпадает под классификатор "Выявление скрытых каналов и горизонтального перемещения" сразу после включения описываемого функционала.

Для исключения лишних сетевых потоков необходимо воспользоваться белыми списками (настройка ниже).

Настройка выявления скрытых каналов и горизонтального перемещения

Чувствительность

В поле **Чувствительность** - выбирается степень чувствительности классификатора при выставлении алерта. Чувствительность - это отсечка по разнообразию и количеству анализируемых событий от одной машины за 10 минут, в течении которых определяется злоумышленное поведение. При этом в случае выявления числа событий, переходящих определённый порог злоумышленное поведение может быть определено в более короткие периоды.

Белый список

Для добавления IP-адреса в белый список, необходимо нажать на кнопку 

, заполнить появившееся поле и сохранить настройки. По мимо непосредственно IP адреса возможно задать направление анализируемого потока для исключения из анализа. Таким образом возможно эффективно использовать ресурсы NTA, уменьшается количество false-positive алертов, а также позволяет целенаправленно обнаружить факты выявления скрытых каналов и горизонтальных перемещений, проводимых в нужном направлении.

Если необходимо изменить настройки детектирования для уже имеющегося IP-адреса, то его можно найти в строке поиска 

14. Редактирование настроек модуля Sensor Industrial

14.1. Блок «Общие настройки»

Данный блок содержит в себе набор функций, позволяющих: связывать Sensor Industrial с устройствами поведенческого анализа (MDP, MDP Cloud), создавать белые списки индикаторов для исключения из анализа, создавать правила по разрешению сетевых адресов в доменные и сетевые имена, передавать регистрируемые события во

внешние системы через Syslog, изменять синхронизацию времени устройства с XDR, настраивать функции для мониторинга работы и состояния устройства.

14.1.1. Группировка событий по подразделениям

Данная настройка позволяет разделить события и алерты внутри одной инсталляции, в разрезе одной Компании. Таким образом возможно разделять обработку инцидентов внутри одной компании между аналитиками ответственными за различные подразделения.

Из меню **Подразделение** возможно выбрать как подразделение, так и саму компанию. Видимость компаний XDR Console зависит от привязки выбранного сенсора к Компании на стадии регистрации (создания) устройства (см. Добавить Устройство).

После выбора подразделения станет доступно меню группировки данных по сетевым адресам и почтовым адресам (см рис. "Разделение данных по подразделению).

- **IP-адреса**

Позволяет ввести сетевые адреса в форматах CIDR. В данном разделе необходимо вводить адреса из диапазона Homenet адресов. Homenet диапазон задаётся в процессе настройки сигнатурного анализа трафика в разделе "Анализ сетевого трафика"

- **Почтовый адрес**

Позволяет ввести адреса или домены почтовых адресов. В данном разделе необходимо вводить адреса целевых получателей, то есть внутренние для клиента.

Изменения вступают в силу сразу после сохранения. События, предшествующие по датам данным изменениям, не будут промаркированы новым подразделением.

14.1.2. Интеграция с MDP

Данная настройка предлагает возможность интегрировать выбранный Sensor Industrial 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 одна из следующих записей:

10.144.178.1:3000

14.1.3. Белый список

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

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.

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.

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.

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
-

14.1.4. Настройки управления Mediator /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.

14.1.5. Экспорт данных

При установке MXDR важно организовывать обновления эксплуатируемых устройств и сбор регистрируемых событий.

При необходимости функция мониторинга состояния систем может быть возложена на Пользователя. Для этого реализована возможность интеграции с различными SIEM-системами. Данная процедура осуществляется с помощью передачи хартбитов через syslog.

По умолчанию логи работы Sensor Industrial отправляются и хранятся в XDR Console и SOC АО «БУДУЩЕЕ» (***в зависимости от заданного режима работы XDR Console***). 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 Sensor Industrial формируются в формате *syslog* и затем упаковываются в указанные ниже форматы. Таким образом возможно интегрировать MXDR 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.

Система MXDR может детектировать события четырех различных категорий:

- Сигнатурные события (на основе анализа трафика)
- Сетевые аномалии
- События о вредоносных файлах (полученные от модуля MDP)
- Сообщения самодиагностики (хартбиты)

События в формате JSON

Сигнатурные события в формате JSON

Описание возможных полей при получении сигнатурных событий в формате JSON представлено в таблице ниже.

Поле	Описание
Timestamp	*Дата и время события*
flow_id	*Идентификатор потока данных*
event_type	*Тип события*
src_ip	*IP источника*
src_port	*Порт источника*
dest_ip	*IP назначения*
dest_port	*Порт назначения*
Proto	*Протокол*
Gid	*ID генератора сигнатуры*
signature_id	*Идентификатор сигнатуры*
Rev	*Номер ревизии сигнатуры*
Signature	*Название сигнатуры*
Category	*Категория угрозы*
Severity	*Уровень угрозы*
Hostname	*Доменное имя*
url	*Адрес страницы*
http_user_agent	*Приложение*
http_content_type	*Тип контента*
http_refer	*URL источника запроса*
http_method	*Метод запроса*
protocol	*Протокол*
status	*Статус*
length	*Длина*

Пример сообщения с сигнатурным событием в формате JSON:

{

"timestamp":"2016-06-30T13:51:28.033623+0300",

```
    "flow_id":2065914546,
    "event_type":"alert",
    "src_ip":"10.5.0.157",
    "src_port":64464,
    "dest_ip":"136.243.81.198",
    "dest_port":80,
    "proto":"TCP",
    "tx_id":0,
    "alert":{
      "action":"allowed",
      "gid":1,
      "signature_id":2808364,
  "rev":3,
      "signature":"MALWARE CheatEngine.AF Variant Checkin",
      "category":"unwanted-software",
      "severity":1
    },
    "http":{
      "hostname":"mobred.net",
      "url":"\/red.php?s=1623677220",
      "http_user_agent":"Mozilla\/5.0 (Windows NT 6.3; WOW64) AppleWebKit\/537.36
(KHTML, like Gecko) Chrome\/51.0.2704.103 Safari\/537.36",
      "http_content_type":"text\/javascript",
      "http_refer":"http:\/\/kinofilmi-online.net\/ekipazh\/",
      "http_method":"GET",
      "protocol":"HTTP\/1.1",
      "status":200,
      "length":50
    },
  "payload":"R0VUIC9yZWQucGhwP3M9MTYyMzY3NzIyMCBIVFRQLzEuMQ0KSG9zdD
ogbW9icmVkLm5ldA0KQ29ubmVjdGlvbjoga2VlcC1hbGl2ZQ0KVXNlci1BZ2VudDogTW96aWxs
YS81LjAgKFdpbmRvd3MgTlQgNi4zOyBXT1c2NCkgQXBwbGVXZWJLaXQvNTM3LjM2IChLSF
RNTCwgbGlrZSBHZWNrbykgQ2hyb21lLzUxLjAuMjcwNC4xMDMgU2FmYXJpLzUzNy4zNg0K
QWNjZXB0OiAqLyoNClJlZmVyZXI6IGh0dHA6Ly9raW5vZmlsbWktb25saW5lLm5ldC9la2lwYXp
oLw0KQWNjZXB0LUVuY29kaW5nOiBnemlwLCBkZWZsYXRlLCBzZGNoDQpBY2NlcHQtTGFu
Z3VhZ2U6IHJ1LVJVLHJ1O3E9MC44LGVuLVVTO3E9MC42LGVuO3E9MC40DQpDb29raWU6
IFBIUFNFU1NJRD1ja3JsMzJtaWplbjl2bWNtYTRzbGNiMTl1Nw0KDQo=",
      "payload_printable":"GET \/red.php?s=1623677220 HTTP\/1.1\r\nHost:
mobred.net\r\nConnection: keep-alive\r\nUser-Agent: Mozilla\/5.0 (Windows NT 6.3; WOW64)
AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/51.0.2704.103 Safari\/537.36\r\nAccept:
*\/*\r\nReferer: http:\/\/kinofilmi-online.net\/ekipazh\/\r\nAccept-Encoding: gzip, deflate,
sdch\r\nAccept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4\r\nCookie:
PHPSESSID=ckrl32mijen9vmcma4slcb19u7\r\n\r\n",
    "stream":1,
     "packet":"uK9nHtAHrPLFETTqCABFAAAozTpFAAAoCjqI81EGCgUKBQCdiPNRxvvQ
AFAAAAAAcO9SJgAAAAAAAAAA"
  }
```


Сетевые аномалии в формате JSON

Описание возможных полей при получении сообщения в формате JSON о сетевых аномалиях представлено в таблице ниже.

Поле	Описание
confidence	*Вероятность вредоносности*
src_port	*Порт источника*
classifier_version	*Версия классификатора*
domain_len	*Длина домена*
ts	*Дата и время события*
src_ip	*IP источника*
domain_idn	*Идентификатор домена*
dst_port	*Порт назначения*
dst_ip	*IP назначения*
msg	*Сообщение*
query	*Web-запрос*
domain_lvl	*Уровень домена*

Пример сообщения о сетевой аномалии в формате JSON:


```
{
   "confidence": "93.57",
   "src_port": "56147/udp",
   "classifier_version": "cf18209f902e244f44a7b510c25b5241b178673a-764c6c-2424",
   "domain_len": 9,
   "ts": 1486386430.751216,
   "src_ip": "10.0.0.2",
   "domain_idn": false,
   "dst_port": "53/udp",
   "dst_ip": "77.88.8.8",
   "msg": "DGA detected by XGB",
   "query": "ruwufluhg.top",
   "domain_lvl": 2
}
```


События о вредоносных файлах в формате JSON

Описание возможных полей при получении сообщения в формате JSON о вредоносных файлах представлено в таблице ниже.

Поле	Описание
sha256	*Контрольная сумма sha25*
sha1	*Контрольная сумма sha1*
filename	*Имя файла*
from	*Отправитель*
event_type	*Тип события*
timestamp	*Дата и время события*
md5	*Контрольная сумма MD5*
to	*Получатель*
probability	*Вероятность вредоносности*

Пример сообщения о вредоносном файле в формате JSON:


```
{
    "sha256":"c90c7c55be28436302c037a1215cb161dc6ff7eff029117122dd48cc833b8ce
6",
   "sha1":"16b1fc6af3901de3802af9643defb06e1d4f9de1",
   "filename":"VM576507_20170802.zip",
   "from":"MSVoice@irk.rshb.ru",
   "event_type":"MDP_alert",
   "timestamp":"2017-08-02T08:24:31.925799",
   "md5":"beefcca95f9b774a27c75d77c6897790",
   "to":[
      "director@irk.rshb.ru"
   ],
   "probability":67.60000000000001
}
```

Сообщения самодиагностики в формате JSON

Описание возможных полей при получении хартбитов в формате JSON представлено в таблице ниже.

Поле	Описание
host	*Идентификатор сенсора*
timestamp	*Время в UTC*
time_delta	*Время в секундах после последнего измерения*
ifaces_packets_delta	*Увеличение счетчика поступивших на интерфейс пакетов*
krnl_packets_delta	*Увеличение счетчика пакетов в kernel space*
ifaces_bytes_delta	*Увеличения счетчика RX-байт на интерфейсе*
vmmem_used	*Выделено виртуальной памяти (в байтах)*
vmmem_free	*Свободно виртуальной памяти (в байтах)*
swapm_free	*Свободно в свопе (в байтах)*
swapm_used	*Выделено в свопе (в байтах)*
disk_free	*Свободно в дисковой системе*
disk_used	*Занято в дисковой системе*
cpu_percent	*Средняя загрузка CPU по ядрам*
kernel_version	*Версия ядра*
bios_version	*Версия BIOS*
uptime	*Uptime устройства*

Пример хартбитов в формате JSON:


```
{
  "host":"kpx37lnychxz7lhw",
  "timestamp":"2017-10-04T16:13:40.158688",
  "time_delta":301.177393,
  "ifaces_packets_delta":4646238,
  "krnl_packets_delta":4660719,
  "ifaces_bytes_delta":3489196566,
  "vmmem_used":8569155584,
  "vmmem_free":24991760384,
  "swapm_free":4198846464,
  "swapm_used":83533824,
  "disk_free":816764354560,
  "disk_used":113368637440,
  "cpu_percent":8.4,
  "kernel_version":"4.4.0-45-generic",
  "bios_version":"2.0.8",
  "uptime":"16 weeks, 51 minutes"
}
```


События в формате CEF

Сигнатурные события в формате CEF

Описание возможных полей при получении сигнатурных событий в формате CEF представлено в таблице ниже.

Поле	Описание
proto	*Протокол*
start	*Дата и время события*
src	*IP источника*
spt	*Порт источника*
dst	*IP назначения*
dpt	*Порт назначения*
cat	*Категория угрозы*
dhost	*Доменное имя*
request	*Адрес страницы*
requestMethod	*Метод запроса*
app	*Протокол*
reason	*Статус*

Сетевые аномалии в формате CEF

Описание возможных полей при получении сообщения в формате CEF о сетевых аномалиях представлено в таблице ниже.

Поле	Описание
src	*IP-адрес источника файла для события, связанного с протоколами HTTP, FTP*
dst	*IP-адрес получателя файла для события, связанного с протоколами HTTP, FTP*
destinationDnsDomain	*Web-запрос*
rt	*Время события в UTC*

События о вредоносных файлах в формате CEF

Описание возможных полей при получении сообщения в формате CEF о вредоносных файлах представлено в таблице ниже.

Поле	Описание
duser	*Получатель письма для события, связанного с электронной почтой*
suser	*Отправитель письма для события, связанного с электронной почтой*
src	*IP-адрес источника файла для события, связанного с протоколами HTTP, FTP*
dst	*IP-адрес получателя файла для события, связанного с протоколами HTTP, FTP*
fileHash	*SHA 1 -хеш файла*
rt	*Время события в UTC*
fname	*Имя файла*

Сообщения самодиагностики в формате CEF

Описание возможных полей при получении хартбитов в формате CEF представлено в таблице ниже.

Поле	Описание
duser	*Получатель письма для события, связанного с электронной почтой*
suser	*Отправитель письма для события, связанного с электронной почтой*
src	*IP-адрес источника файла для события, связанного с протоколами HTTP, FTP*
dst	*IP-адрес получателя файла для события, связанного с протоколами HTTP, FTP*
fileHash	*SHA 1 -хеш файла*
rt	*Время события в UTC*
fname	*Имя файла*

14.1.6. Сервер времени

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.

14.1.7. SNMP-мониторинг

Настройка позволяет обеспечивать мониторинг состояния оборудования, а также мониторинг статистических данных используемых модулей в MXDR.

Поддерживаемые версии протокола SNMP:

- SNMPv1
- SNMPv2
- SNMPv3

При выборе версии протокола появляется возможность задать дополнительные параметры - специфичные для выбранного протокола.

SNMPv1

Доступные настройки:

- Адрес сервера
- Порт
- Community Data

SNMPv2

Доступные настройки:

- Адрес сервера
- Порт
- Имя пользователя
- Протокол авторизации:
    - None
    - MD5
    - SHA
    - SHA224
    - SHA256
    - SHA384
    - SHA512
- Ключ авторизации

SNMPv3

Доступные настройки:

- Адрес сервера
- Порт
- Имя пользователя
- Протокол авторизации:
    - None
    - MD5
    - SHA
    - SHA224
    - SHA256
    - SHA384

    - SHA512
- Ключ авторизации
- Протокол шифрования:
    - None
    - DES
    - 3DES
    - AES128
    - AES192
    - AES256
- Ключ шифрования

14.2. Блок «Сетевой трафик»

Данный блок содержит в себе набор функций, позволяющих: собирать метаинформацию о сетевых соединениях по протоколам уровня L7 (за исключением технологических протоколов); анализировать web-трафик, получаемый от прокси-серверов компании через ICAP; настраивать модуль сигнатурного анализа трафика; управлять загружаемыми файлами с сигнатурами на сетевой трафик; загружать специфичные для Sensor Industrial правила анализа сетевого трафика.

14.2.1. Сбор метаинформации о сетевых соединениях

Для обеспечения безопасности работы коммерческих сетей необходимо осуществлять контроль данных, передаваемых посредством протоколов передачи данных. Изначально переключатель для каждого модуля включен.

Протоколы L7

При включении L7 протокола система будет производить запись метаинформации о сессиях с использованием данного протокола. Таким образом возможно восстанавливать данные сессии, анализировать и ассоциировать их с файлами, передаваемыми в данных сессиях.
Подробная информация будет отображена в пункте "Сетевые соединения"

Логирование неизвестных соединений

Для логирования сессий с использованием нестандартных портов и протоколов необходимо активировать требуемые протоколы UDP, TCP или ICMP. Таким образом, все сессии, не подпадающие под стандартно используемые протоколы седьмого уровня модели OSI будут логироваться и размещаться в разделе Сетевые соединения".

14.2.2. ICAP сервер

Sensor Industrial 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 Sensor Industrial ответа по вердикту для файла по итогам поведенческого анализа на MDP. В случае, если файл вредоносный, Sensor Industrial присылает ICAP-клиенту команду на блокировку проанализированного файла.

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

14.2.3. Анализ сетевого трафика

Важнейший раздел при настройке сигнатурного анализа.

Настройки раздела позволяют системе дифференцировать зловредный трафик относительно легитимного. Позволяет указать локальные интерфейсы, а также интерфейсы для SPAN/RSAN/SPANinGRE.

Разделён на два подраздела.

Анализ сетевого трафика

Позволяет явно указать локальные адреса, сети / подсети, а также адреса локальных Proxy. Данный список определяет так называемую домашнюю сеть (Homenet) для сигнатурного анализа трафика. Выбор Homenet важен для группировки событий по подразделениям.

Введите список локальных подсетей и исключите из них адреса Proxy-серверов (используйте знак отрицания - пример:!proxy-ip/32).

Это позволит различать взаимодействия целевых хостов, сетей / подсетей с открытой сетью Интернет.

Интерфейсы для анализа трафика

- **Интерфейс**

  Имена интерфейсов
- **Текущая нагрузка**

  Это поток трафика, который подается на конкретный интерфейс - без учёта того анализируется данный трафик или нет.
- **BPF**

  Фильтр BPF для анализа трафика по сигнатурным правилам.
- **On/Off**
- **Число тредов**

  Установленное число потоков для каждого процесса сигнатурного анализа SPAN трафика на выбранном интерфейсе. (по умолчанию задано рекомендуемое значение. *Изменение значения может повлиять на производительность системы!*)

14.2.4. Сетевые сигнатуры

В настройке представлен список подклассов сигнатур, с возможностью выборочного отключения или включения определенных подклассов.

Примечание:

Включение новых правил, как и загрузка новых пользовательских правил анализа трафика, может приводить к снижению работоспособности устройства. Меняя перечень активных правил и загружая новые пользовательские правила, всегда

взвешивайте работоспособность устройства в части параметра "Дропы в ядре". Сенсоры протестированы на поддержку номинальной полосы пропускания только при условии использования конфига по умолчанию.

Ниже приведен список возможных сигнатур.

- Целевые атаки ;
- Уязвимости в серверном ПО;
- Уязвимости прикладного ПО;
- Бэкдоры и нелегальные средства удаленного управления;
- Банковские трояны;
- Мобильные трояны;
- Неспецифичная активность троянов;
- Drive-by атаки;
- Подозрительные события;
- Фишинговые ресурсы;
- Нарушение политик;
- Нежелательное ПО;
- Троян-вымогатель;
- Исследование сетевого периметра;
- Шпионское ПО.

14.2.5. Пользовательские сетевые сигнатуры

Загрузка пользовательских сигнатур в формате Suricata.

Примечание: ID пользовательских сигнатур должны быть в пределах 1300001 - 1500000.

14.3. Блок «Почта»

Данный блок содержит в себе набор функций, позволяющих: осуществлять настройку почтового клиента для скачивания писем на анализ по протоколам POP3/IMAP; управлять функцией SMTP-сервера в части получения и роутинга почты; определять поведение системы (из предлагаемого списка) в отношении работы со ссылками в письмах; настраивать параметры уведомления о заблокированных сообщениях.

14.3.1. 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 Sensor Industrial для ретроспективного анализа почтовых сообщений и вложений в них.

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.

Для анализа почтовых сообщений по протоколу POP3/IMAP перейдите в раздел настройки "Почтовый клиент".

Дополнительная информация по режиму работы представлена в разделе "Интеграция по SMTP"

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 MXDR 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 Sensor Industrial ограничивает передачу сообщений до получения вердикта от Sensor Industrial 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.

Более подробно об инфраструктурных требованиях можно почерпнуть в разделе "Интеграция inline (MTA)"

14.3.2. Почтовый клиент

Настройка почтового клиента позволяет Sensor Industrial 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 Sensor Industrial 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.

14.3.3. 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 Sensor Industrial 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.

- **Прокси сервер**

Позволяет задать прокси сервер для обеспечения web доступа сенсора при анализе ссылок в почтовых сообщениях и вложенных в них документах.

Примечание!

Для использования прямого взаимодействия сенсора через интерфейс управления с Интернет оставьте данное поле пустым.

После выбранной стратегии необходимо сохранить настройки.

14.3.4. Уведомления о заблокированных письмах

Настройка позволяет задать собственный шаблон отсылаемых информационных сообщений о факте блокировки письма.

14.4. Блок «Файлы»

Данный блок содержит в себе набор функций, позволяющих: управлять анализом и извлечением файлов из трафика, подключать общие папки для анализа файлов, а также настраивать общие ресурсы для сбора и анализа файлов.

14.4.1. 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 файлов или почтовых сообщений.

BPF для захвата трафика

BPF фильтр - это open-source проект позволяющий задавать фильтры извлечения данных из анализируемого трафика.

Фильтры действуют по принципу **white list** списка.

Протоколы

Переключатели активируют предустановленные BPF фильтры для анализа файлов из указанных протоколов.

- **SMTP/POP3**

Данный переключатель активирует функциональность по анализу почтовых сообщений в отсутствие возможности полноценной почтовой интеграции. *Обратите внимание: при реализации полноценной почтовой интеграции данную функцию необходимо отключить*

- **HTTP**

Восстанавливает из SPAN сессий файлы, передаваемые протоколом http (обычно при скачивании из сети Интернет)

- **FTP/SMB**

Восстанавливает из SPAN сессий файлы, передаваемые при работе с файловыми хранилищами.

14.4.2. Монтирование и анализ общих ресурсов

Настройка анализа файлов в сетевых папках осуществляется в два этапа:

- Монтирование общих ресурсов
- Анализ общих ресурсов

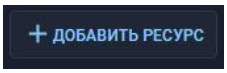
Монтирование общих ресурсов

Расположение: UI -> Настройки -> Устройства -> *в списке устройств выбрать необходимый* Sensor Industrial -> Блок "Файлы" -> Монтирование общих ресурсов.

В разделе "Монтирование общих ресурсов" выполняется только подключение папок для дальнейшего анализа.

Чтобы добавить папки для подключения к общей сетевой папке Sensor Industrial необходимо нажать на кнопку **Добавить ресурс** и заполнить следующие поля:

- Название - наименование папки, присвоенное пользователем, которое будет отображаться разделе "Анализ общих ресурсов"
- Тип ресурса - протокол, по которому будет проходить соединение с ресурсом (SMB, WebDAV, NFS, FTP)
- Адрес - расположение ресурса
- Логин - логин для подключения к выбранному ресурсу
- Пароль - пароль для подключения к выбранному ресурсу
- Статус - состояние подключения к выбранному ресурсу

Для добавления нового ресурса нажмите кнопку	
Для редактирования существующей записи нажмите кнопку	
Для удаления существующего ресурса нажмите кнопку	
После этого проверьте введённые данные и нажмите кнопку **Сохранить**	
В случае успешного подключения ресурса, в колонке Статус появится значок	

Анализ общих ресурсов

Расположение: UI -> Настройки -> Устройства -> *в списке устройств выбрать необходимый* Sensor Industrial > Блок "Файлы" > Анализ общих ресурсов

В разделе "Анализ общих ресурсов" осуществляется настройка режима обработки уже подключенных в разделе "Монтирование общих ресурсов" файловых ресурсов для сбора и анализа файлов.

Чтобы начать анализ ресурсов, необходимо нажать на кнопку **Добавить ресурс** и заполнить следующие поля:

- Имя - наименование ресурса из списка смонтированных
- Путь анализа - указываем путь относительно указанного в разделе "Монтирование общих ресурсов" (путь до дополнительного элемента в папке)
- Время анализа - временная метка создания или модификации файла, начиная с которой будет производиться анализ
- Период анализа – периодичность, с которой производится проверка ресурса на появление новых файлов
- Игнорировать скрытые - не проверять скрытые файлы
- Первичный анализ - проверить все существующие на момент включения анализа файлы
- Режим - режим работы:
    - *Анализ* - режим мониторинга, при котором только выдаётся алерт на вредоносные файлы. Файл остаётся в папке неизменным.
    - *Удаление* - режим мониторинга с блокировкой. Вредоносные файлы помещаются в карантин.
    - *Перемещение* - режим работы с двумя папками. Вредоносные файлы помещаются в карантин. Проверенные безопасные файлы перемещаются в указанную папку.

  При выборе режима работы *"Перемещение"* будут доступны следующие поля:
- Место назначения - наименование папки, созданной в разделе "Монтирование общих ресурсов", в которую будут перемещаться проанализированные безопасные файлы
- Путь назначения - относительный путь внутри папки, в которую будут перемещаться проанализированные безопасные файлы.

После того, как все необходимые параметры заданы, нажмите кнопку **Сохранить** 

14.5. Блок «Интеллектуальный анализ трафика»

Данный блок содержит в себе набор функций, позволяющих: выявлять взаимодействия с управляющими серверами через DGA, а также управлять модулем выявления туннелей в верхнеуровневых протоколах.

14.5.1. Модуль выявления DGA-коммуникаций

Настройка позволяет выявлять взаимодействия с управляющими серверами через DGA.

Для того чтобы запустить процесс, необходимо заполнить поля:

- **Порог обращений**

Количество DGA запросов для порождения одного события безопасности.

- **Порог секунд**

Время, за которое учитываются DGA запросы в количестве, заданном в пороге обращений.

После того как поля будут заполнены, нажмите на кнопку **Сохранить.**

14.5.2. Выявление туннелей

Переключатель «Выявление туннелей» предназначен для управления верхнеуровневыми протоколами:

- UDP
- TCP
- DNS
- SSL
- HTTP

При обнаружении в сети соединений, создаваемых разными фреймворками (meterpreter, dnscat, assitsov и т.п.) автоматически создается алерт, который будет отображен в пункте "Алерты"

Для настройки управления модулем выявления туннелей в верхнеуровневых протоколах необходимо включить/выключить переключатель, затем нажать кнопку **Сохранить**.

14.5.3. Выявление скрытых каналов и горизонтального перемещения

В блоке "Интеллектуальный анализ трафика" настройка "Выявление скрытых каналов и горизонтального перемещения" представляет собой модуль для выявления распространения угроз во внутренней инфраструктуре.

Логика обработки

Используются ML классификаторы.

Sensor Industrial анализирует kerberos(update), smb, ntlm, dce-rpc протоколы на предмет обращения к файловым хранилищам администратора, записи на них файлов, использования wmi и т.п.

В зависимости от выбранной чувствительности алгоритм на основе совокупности индикаторов, описанных выше, создаёт события и алерты.

По умолчанию весь трафик, настроенный на обработку в пункте "Анализ сетевого трафика" подпадает под классификатор "Выявление скрытых каналов и горизонтального перемещения" сразу после включения описываемого функционала.

Для исключения лишних сетевых потоков необходимо воспользоваться белыми списками (настройка ниже).

Настройка выявления скрытых каналов и горизонтального перемещения

Чувствительность

В поле **Чувствительность** - выбирается степень чувствительности классификатора при выставлении алерта. Чувствительность — это отсечка по разнообразию и количеству анализируемых событий от одной машины за 10 минут, в течении которых определяется злоумышленное поведение. При этом в случае выявления числа событий, переходящих определённый порог, злоумышленное поведение может быть определено в более короткие периоды.

Белый список

Для добавления IP-адреса в белый список, необходимо нажать на кнопку 

, заполнить появившееся поле и сохранить настройки. По мимо непосредственно IP адреса возможно задать направление анализируемого потока для исключения из анализа. Таким образом возможно эффективно использовать ресурсы

Sensor Industrial, уменьшается количество false-positive алертов, а также позволяет целенаправленно обнаружить факты выявления скрытых каналов и горизонтальных перемещений, проводимых в нужном направлении.

Если необходимо изменить настройки детектирования для уже имеющегося IP-адреса, то его можно найти в строке поиска 

14.6. Блок «Технологический сегмент»

Данный блок содержит в себе набор функций, позволяющих: собирать метаинформацию о сетевых соединениях и управлять поддержкой промышленных протоколов; настраивать системы реагирования на неизвестные сетевые взаимодействия, а также настраивать правила для осуществления контроля соединений по технологическим протоколам.

14.6.1. Технологическое оборудование

Использование данного раздела позволяет включить функцию поиска и контроля целостности технологического оборудования в автоматическом режиме.

14.6.2. Реагирование на неизвестные сетевые взаимодействия

Переключатель Экспорт событий в syslog включен по умолчанию и позволяет автоматически добавлять логи подсистемы в syslog для дальнейшей выгрузки во внешние системы.

Переключатель **Обрабатывать L2 соединения** включен по умолчанию и выдает неизвестные сетевые взаимодействия на уровне L2.

Вывод неизвестных сетевых взаимодействий представлен в виде таблицы и содержит в себе следующие поля:

Время - дата и время обнаружения;

Адрес отправителя/ получателя - для соединений, реализованных на уровнях L2, L4;

MAC-адрес/ IP-адрес - для соединений MAC/IP.

Поле **Режим** позволяет выбрать режим обучения/ классификации модели:

- **режим обучения** - создание эталонного образа сети для дальнейшего использования при обнаружении и классификации неизвестных сетевых соединений;
- **режим классификации** - применение эталонного образа, созданного в режиме обучения для выявления аномалий в сети.

Чтобы создать новую модель реагирования на неизвестные сетевые взаимодействия, нажмите на кнопку **Сбросить модель.** В появившемся окне нажмите **OK**.

14.6.3. Контроль прикладных протоколов

В данном разделе осуществляется настройка правил анализа промышленных протоколов для защиты технологического процесса АСУ.

Раздел состоит из двух основных частей:

- **Предустановленные правила**
- **Пользовательские правила**

Подразделы **"Предустановленные правила"** и **"Пользовательские правила"** содержат в себе следующую информацию:

- **Название** - название правила, которое является ключевой фразой при срабатывании правила. Служит для идентификации правила.
- **Протокол** - наименование технологического протокола
- **Функция** - операция, примененная к устройству, указанная в протоколе
- **Источник** - узел, подсеть или сеть, с которого отправляется функция (можно указывать несколько через символ ",")
- **Получатель** - узел, подсеть или сеть, на который отправлена функция (можно указывать несколько через символ ",")
- **Достоверный источник** - узел, подсеть или сеть, с которого отправляется функция и на который не требуется реагировать (whitelist)
- **Достоверный получатель** - узел, подсеть или сеть, на который отправлена функция и на который не требуется реагировать (whitelist)
- **Критичность** - уровень критичности угрозы, возникающий при алерте (5 - самый критичный уровень угрозы)

Символом * указываются все сети защищаемой инфраструктуры. Применяется для полей Источник и Получатель

Пользовательские правила

При создании нового пользовательского правила необходимо заполнить поля, описанные выше и нажать на кнопку 

В поле **Протокол** в контекстном меню выберите необходимый технологический протокол:

- **IEC104** - промышленный протокол передачи данных, реализующий прикладной уровень TCP/IP, широко используемый в технологических сетях объектов электроэнергетики для организации передачи данных между распределительными устройствами, контроллерами телемеханики, РЗА, АИСКУЭ и АРМ оператора
- **MODBUS** - открытый коммуникационный промышленный протокол для машинного взаимодействия, основанный на архитектуре "ведущий — ведомый" (master-slave). Является стандартом де-факто и поддерживается почти всеми производителями промышленного оборудования
- **OPCUA** - фильтр позволяет рассмотреть выявленные коммуникации, реализованные в соответствии с спецификацией OPC Unified Architecture
- **S7** - промышленный протокол, разработанный компанией Siemens для реализации передачи данных между контроллерами автоматизации, устройствами полевого уровня, периферийными модулями, серверами и АРМ оператора со SCADA
- **S7P** - промышленный протокол, являющийся развитием S7COMM и предназначенный для работы нового поколения устройств автоматизации производства компании Siemens
- **UMAS** - промышленный протокол, широко используемый промышленным оборудованием автоматизации производства компании Schneider Electric для реализации коммуникаций в сегменте АСУ ТП. Часто используется для обмена данными по монтажной шине между процессорным модулем контроллера автоматизации и модулями периферии. OFS использует OPC для подключения к SCADA.

В поле **Функции** укажите от одной и более функций из предлагаемого списка контекстного меню:

Для протокола IEC104

- M_SP_TB_1 - одноэлементная информация с меткой времени
- M_SP_NA_1 - одноэлементная информация
- M_DP_NA_1 - двухэлементная информация
- M_DP_TB_1 - двухэлементная информация с меткой времени
- C_SC_NA_1 - одноэлементная команда
- C_DC_NA_1 - двухэлементная команда
- C_SC_TA_1 - одноэлементная команда с меткой времени
- C_DC_TA_1 - двухэлементная команда с меткой времени

Для протокола MODBUS

- READ_COILS - чтение значений нескольких регистров флагов
- READ_DISCRETE_INPUTS - чтение значений нескольких дискретных входов
- READ_HOLDING_REGISTERS - чтение значений нескольких регистров хранения
- READ_INPUT_REGISTERS - чтение значений нескольких регистров ввода
- WRITE_SINGLE_COIL - запись одного регистра флагов
- WRITE_SINGLE_REGISTER - запись одного регистра (ввода или хранения)
- WRITE_MULTIPLE_COILS - запись нескольких регистров флагов
- WRITE_MULTIPLE_REGISTERS - запись нескольких регистров (ввода или хранения)
- READ_WRITE_MULTIPLE_REGISTERS
- FIRMWARE_REPLACEMENT

Для протокола OPCUA

- SECURE_MESSAGE_WRITE_REQUEST_BIN - запрос записи
- SECURE_MESSAGE_REGISTER_SERVER_REQUEST_BIN
- SECURE_MESSAGE_OPENSECURECHANNEL_REQUEST_BIN
- SECURE_MESSAGE_DELETE_NODES_RESPONSE_BIN
- SECURE_MESSAGE_REGISTER_NODES_REQUEST_BIN
- SECURE_MESSAGE_UNREGISTER_NODES_REQUEST_BIN
- SECURE_MESSAGE_MODIFY_MONITORED_ITEMS_REQUEST_BIN
- SECURE_MESSAGE_DELETE_MONITORED_ITEMS_REQUEST_BIN
- SECURE_MESSAGE_DELETE_SUBSCRIPTIONS_REQUEST_BIN

Для протокола UMAS

- READ_ID -
- READ_PROJECT_INFO - получение данных о программе управления ПЛК
- READ_PLC_INFO - получение данных о ПЛК
- READ_CARD_INFO - получение данных с внешней карты памяти ПЛК (которая устанавливается из вне)
- READ_MEMORY_BLOCK -
- WRITE_MEMORY_BLOCK -
- READ_VARIABLES - получение данных с регистров ПЛК
- WRITE_VARIABLES - запись данных на регистры ПЛК
- READ_COILS_REGISTERS - получение данных с регистров ПЛК
- WRITE_COILS_REGISTERS - запись данных на регистры ПЛК
- CARD_MANAGEMENT -

- START_PLC - запуск ПЛК
- STOP_PLC - завершение работы ПЛК
- MONITOR_PLC -
- CHECK_PLC -
- INITIALIZE_UPLOAD - инициация загрузки данных на ПЛК
- UPLOAD_BLOCK - загрузка данных на ПЛК
- END_STRATEGY_UPLOAD - завершение загрузки данных на ПЛК
- INITIALIZE_DOWNLOAD - инициация скачивания данных с ПЛК
- DOWNLOAD_BLOCK - скачивание данных с ПЛК
- END_STRATEGY_DOWNLOAD - завершение скачивания с ПЛК

Для протокола S7

- REQUEST_DOWNLOAD - инициация скачивания данных с ПЛК
- DOWNLOAD_BLOCK - скачивание данных с ПЛК
- DOWNLOAD_END - завершение скачивания данных с ПЛК
- START_UPLOAD - инициация загрузки данных на ПЛК
- UPLOAD - процесс загрузки данных на ПЛК
- END_UPLOAD -завершение загрузки данных на ПЛК
- WRITE_DATA - запись данных
- READ_DATA -получение данных
- CYCLE_MEMORY - циклическое чтение данных с памяти ПЛК

Для протокола S7P

- SET_VARIABLE - установка значения данных
- EXPLORE -
- CREATE_OBJECT
- DELETE_OBJECT
- GET_VARIABLE

При нажатии на кнопку **Добавить правило** откроется дополнительное поле для создания нового правила.

При нажатии на кнопку **Загрузить правила** предоставляется возможность загрузить правила с ПК пользователя в решение XDR Console в формате .json.

При нажатии на кнопку **Скачать правила** предоставляется возможность загрузить правила на ПК пользователя в формате .json.

14.6.4. Сбор метаинформации о сетевых соединениях

Для обеспечения безопасности работы автоматизированных систем управления технологическим процессом необходимо осуществлять контроль данных, передаваемых посредством промышленных протоколов передачи данных. Изначально переключатель для каждого модуля включен.

15. Редактирование настроек модуля MDP

Расположение: UI > Настройки > Устройства > *в списке устройств выбрать необходимый* MDP

На странице представлены общие показатели по работе подключенного MDP. Данные по каждому MDP-у доступны при раскрытии соответствующей карты в списке подключённых устройств.

Общая информация

- Имя - заданный идентификатор может быть любым
- Номер лицензии - получен при покупке или тестировании решения
- Комментарий
- VPN IP - адрес внутри VPN туннеля получаемый при подключении MDP к XDR Console для управляющих коммуникаций
- Внешний IP - адрес управляющего интерфейса, выданный на стороне клиента (через DHCP или статическими правилами)
- Компания - задаются при создании нового устройства из списка Настройки -> Компании

Состояние устройства

- Последний HeartBeat - последний замеченный heartbeat с данного устройства
- Последнее обновление
- CPU / RAM / HDD
- Дропы в ядре / на интерфейсе
- Последняя активность - крайнее время активности VPN между MDP и управляющим XDR
- Длительность - временной отрезок, в течение которого между MDP и XDR был установлен управляющий VPN канал. Отчитывается с момента последней потери связи между устройствами
- Загрузка канала

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 (%)

Кнопка редактирования базовых свойств  - доступны для редактирования:

- Имя
- Комментарий

Примечание: данная кнопка доступна только для пользователей с типом аккаунта ***owner***.

15.1. Доступ виртуальных машин в Интернет

Одной из крайне важных настроек MDP является возможность предоставления доступа в открытую сеть Интернет образа ОС развёрнутым в виртуальной среде.

Настройка позволяет, в первую очередь, определять используемый для доступа в Интернет маршрут, а именно:

Выход через соединение с XDR

Все сетевые запросы из виртуальной среды в открытую сеть Интернет инкапсулируются в VPN соединение до XDR Console. Таким образом запросы анализируемого ПО в Интернет обрабатываются XDR Console.

Для проведения качественного поведенческого анализа анализируемому ПО необходимо предоставлять неблокируемый доступ до требуемых ресурсов в открытой сети Интернет, даже если эти ресурсы являются заведомо вредоносными!

Учитывая данный факт, при выбранной настройке, XDR Console необходимо предоставлять неблокируемый доступ до открытой сети Интернет без ограничений!

Выход напрямую через mgmt-порт

Все сетевые запросы из виртуальной среды в открытую сеть Интернет направляются на маршрутизатор по умолчанию через интерфейс управления MDP. Таким образом запросы анализируемого ПО в Интернет обрабатываются MDP.

Для проведения качественного поведенческого анализа анализируемому ПО необходимо предоставлять неблокируемый доступ до требуемых ресурсов в открытой сети Интернет, даже если эти ресурсы являются заведомо вредоносными!

Учитывая данный факт, при выбранной настройке, MDP необходимо предоставлять неблокируемый доступ до открытой сети Интернет без ограничений!

Контроль обращения по ссылкам из виртуальной среды

В MDP присутствует отдельный модуль, обрабатывающий сценарии обращения по ссылкам, обнаруженным в файлах анализируемого ПО. Такие обращения, возможно, проксировать отдельно от остального потока обращений из виртуальной среды в открытую сеть Интернет.

Для настройки прокси задайте (в нижней части раздела) в поле **Прокси сервер:** *Адрес прокси-сервера* и *Порт прокси-сервера разделив* их символом "**:**".

15.2. Экспорт данных из MDP

В разделе "Экспорт данных" возможно настроить автоматическую отправку сведений о состоянии (heartbeat) MDP в SIEM-систему. Для этого необходимо указать соответствующие параметры Syslog-сервера: сетевой адрес, порт и тип протокола. Данные передаются по протоколу Syslog в двух форматах:

- CEF
- JSON

Система MXDR может детектирует сообщения самодиагностики (хартбиты)

Сообщения самодиагностики в формате JSON

Описание возможных полей при получении хартбитов в формате JSON представлено в таблице ниже.

Поле	Описание
host	*Идентификатор сенсора*
timestamp	*Время в UTC*
time_delta	*Время в секундах после последнего измерения*
ifaces_packets_delta	*Увеличение счетчика поступивших на интерфейс пакетов*

krnl_packets_delta	*Увеличение счетчика пакетов в kernel spac*
ifaces_bytes_delta	*Увеличения счетчика RX-байт на интерфейсе*
vmmem_used	*Выделено виртуальной памяти (в байтах)*
vmmem_free	*Свободно виртуальной памяти (в байтах)*
swapm_free	*Свободно в свопе (в байтах)*
swapm_used	*Выделено в свопе (в байтах)*
disk_free	*Свободно в дисковой системе*
disk_used	*Занято в дисковой системе*
cpu_percent	*Средняя загрузка CPU по ядрам*
kernel_version	*Версия ядра*
bios_version	*Версия BIOS*
uptime	*Uptime устройства*

Пример хартбитов в формате JSON:


```
{
  "host":"kpx37lnychxz7lhw",
  "timestamp":"2017-10-04T16:13:40.158688",
  "time_delta":301.177393,
  "ifaces_packets_delta":4646238,
  "krnl_packets_delta":4660719,
  "ifaces_bytes_delta":3489196566,
  "vmmem_used":8569155584,
  "vmmem_free":24991760384,
  "swapm_free":4198846464,
  "swapm_used":83533824,
  "disk_free":816764354560,
  "disk_used":113368637440,
  "cpu_percent":8.4,
  "kernel_version":"4.4.0-45-generic",
  "bios_version":"2.0.8",
  "uptime":"16 weeks, 51 minutes"
}
```


Сообщения самодиагностики в формате CEF

Описание возможных полей при получении хартбитов в формате CEF представлено в таблице ниже.

Поле	Описание
duser	*Получатель письма для события, связанного с электронной почтой*
suser	*Отправитель письма для события, связанного с электронной почтой*
src	*IP-адрес источника файла для события, связанного с протоколами HTTP, FTP*
dst	*IP-адрес получателя файла для события, связанного с протоколами HTTP, FTP*
fileHash	*SHA 1 -хеш файла*
rt	*Время события в UTC*
fname	*Имя файла*

15.3. Сервер времени MDP

По умолчанию каждый MDP 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.

16. Редактирование настроек модуля Storage

Расположение: UI -> Настройки -> Устройства -> *в списке устройств выбрать необходимый* Storage.

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

Общая информация

- Имя - заданный идентификатор может быть любым
- Номер лицензии - получен при покупке или тестировании решения
- Серийный номер - серийный номер оборудования
- Комментарий
- VPN IP - адрес внутри VPN туннеля получаемый при подключении Storage к XDR Console для управляющих коммуникаций
- Внешний IP - адрес управляющего интерфейса, выданный на стороне клиента (через DHCP или статическими правилами)
- Компания - задаются при создании нового устройства из списка Настройки -> Компании

Состояние устройства

- Последний HeartBeat - последний замеченный heartbeat с данного устройства
- Последнее обновление - дата последнего обновления
- CPU / RAM / HDD
- Дропы в ядре / на интерфейсе

- Последняя активность - крайнее время активности VPN между сенсором и управляющим XDR
- Длительность - временной отрезок, в течение которого между Storage и XDR был установлен управляющий VPN канал. Отчитывается с момента последней потери связи между устройствами
- Загрузка канала

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 (%)

16.1. Настройка устройства Storage

В разделе UI Настройки Устройства -> XDR при имеющихся устройствах типа Storage, осуществляется настройка кластеризации данных.

В данном разделе отображается информация:

«Настройка главного устройства»

- Статус - текущий статус ноды (устройства)
- Ноды – количество устройств
- Документы – количество объектов в хранилище
- Объем данных – общий размер дискового хранилища
- «Управление устройствами»
- Имя ноды – название, присвоенное устройству
- UID
- IP-port
- Статус ноды
- CPU – использование процессора
- Memory usage – использование памяти
- Disk usage – использование дискового хранилища

Добавление и удаление устройств

Чтобы добавить устройство, нажмите на кнопку **<Добавить устройство в кластер>**

В появившемся окне выберите необходимое устройство из списка доступных устройств типа Storage и добавьте его в кластер.

17. Редактирование настроек модуля EDR

Данный раздел расположен в UI XDR Console -> Расследования -> Компьютеры

17.1. Управление версиями

Для ручной загрузки пакетов с новыми версиями EDR, необходимо нажать на кнопку Управление версиями. В появившемся поле прикрепите файл.

17.2. Обновление компьютеров до новых версий EDR

Чтобы обновить компьютеры вручную до новых версий XDR, необходимо выбрать один или несколько компьютеров, после чего выбрать версию обновления.

18. Редактирование настроек модуля BEP

На странице представлены общие показатели по работе модуля BEP.

Общая информация

- Имя - заданный идентификатор может быть любым
- Номер лицензии - получен при покупке или тестировании решения
- Серийный номер - серийный номер оборудования
- Комментарий
- VPN IP - адрес внутри VPN туннеля получаемый при подключении BEP к XDR Console для управляющих коммуникаций
- Внешний IP - адрес управляющего интерфейса, выданный на стороне клиента (через DHCP или статическими правилами)
- Компания - задаются при создании нового устройства из списка Настройки -> Компании
- Скрыть от CERT -свойство сенсора, скрывающее его события из выдачи для мониторинга пользователям с ролью CERT

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 (%)

Кнопка редактирования базовых свойств  - доступны для редактирования:

- Имя
- Комментарий
- Скрыть от CERT

Примечание: данная кнопка доступна только для пользователей с типом аккаунта ***owner***.

Управление лицензиями модуля BEP доступно при нажатии на кнопку **"Управление лицензией"**. Существуют два типа лицензии: • BEP_STANDARD • BEP_ENTERPRISE	
Для изменения основных настроек нажмите на кнопку	

Основные настройки

При нажатии на кнопку **"Основные настройки"** будет осуществлен автоматический переход на страницу настроек модуля BEP.

18.1. Блок «Домены и маршруты»

Данный блок содержит в себе набор функций, позволяющих: добавлять и верифицировать домены, а также настраивать маршруты движения почты и балансировки нагрузки.

18.1.1. Почтовые домены

Использование данного раздела позволяет добавлять и верифицировать почтовые домены.

Для защиты почтовых входящих сообщений необходимо:

1. Добавить домен клиента в данный список.
2. Сформированный код подтверждения необходимо добавить в TXT запись домена. Клиент осуществляет данную операцию в административной панели регистратора домена.
3. Необходимо дождаться верификации данного домена комплексом Атмосфера.

Статус домена:

- подтверждено - подтверждённый статус домена. Код подтверждения добавлен в TXT запись домена.
- не подтверждено - Код подтверждения не был добавлен в TXT запись домена или валидация еще не окончилась.

18.1.2. Почтовые маршруты

Использование данного раздела позволяет осуществлять настройку маршрутов движения почты и балансировки нагрузки.

Необходимые настройки:

- Домены получателя - обслуживаемые почтовые домены и/или поддомены клиента.
- Подтв. RCPT TO - при включении Атмосфера проверяет наличие получателя в MX серверах клиента. (Открывается встречная SMTP сессия на требуемое имя. По ответу от MX определяется наличие или отсутствие данного получателя у клиента).
- MX адрес - адрес почтового сервера клиента. Он же адрес следующего хопа в цепочке проверки почтовых сообщений.
- Порт - порт на MX сервере клиента для отправки проверенных сообщений
- TLS - использование TLS для формирования всех коммуникаций с отправителями и получателями почтовых сообщений.
- Приоритет - приоритетность опроса серверов клиента.
- Вес - балансировка нагрузки на сервера клиента.

18.2. Блок «Политика и обнаружение»

Данный блок содержит в себе набор функций, позволяющих: выбирать регион анализа файлов, настраивать политики действий на основе результата проверки отправителя письма, настраивать политики действий на основе формата содержимого писем, определять желаемое поведение системы в случае невозможности полного анализа писем, а также выбирать желаемую стратегию обработки ссылок в письмах.

18.2.1. Детонация файлов

Использование данного раздела позволяет осуществлять выбор региона для облачной площадки, выполняющей поведенческий анализ объектов, вложенных в письма или полученных в результате исследования ссылок в письмах или во вложениях.

Детонация файлов осуществляется отдельно для каждого региона.

В поле **"Действие"** можно:

- Отметить тему - пропустить письмо с добавлением в текст темы письма дополнительную информацию о вложении.
- Добавить заголовок - пропустить письмо с добавлением в SMTP-заголовки письма дополнительную информацию о детонации файлов.
- Карантин + Уведомление отправителя - блокировка письма с уведомлением.

Язык виртуальных машин может быть как русский, так и английский.

18.2.2. Проверки отправителя

Использование данного раздела позволяет осуществлять настройку политик действий на основе результата отправителя письма.

Общая информация содержит в себе следующие параметры:

- Категория -
  - DKIM - проверка подлинности сообщения по открытому ключу в записи DKIM домена отправителя.
  - DMARC - проверка соответствия письма установленным политикам в записи DMARC домена отправителя.
  - SPF - проверка авторизованности IP адреса отправителя по записи SPF домена отправителя.
- Описание - общие описания нарушения политик
- Действие -
  - Отметить тему - пропустить письмо с добавлением в текст темы письма дополнительную информацию о вложении.
  - Добавить заголовок - пропустить письмо с добавлением в SMTP-заголовки письма дополнительную информацию о детонации файлов.
  - Карантин + Уведомление отправителя - блокировка письма с уведомлением.

18.2.3. Проверки форматов содержимого

Использование данного раздела позволяет осуществлять настройку политик действий на основе форматов содержимого писем.

Общая информация содержит в себе следующие параметры:

- Имя правила - название политики для ее дальнейшего использования
- Условие - правило, на основе которого производится проверка форматов содержимого
  - file_name - реакции на определённые имена файлов;
  - file_magic - реакция на заданные расширения файлов;
  - url - реакция на заданные ссылки;
  - sender - реакция на определенного получателя;
  - recipient - реакция на определенного получателя;
  - dkim;
  - spf;
  - dmarc;

- Действие -
    - Отметить тему - пропустить письмо с добавлением в текст темы письма дополнительную информацию о вложении.
    - Добавить заголовок - пропустить письмо с добавлением в SMTP-заголовки письма дополнительную информацию о детонации файлов.
    - Карантин + Уведомление отправителя - блокировка письма с уведомлением.

18.2.4. Непроверенный контент

Использование данного раздела позволяет определять желаемое поведение системы в случае невозможности полного анализа письма.

Общая информация содержит в себе следующие параметры:

- Категория - категория проверяемого контента
    - Зашифрованные архивы
    - Недоступная ссылка
- Описание - причина, препятствующая полному анализу письма
- Действие -
    - Отметить тему - пропустить письмо с добавлением в текст темы письма дополнительную информацию о вложении.
    - Добавить заголовок - пропустить письмо с добавлением в SMTP-заголовки письма дополнительную информацию о детонации файлов.
    - Карантин + Уведомление отправителя - блокировка письма с уведомлением.

18.2.5. Стратегия обработки ссылок

При интеграции с почтовой системой ВЕР будет осуществлять анализ почтовых сообщений на предмет содержания в нём ссылок на внешние ресурсы. При обнаружении ссылок ВЕР 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.

19. Графовый анализ

Расположение: UI -> Граф

Комплекс позволяет определять связанную с найденным потенциальным инцидентом инфраструктуру в виде графа.

Правильное построение графа

Чтобы начать использовать сетевой граф, нужно ввести в поисковую строку домен, IP-адрес, email или отпечаток SSL-сертификата. Есть три условия, которыми может управлять аналитик: время, глубина шагов и очистка.

- Временные метки 

  Важный параметр при котором учитываются временные интервалы активности доменов, сервисов, серверов, передача доменов и т.п. Временные интервалы могут быть разными для домена и для IP, который с ним связан. Если не указать этот параметр, то система сама определит последний интервал владения этим ресурсом.

- Шаги 

  Шаги - это рекурсивное построение графов от каждого уже вынесенного на графе элемента.

  Максимальное количество шагов - неограниченно. Чем больше шагов, тем больше данных, но и больше ложноположительных событий. По умолчанию глубина равна 3. Это означает, что от искомого элемента будут найдены все напрямую связанные элементы, потом это каждого нового элемента будут построены новые связи до других элементов, и уже от новых элементов с прошлого шага будут новые элементы.

- Очистка графа 

  Автоматически удаляем с графа элементы, не связанные с исследуемым хостом, но даем возможность отключить очистку. По умолчанию опция “Очистка графа” включена и все нерелевантные элементы будут удаляться с графа

Особенности построения графа

- Скрытые данные

  Учитываются неявные связи или недоступные в публичном пространстве данные.

- Полный поиск

  Поиск по всем данным, а не только по индикаторам.

  Помимо визуального отображения связанных с инцидентом элементов, ниже, под графом, представлен список обнаруженных компонент с подробным описанием каждой.

Домены

Список доменов отображает только домены, охваченные графом. По каждому домену доступна историческая информация за выбранный временной период.

При раскрытии каждой записи может быть доступна следующая информация:

- **WHOIS**

  Whois данные по доменному имени отображают данные, полученные путём сканирования и запросов с иных сервисов данных по открытой сети Интернет. Причём в левом столбце отображаются временные периоды, в течении которых whois данные по домену не менялись. Таким образом возможно заглянуть в историю изменения доменной записи на сколько это возможно из данных имеющихся в АО «БУДУЩЕЕ».

  Информация данного раздела может содержать: Адрес, Name servers, Domain name, Updated date, City, State, Expiration date, Контактный данные регистрирующего, Whois server, Status, Zipcode, Customer id, Registrar, Данные организации, Country, Phone, Creation date, Email
- **DNS**

  Па данному столбцу возможно отследить изменение различных типов записей, присутствовавших в выбранной DNS на различных промежутках времени. Данные могут содержать: MX, SOA, A, NS, и иные типы записей.

IP-адреса

Раздел предоставляет актуальные, в том числе исторические, данные по серверам, используемым злоумышленниками для реализации выбранной целевой атаки. При раскрытии каждой записи может быть доступна следующая информация:

- **WHOIS**

  Whois данные по выбранному IP адресу отображают данные, полученные путём сканирования и запросов с иных сервисов данных по открытой сети Интернет. Причём в левом столбце отображаются временные периоды, в течении которых whois данные по адресу не менялись. Таким образом возможно заглянуть в историю изменения IP адреса на сколько это возможно, из данных имеющихся в АО «БУДУЩЕЕ».

  Информация данного раздела определяет физическое расположение хостинга, а также может предоставлять иные важные данные по хостингу.
- **SERVICES**

  Данный подраздел определяет актуальные и исторические данные по поднятым на данном хосте сервисам. А также предоставляет данные по каждому обнаруженному сервису, исходя из откликов данных сервисов на сканирование со стороны АО «БУДУЩЕЕ». Этот процесс необходим, чтобы установить, где реально находится вредоносный сервер.
  99% кардшопов, хакерских форумов, множество фишинговых ресурсов и других вредоносных серверов скрываются как за собственными прокси-серверами, так и за прокси легитимных сервисов, например, Cloudflare. Знание о реальном бэкенде очень важно для расследований: становится известен хостинг-провайдер, у которого можно изъять сервер, появляется возможность построить связи с другими вредоносными проектами.

SSL сертификаты

Список сертификатов, связанных с инфраструктурой атакующего, представлен в настоящем разделе.

SSH ключи

Публичные SSH ключи, связанные с атакующими, отображаются в настоящем разделе.

Файлы

Данный раздел содержит информацию о файлах, которые были замечены в связях с искомой инфраструктурой.

Данные файлы подгружаются не только из системы MXDR, но и из других источников, например, Virustotal, AnyRun,HybridAnalysis и т.д.

E-mails

Электронные адреса, связанные с инфраструктурой злоумышленника представлены в настоящем разделе.

Телефоны

Телефоны, найденные в элементах графа или имеющие отношение обнаруженным связям, представлены в настоящем разделе.

Тэги

Раздел, позволяющий атрибутировать группировки/инструменты.