ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 XDR»

Руководство администратора

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Определение
ОС	Операционная система
ПО	F6 XDR, MXDR Console
iDRAC	Integrated Dell Remote Access Controller, проприетарный контроллер удалённого доступа, мониторинга и управления
iLO	Проприетарный интерфейс Integrated Lights-Out
IPv4	Internet Protocol version 4
KVM	Kernel-based Virtual Machine
MXDR	Программный комплекс Managed Extended Detection and Response (Managed XDR)
SaaS	Software as a service
SOC	Security operation center
SSH	Secure shell

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ описывает процесс установки экземпляра программного обеспечения «F6 XDR» (далее – ПО, MXDR Console).

Инструкция по установке распространяется только на вариант распространения ПО в формате On-prem. Для Cloud (SaaS) версии установка ПО не требуется.

В случае возникновения проблем с разворачиванием ПО необходимо обратиться в техническую поддержку.

1.2 Назначение ПО

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

2 ТРЕБОВАНИЯ К СИСТЕМЕ

ПО может быть установлено либо на физический сервер, либо на виртуальную машину.

2.1 Минимальные технические требования для физического сервера

Ниже приведены минимальные технические требования к серверу в зависимости от типа ПО - Standard или Enterprise.

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

2.2 Минимальные технические требования для виртуальной машины

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

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

2.3 Требования к программному обеспечению

Требования к программному обеспечению не предъявляются, так как ПО является самостоятельной операционной системой, реализованной на базе Arch Linux с версией ядра Linux 5.11.16-arch1-1.

3 УСТАНОВКА ТЕСТОВОЙ ВЕРСИИ ПО

3.1 Подготовка образа

Установочный образ можно создать с использованием следующих средств:

– 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**)

3.2 Установка образа

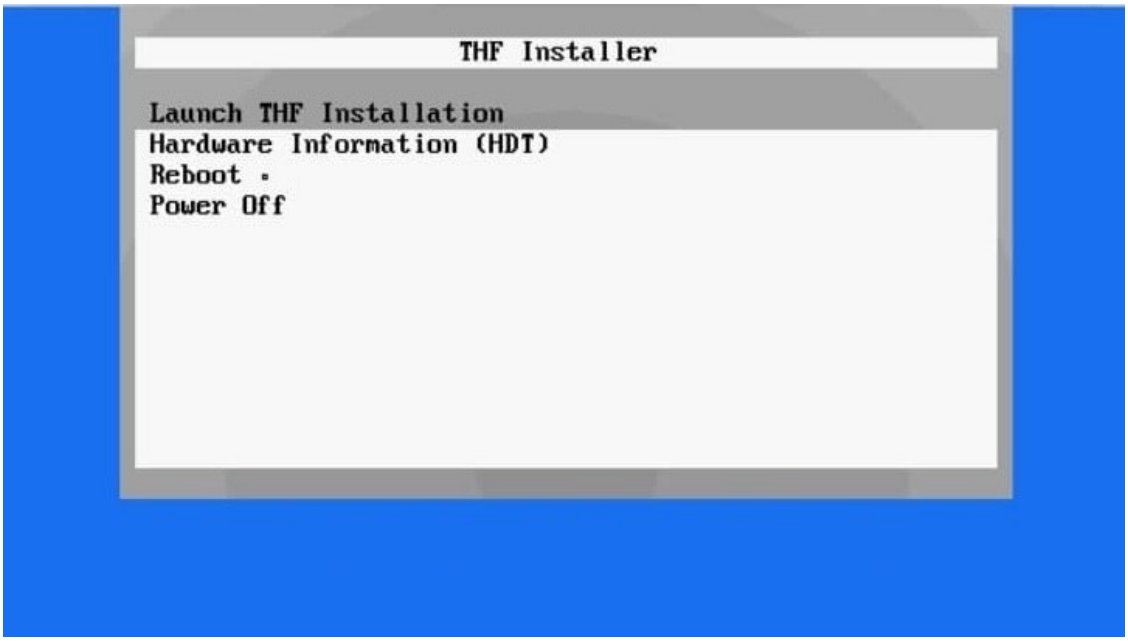
1. Во время загрузки с образа на экране появится меню установщика MXDR **MXDR Console**, которое содержит следующие пункты:

– **Launch MXDR 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

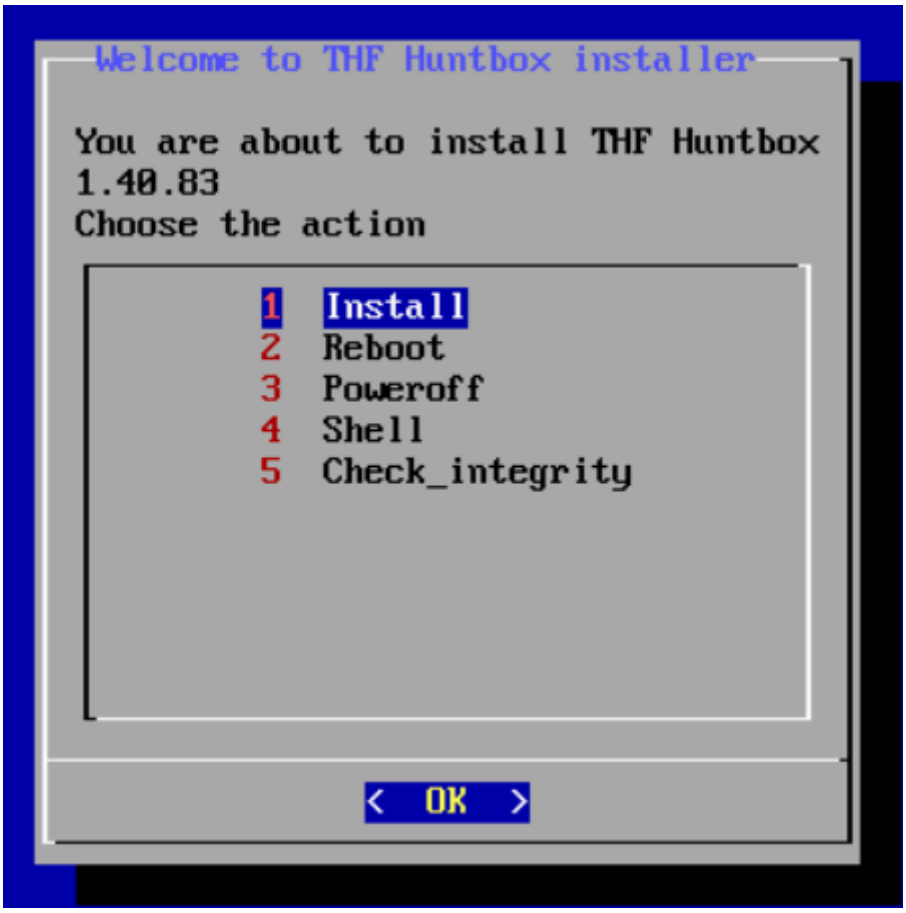
– **Power Off** – выключает сервер



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

2. Меню содержит следующие пункты:

- **Install** – запускает процесс установки
- **Reboot** – перезагружает сервер
- **Poweroff** – выключает сервер
- **Shell –** загружает командную строку
- **Check_integrity** — открывает меню проверки целостности



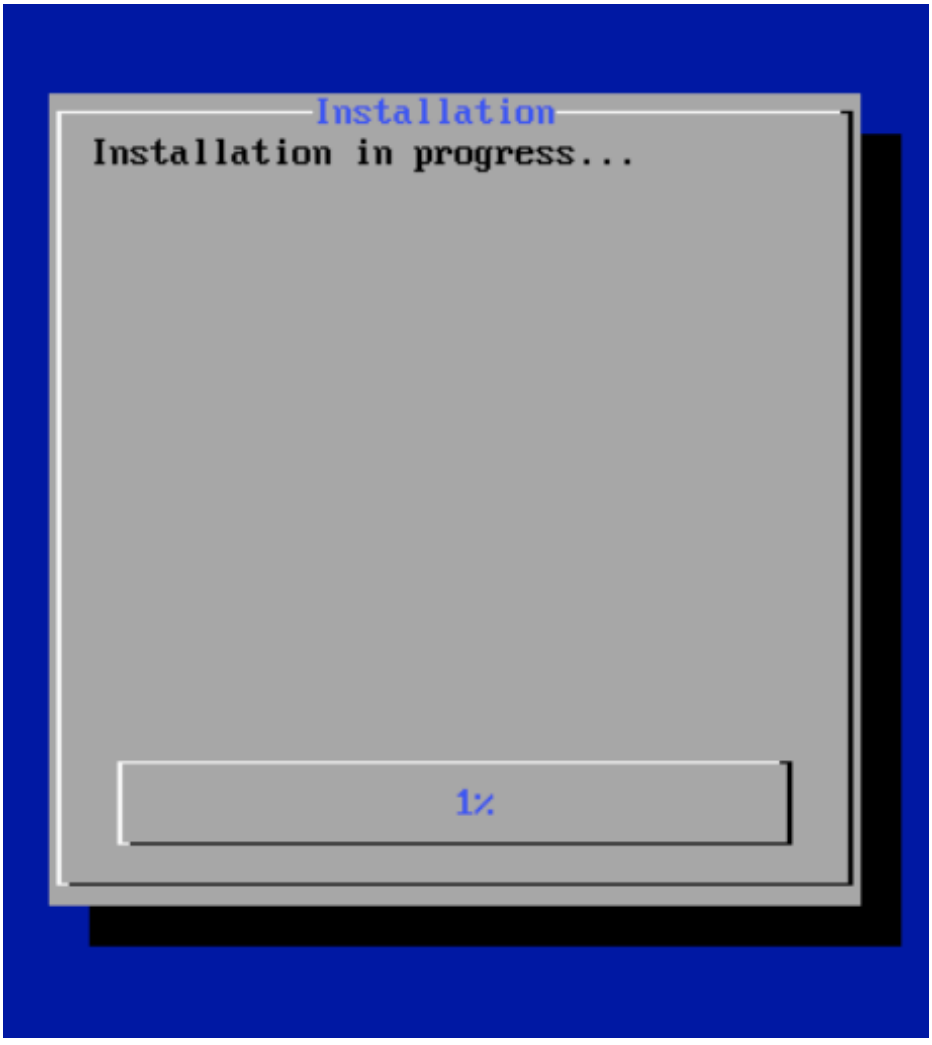
При выборе пункта **`Install`** пользователю предлагается прочитать лицензионное соглашение на русском или английском языках.

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

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

4. Выберете диск, дождитесь окончания процесса установки и процесса настройки файловой системы.


Select installation disk
Select disk
0 /dev/sdb:[]
1 /dev/sda:[1200GB]
< OK >
<Cancel>


Installation
Installation in progress...
1%

После перезагрузки загрузится командная строка **MXDR Console**. Можно будет перейти к настройке и активации решения.

3.3 Подключение к консоли MXDR Console

Консоль **MXDR 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

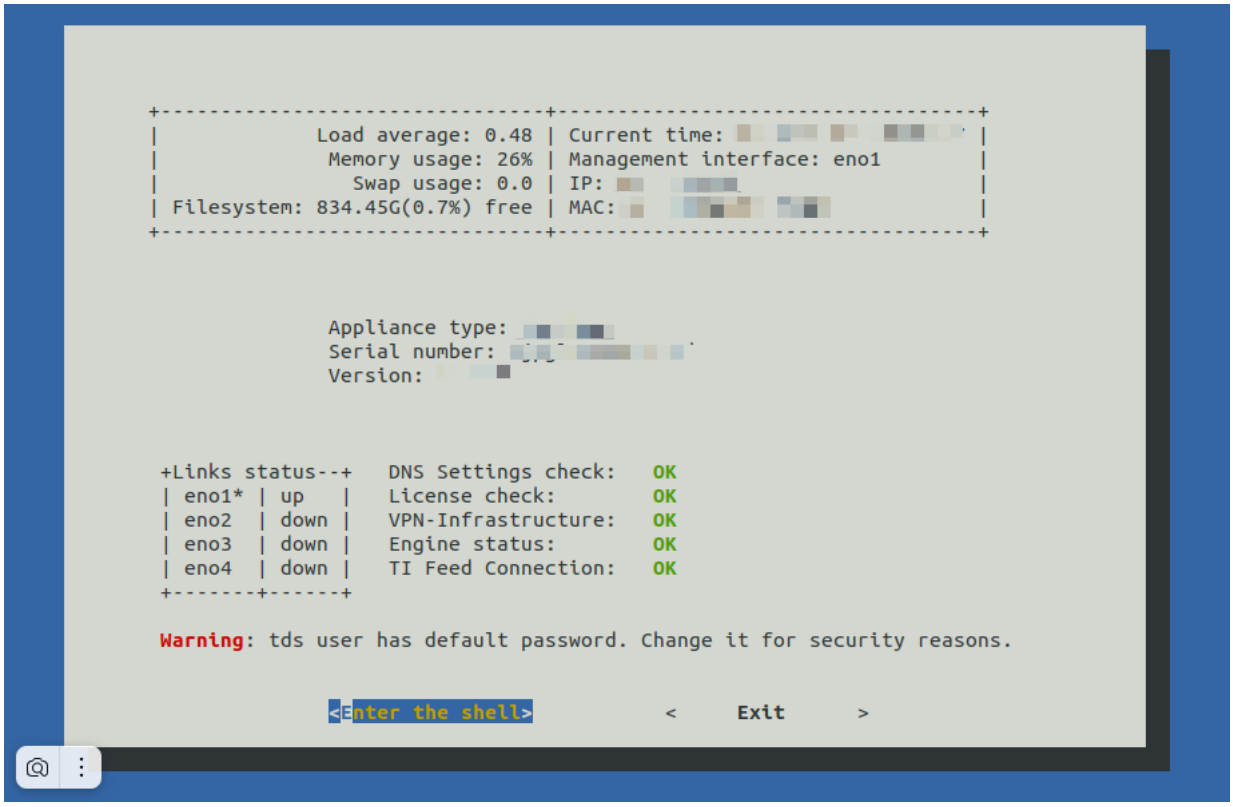
3.4 Логин / Пароль консоли MXDR Console

Для управления сервером авторизуйтесь, используя следующие учетные данные:

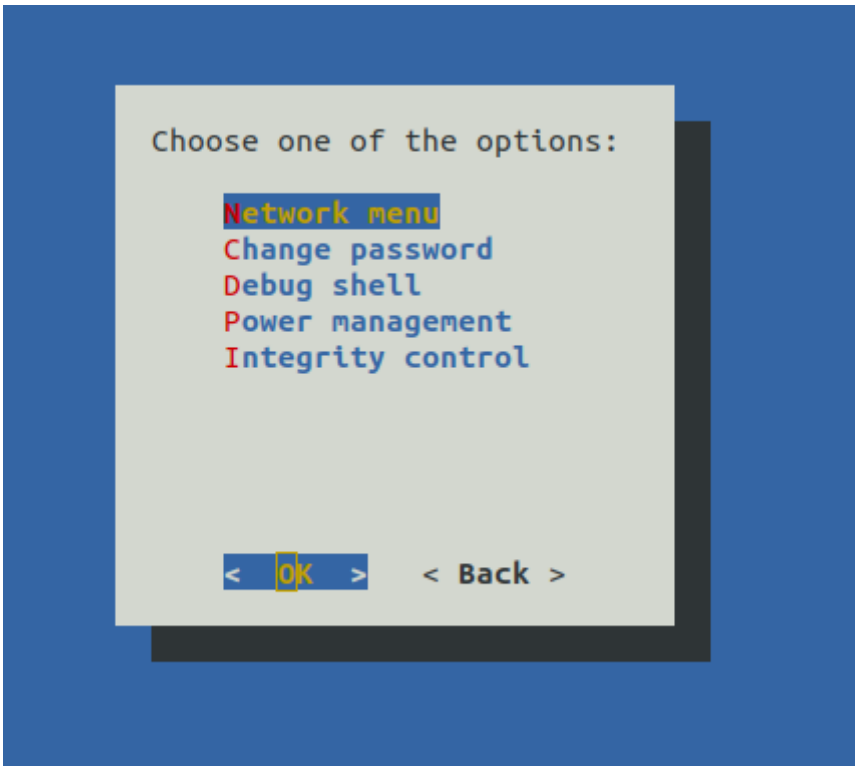
Логин: `tds`

Пароль: `tds`

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



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



3.5 Настройка сети MXDR Console

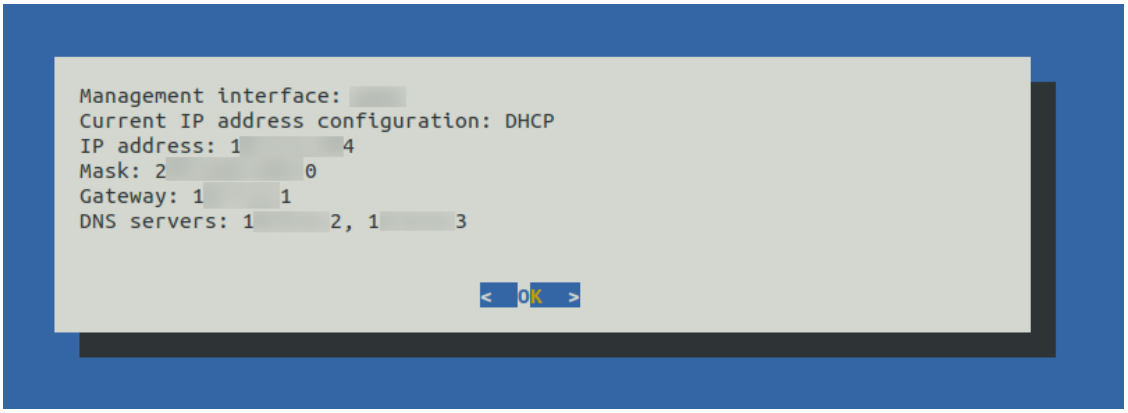
Пункты главного меню:

- **Show current network settings** — просмотр и изменение настройки сети
- **Configure network** — настройки сети
- **Configure proxy** — настройки прокси
- **Configure management interface** — настройки интерфейса управления
- **Reactivation** — повторная активация
- **< Back >** — вывод основной информации о статусе сервера. Эта информация также выводится при входе в систему

3.5.1 Configure network

Доступны следующие варианты настроек:

- **DHCP** - автоконфигурация адреса и прочих настроек по протоколу **DHCP**. Производится автоконфигурация интерфейса и перезапуск сети
- **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**
- **Cancel** - возврат на уровень меню выше



3.5.2 Configure proxy

Настройка прокси-сервера для доступа к обновлениям и облачному сервису **MXDR 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`.

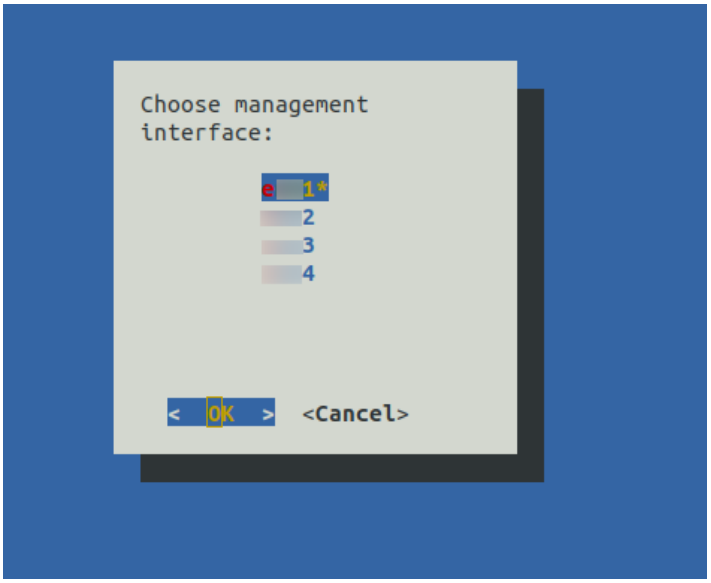
Проверьте введенные значения:

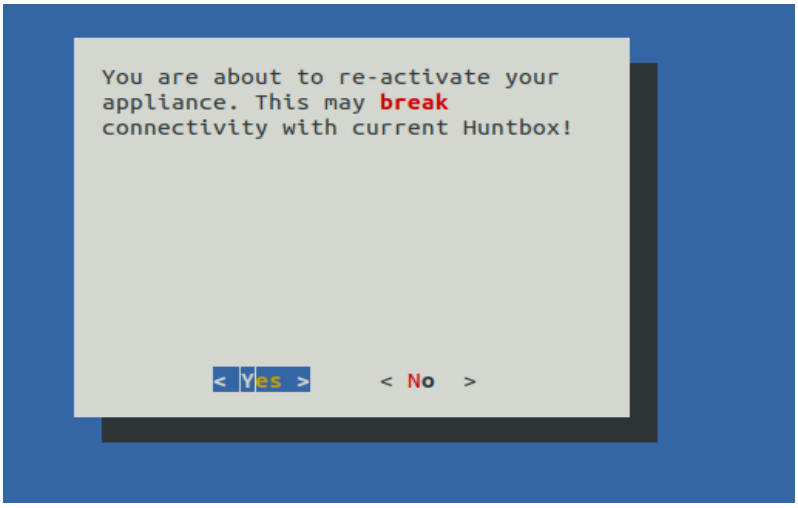
`Proxy Settings` → `Show current proxy settings`

Для успешного использования прокси-сервера сервер должен поддерживать метод **`CONNECT`** с открытием соединений на **443** порт.

3.5.3 Configure management interface

В данном меню предоставляется возможность выбора управляющего интерфейса из доступных на **MXDR Console**. Управляющий интерфейс будет использоваться всеми компонентами для работы с **MXDR Console**.





3.5.4 Debug Shell

Debug Shell предоставляет низкоуровневые инструменты для анализа сетевого подключения и анализа состояния устройства.

```
Avaliable commands are:
  list_interfaces -- list ethernet interfaces and their properties
  http-monitor -- watch http traffic on all interfaces
  bwm-ng -- network bandwidth monitor
  telnet -- check connection to arbitrary address/port
  mtr -- display network route to arbitrary host
  tcpdump -- watch tcp packet stream on chosen interface
  ping -- check arbitrary host availability
Press Ctrl+D to return to TDS menu
tds-debug:
```

– **list_interfaces** — список интерфейсов с обозначением как работающих, так и отключенных, также с обозначаем управляющего интерфейса

– **http-monitor** — показывает http сессии, выявленные в **SPAN** трафике

– **bwm-ng** — монитор загруженности интерфейсов в реальном времени

Для открытия страницы помощи нажмите **h**.

```
bwm-ng v0.6.2 (probing every 0.500s), press 'h' for help
input: /proc/net/dev type: rate
/         iface                   Rx                   Tx                Total
==============================================================================
          eno4:           0.00 KB/s            0.00 KB/s            0.00 KB/s
          tun1:           4.26 KB/s            2.20 KB/s            6.46 KB/s
            lo:         836.17 KB/s          836.17 KB/s         1672.34 KB/s
          eno3:           0.00 KB/s            0.00 KB/s            0.00 KB/s
       eno2np1:           0.00 KB/s            0.00 KB/s            0.00 KB/s
       eno1np0:           0.00 KB/s            0.00 KB/s            0.00 KB/s
------------------------------------------------------------------------------
         total:         840.43 KB/s          838.37 KB/s         1678.80 KB/s
```

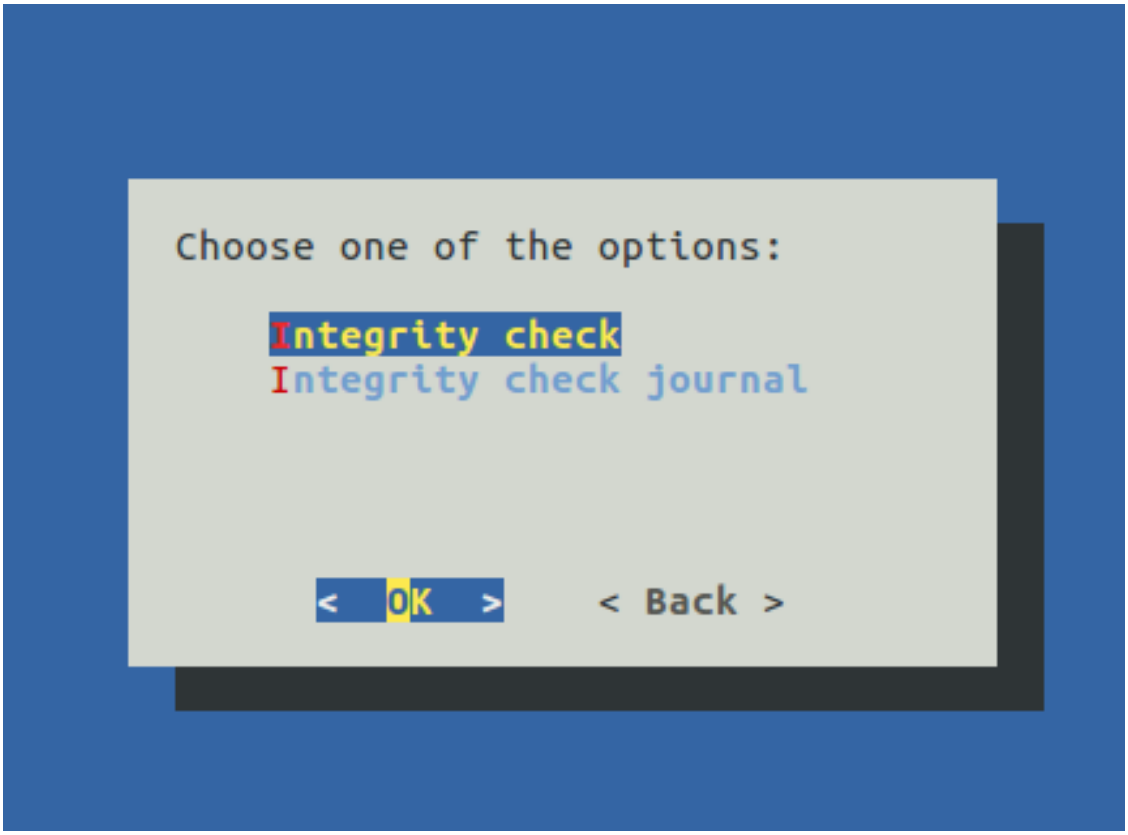
– **telnet** — стандартная утилита проверки telnet соединения

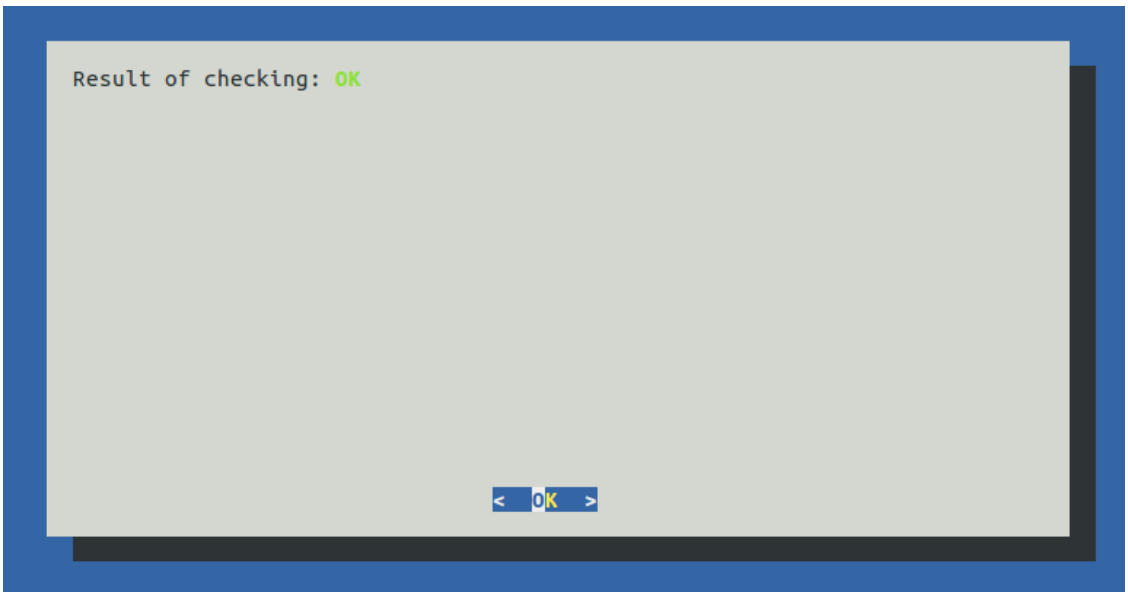
– **mtr** — трассировка сети

- **tcpdump** — стандартная утилита снятия дампа трафика
- **ping** — стандартная утилита ping

3.5.5 Проверка целостности ПО

Меню позволяет проверять целостность программного обеспечения продукта.

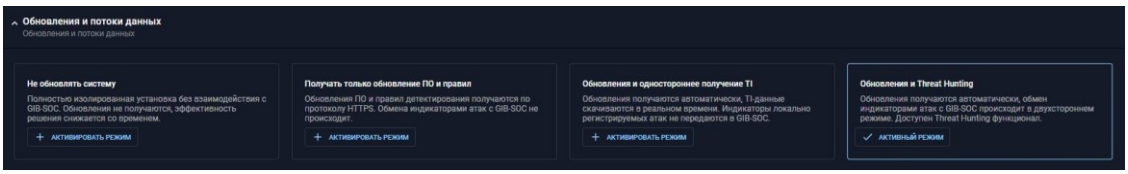




```
2019-08-15 16:06:52,759 Started integrity check
2019-08-15 16:06:52,759 pki/serializers.py: Check is OK
2019-08-15 16:06:52,759 pki/apps.py: Check is OK
2019-08-15 16:06:52,759 pki/views.py: Check is OK
2019-08-15 16:06:52,759 pki/utils.py: Check is OK
2019-08-15 16:06:52,760 pki/__init__.py: Check is OK
2019-08-15 16:06:52,760 pki/models.py: Check is OK
2019-08-15 16:06:52,760 pki/migrations/__init__.py: Check is OK
2019-08-15 16:06:52,760 authentication/urls.py: Check is OK
2019-08-15 16:06:52,760 authentication/backends.py: Check is OK
2019-08-15 16:06:52,760 authentication/serializers.py: Check is OK
2019-08-15 16:06:52,760 authentication/apps.py: Check is OK
2019-08-15 16:06:52,761 authentication/views.py: Check is OK
2019-08-15 16:06:52,761 authentication/utils.py: Check is OK
2019-08-15 16:06:52,761 authentication/__init__.py: Check is OK
2019-08-15 16:06:52,761 authentication/migrations/__init__.py: Check is OK
2019-08-15 16:06:52,761 activation/urls.py: Check is OK
2019-08-15 16:06:52,761 activation/serializers.py: Check is OK
2019-08-15 16:06:52,762 activation/apps.py: Check is OK
2019-08-15 16:06:52,762 activation/views.py: Check is OK
2019-08-15 16:06:52,762 activation/__init__.py: Check is OK
2019-08-15 16:06:52,762 activation/migrations/__init__.py: Check is OK
2019-08-15 16:06:52,762 devices/filtersets.py: Check is OK
2019-08-15 16:06:52,762 devices/management/__init__.py: Check is OK
2019-08-15 16:06:52,762 devices/management/commands/update_appliance_status.py: Check is OK
2019-08-15 16:06:52,763 devices/management/commands/__init__.py: Check is OK
2019-08-15 16:06:52,763 devices/locale/ru/LC_MESSAGES/django.mo: Check is OK
2019-08-15 16:06:52,763 devices/locale/ru/LC_MESSAGES/django.po: Check is OK
2019-08-15 16:06:52,763 devices/serializers.py: Check is OK
2019-08-15 16:06:52,763 devices/apps.py: Check is OK
2019-08-15 16:06:52,764 devices/views.py: Check is OK
2019-08-15 16:06:52,764 devices/utils.py: Check is OK
2019-08-15 16:06:52,764 devices/__init__.py: Check is OK
2019-08-15 16:06:52,764 devices/models.py: Check is OK
2019-08-15 16:06:52,764 devices/migrations/0006_appliance_state.py: Check is OK
2019-08-15 16:06:52,764 devices/migrations/0014_appliance_new_company.py: Check is OK
2019-08-15 16:06:52,765 devices/migrations/0003_auto_20180703_1615.py: Check is OK
2019-08-15 16:06:52,765 devices/migrations/0019_auto_20190123_1303.py: Check is OK
2019-08-15 16:06:52,765 devices/migrations/0016_auto_20181029_1430.py: Check is OK
2019-08-15 16:06:52,765 devices/migrations/0007_appliance_appliance_status.py: Check is OK
2019-08-15 16:06:52,765 devices/migrations/0020_auto_20190227_1235.py: Check is OK
2019-08-15 16:06:52,765 devices/migrations/0015_remove_appliance_company.py: Check is OK
2019-08-15 16:06:52,766 devices/migrations/0008_auto_20180730_1356.py: Check is OK
2019-08-15 16:06:52,766 devices/migrations/0018_endpoint.py: Check is OK
2019-08-15 16:06:52,766 devices/migrations/0012_galaxy_to_huntbox.py: Check is OK
2019-08-15 16:06:52,766 devices/migrations/0002_auto_20180703_1439.py: Check is OK
2019-08-15 16:06:52,766 devices/migrations/0013_change_types_in_appliance.py: Check is OK
2019-08-15 16:06:52,766 devices/migrations/0010_auto_20180731_1614.py: Check is OK
2019-08-15 16:06:52,766 devices/migrations/__init__.py: Check is OK
2019-08-15 16:06:52,767 devices/migrations/0017_auto_20181029_1718.py: Check is OK
2019-08-15 16:06:52,767 devices/migrations/0011_auto_20180911_1243.py: Check is OK
2019-08-15 16:06:52,767 devices/migrations/0009_auto_20180731_1318.py: Check is OK
2019-08-15 16:06:52,767 devices/migrations/0005_appliance_company.py: Check is OK
2019-08-15 16:06:52,767 devices/migrations/0001_initial.py: Check is OK
2019-08-15 16:06:52,767 devices/migrations/0004_auto_20180706_1410.py: Check is OK
2019-08-15 16:06:52,767 devices/managers.py: Check is OK
2019-08-15 16:06:52,768 logger/sql.py: Check is OK
2019-08-15 16:06:52,768 logger/filtersets.py: Check is OK
2019-08-15 16:06:52,768 logger/mixins.py: Check is OK
2019-08-15 16:06:52,768 logger/signals.py: Check is OK
2019-08-15 16:06:52,768 logger/locale/ru/LC_MESSAGES/django.mo: Check is OK
2019-08-15 16:06:52,768 logger/locale/ru/LC_MESSAGES/django.po: Check is OK
2019-08-15 16:06:52,769 logger/serializers.py: Check is OK
```

3.6 Обновления и потоки данных

Данная настройка определяет способ и типы данных, которыми будет обмениваться **MXDR Console** с инфраструктурой компании АО БУДУЩЕЕ.



3.6.1 Не обновлять систему

Обновление программного обеспечения, IOC-ов и сетевых сигнатур не производится. Отсутствует взаимодействие с инфраструктурой нашей компании.

3.6.2 Получать только обновления ПО и правил

Обмен событиями безопасности с облачной инфраструктурой не осуществляется. Возможны только односторонние обновления сигнатур, IOC и системного программного обеспечения.

3.6.3 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 **Threat Intelligence**. Обмен информацией происходит по защищенным каналам. Для **MXDR Console** необходим доступ до серверов – по порту 443/tcp. События ИБ и уведомления по ним в **MXDR** не передаются. Имеется возможность активации аккаунта удаленной технической поддержки.

3.6.4 Обновления + Threat Hunting

Система работает в полнофункциональном режиме. Автоматически загружаются обновления сигнатур и ПО. **MXDR Console** автоматически получает информацию из системы **Threat Intelligence**, поэтому имеется возможность осуществлять Threat Hunting. События ИБ передаются в **MXDR** и пользователь системы может получать поддержку от экспертов **Центра кибербезопасности** в режиме 24/7. Все данные передаются по защищенным каналам.

Для **MXDR Console** необходим доступ до серверов - `443/tcp`

Имеется возможность активации аккаунта удаленной технической поддержки.

4 Сценарии проверки работоспособности ПО

4.1 Локальное размещение «F6 XDR» (On-prem)

4.1.1 Проверка физической работоспособности «F6 XDR»

1. Проверить наличие и размещение оборудования Системы.
   Результат: Сервер установлен в серверную стойку.

2. Проверить подачу питания на серверы Системы.
   Результат: наличие подключения блоков питания сервера к сети электропитания.

3. Проверить интеграцию с инфраструктурой заказчика.
   Результат: необходимые сетевые интерфейсы подключены к локальной сети заказчика.

4. Убедиться, что оборудование включается при нажатии кнопки включения.

4.1.2 Проверка корректности загрузки исполняемого программного обеспечения «F6 XDR»

После корректной загрузки программного обеспечения на устройствах Системы отображается поле для ввода логина и пароля на вход в программную оболочку.

4.1.3 Проверка работоспособности интерфейса «F6 XDR»

1. Перейти по адресу локальной MXDR Console и ввести учетные данные пользователя системы.

2. После успешного входа должны появиться панель управления и разделы MXDR Console в соответствии с ролью пользователя.

3. Перейти в Профиль пользователя → Безопасность и доступ → Двухфакторная аутентификация → Защитить аккаунт. После нужно отсканировать QR код в приложении для двойной аутентификации и ввести 6 цифр которые выдаст приложение для аутентификации.

4.1.4 Проверка режима обновления «F6 XDR»

Перейти в раздел Настройки → MXDR Console → Основные настройки → Обновления и потоки данных и проверить совпадение режима в соответствии с выбранным режимом проведения пилота.

4.1.5 Проверка наличия дочерних лицензий

1. Перейти в Настройки → Лицензии и сверить выписанные лицензии с требующимися лицензиями для реализации проекта.

2. Перейти в раздел Настройки → Модули и создать устройства в соответствии с имеющимися лицензиями (если это не было сделано ранее).

4.2 Облачное размещение «F6 XDR»

4.2.1 Проверка работоспособности интерфейса «F6 XDR»

1. Перейти по адресу MXDR Console и ввести учетные данные пользователя системы.

2. После успешного входа должны появиться панель управления и разделы MXDR Console в соответствии с ролью пользователя.

3. Перейти в Профиль пользователя → Безопасность и доступ → Двухфакторная аутентификация → Защитить аккаунт. После нужно отсканировать QR код в приложении для двойной аутентификации и ввести 6 цифр которые выдаст приложение для аутентификации.

4.2.2 Проверить наличие дочерних лицензий

1. Перейти в Настройки → Лицензии и сверить выписанные лицензии с требующимися лицензиями для реализации проекта.

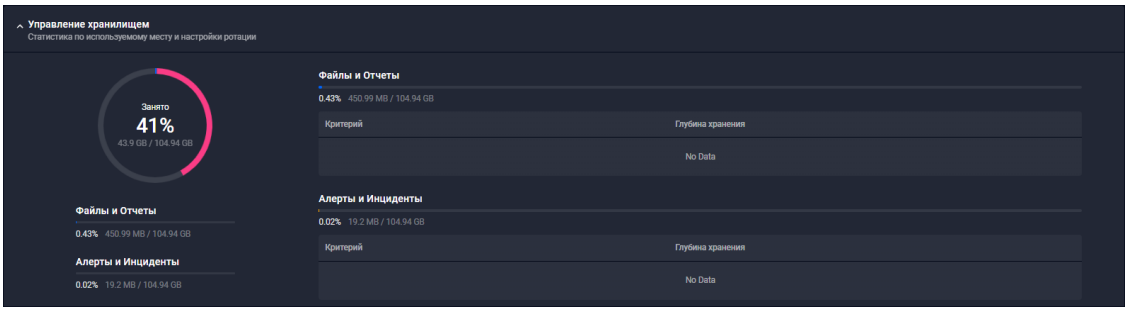
2. Перейти в раздел Настройки → Модули и создать устройства в соответствии с имеющимися лицензиями (если это не было сделано ранее).

5 Администрирование «F6 XDR»

Настройки, описанные в данном разделе, доступны как для устройств **MXDR Console On-prem**, так и для **MXDR Console Cloud**. Для некоторых опций введены исключения, которые обозначены в описании каждой настройки.

5.1 Управление хранилищем (только для «F6 XDR» On-prem)

В данном разделе настроек отображается статистика заполнения хранилища, включая глубину хранения для различных категорий данных, сортированных по критериям.



Доступны следующие категории данных:

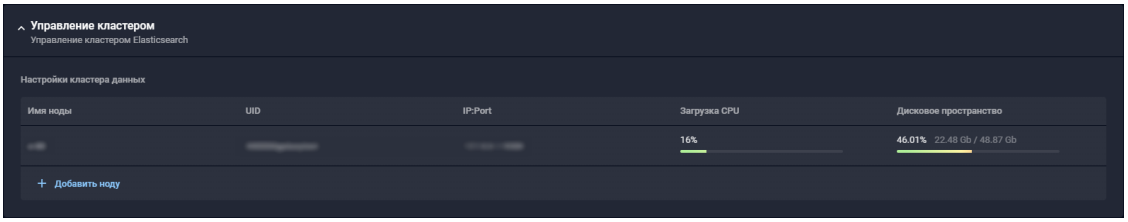
- Файлы и Отчеты;
- Алерты и Инциденты;
- Системные логи;
- События Huntpoint;
- Почта;
- Метаинформация о Сетевых Соединениях;
- Занято системой.

5.2 Управление кластером (только для «F6 XDR» On-prem)

Для MXDR Console Cloud опция доступна только в режиме Read-only.

Данная настройка позволяет увеличить объем хранилища **MXDR Console**.

Для этого необходимо создать кластер, состоящий из устройства **MXDR Console** и как минимум двух устройств Data Storage.



Для создания кластера:

1. Нажмите **Добавить ноду.**

Появится окно с доступными нодами.

2. Выберите необходимые ноды **Data Storage** и нажмите **Добавить** в соответствующих строках.

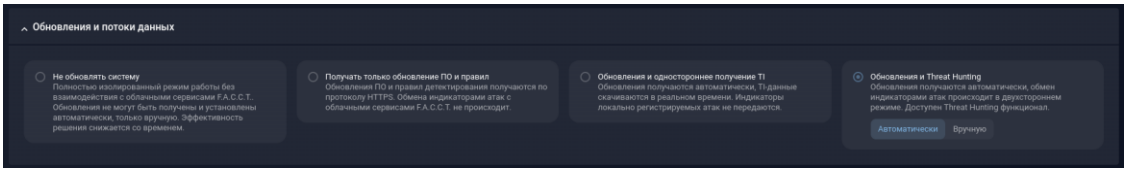
Примечание – Устройство MXDR Console включено в кластер по умолчанию

MXDR Console проверяет **UUID** нод **Data Storage** и при успешной проверке добавляет их в кластер. При неудачной проверке, в колонке статус напротив соответствующего устройства появится сообщение об ошибке. Если ошибка исправлена, нажмите **Повторить**.

5.3 Обновления и потоки данных (только для MXDR Console On-prem)

*Примечание – для **MXDR Console Cloud** опция доступна только в режиме Read-only. Для облачного интерфейса доступно только переключение режима обновлений Ручной <-> Автоматический.*

Данная настройка определяет способ и типы данных, которыми будет обмениваться **MXDR Console** с инфраструктурой АО БУДУЩЕЕ.



5.3.1 Режимы работы

Не обновлять систему Обновление программного обеспечения, IOC-ов и сетевых сигнатур не производится. Отсутствует взаимодействие с инфраструктурой нашей компании.

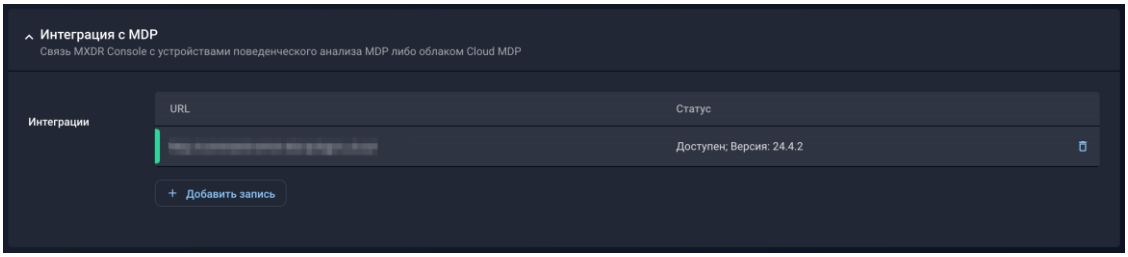
Получать только обновление ПО и правил Обмен событиями безопасности с облачной инфраструктурой не осуществляется. Возможны только односторонние обновления сигнатур, IOC и системного программного обеспечения.

Обновления и 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 **Threat Intelligence**. Обмен информацией происходит по защищенным каналам. Для **MXDR Console** необходим доступ до серверов - 443/tcp. События ИБ и уведомления по ним в MXDR не передаются. Имеется возможность активации аккаунта удаленной технической поддержки.

Обновления и Threat Hunting Система работает в полнофункциональном режиме. Автоматически загружаются обновления сигнатур и ПО. **MXDR Console** автоматически получает информацию из системы **Threat Intelligence**, поэтому имеется возможность осуществлять Threat Hunting. События ИБ передаются в MXDR и пользователь системы может получать поддержку от экспертов **Центра кибербезопасности** в режиме 24/7. Все данные передаются по защищенным каналам. Для **MXDR Console** необходим доступ до серверов - 443/tcp Имеется возможность активации аккаунта удаленной технической поддержки.

5.4 Интеграция с MDP

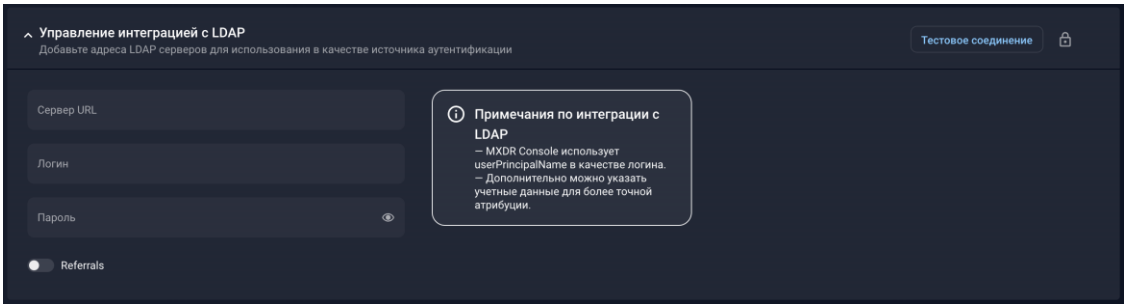
Данная настройка предлагает возможность интегрировать выбранный **MXDR Console** с определенным модулем **Malware Detonation Platform** для осуществления функций поведенческого анализа.



В меню задаётся запись в виде DNS имени или IP адреса MDP. Существует возможность задавать более одной записи, чтобы обеспечить распределение нагрузки по поведенческому анализу. Управление очередью производится на стороне **MXDR Console**. **MXDR Console** делает опрос всех подключённых к нему MDP на предмет размера очереди поведенческого анализа и выбирает минимальную для следующего анализа.

5.5 Управление интеграцией с LDAP

При помощи данной настройки можно добавить в **MXDR Console** адреса LDAP-серверов, которые будут использованы в качестве источников аутентификации.



*Примечание – прежде чем настроить интеграцию с LDAP убедитесь, что на сервере LDAP присутствует база данных **Active Directory (AD)** для управления пользователями системы.*

В настройке доступны следующие поля ввода данных:

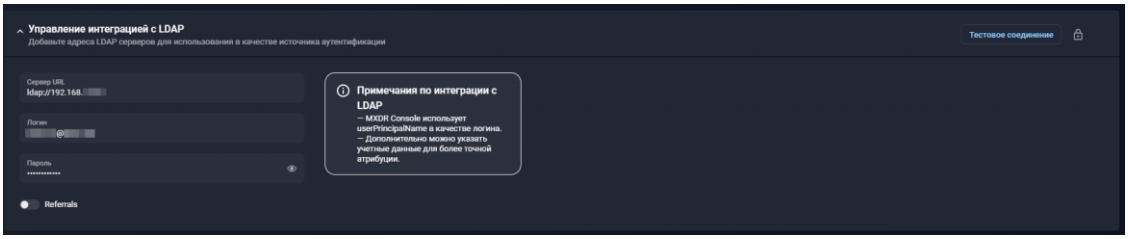
Поле	Описание
Сервер URL	Ссылка на LDAP-сервер. Ссылка должна быть указана с указанием схемы шифрования. Для незашифрованных **LDAP** серверов ссылка будет выглядеть следующим образом: ldap://<ссылка_на_сервер> Для зашифрованных LDAPS серверов ссылка будет выглядеть так: ldaps://<ссылка_на_сервер>. По-умолчанию MXDR Console использует порт 389.
Логин	Логин учетной записи, которая будет использоваться для операций администрирования на сервере LDAP. Должна быть введена в форме почтового адреса. Пример: name.domain.com
Пароль	Пароль от учетной записи.

Опция Referrals отвечает за свойство взаимодействия с контроллером (OPT_REFERRALS). При активации LDAP-сервер будет возвращать не результат запроса, а ссылку на другой сервер, где может содержаться дополнительная информация.

Прежде чем сохранить изменения можно проверить соединение с LDAP-сервером при помощи кнопки **Тестовое соединение**

5.5.1 Схема настройки интеграции с LDAP

1. Заполните поля **Сервер URL**, **Логин**, **Пароль**. При необходимости активируется опция **Referrals**.



2. Перед сохранением протестируйте соединение кнопкой **Тестовое соединение**. Нажмите **Сохранить**, если тестовое соединение прошло успешно.

3. Перейдите в раздел **Моя компания** → **Сотрудники**. Синхронизируйте список сотрудников при помощи кнопки в правом верхнем углу страницы.

4. Нужные пользователи из базы AD появятся в списке сотрудников. Нажмите кнопку `Привязать`, чтобы связать пользователей из **AD** и **MXDR Console** и разрешить доступ к веб-интерфейсу **MXDR Console**. Кнопка появится при наведении курсора на строку с определенным сотрудником.

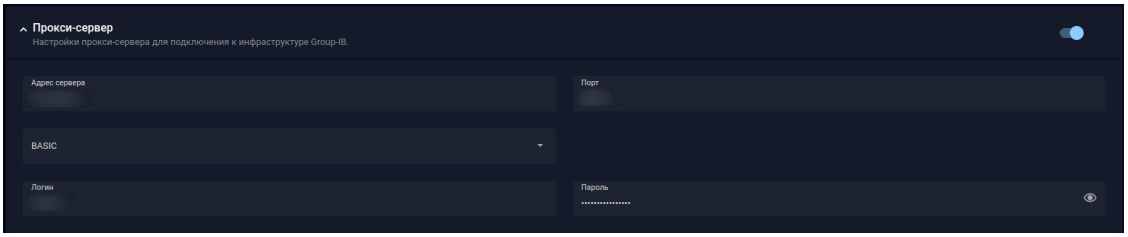
*Примечание – доступ к **MXDR Console** по учетным данным **AD** возможен только если учетные записи сотрудников в **MXDR Console** и **AD** связаны при помощи кнопки `Привязать`.*

5.6 Прокси-сервер

Для работы **MXDR Console** во всех режимах исключая первый (Не обновлять систему) системе необходима связь с серверами нашей компании. Данное подключение может осуществляться через прокси сервера.

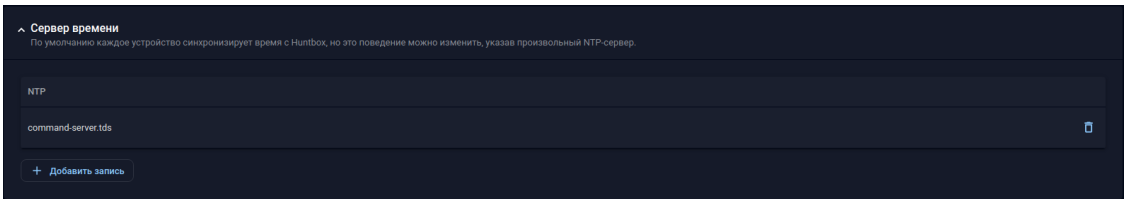
Доступные настройки:

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



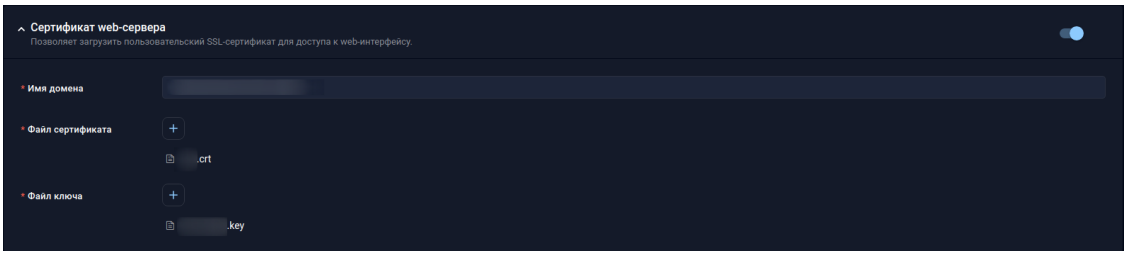
5.7 Сервер времени

В настройках сервера NTP возможно задать адрес сервера синхронизации времени для всех устройств Network Traffic Analysis, подключенных к данному **MXDR Console** серверу. Все подключенные Network Traffic Analysis и Malware Detonation Platform синхронизируют своё время с **MXDR Console**.



5.8 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 **MXDR Console** для домена которого выписан сертификат.

5.9 Настройки почтового сервера

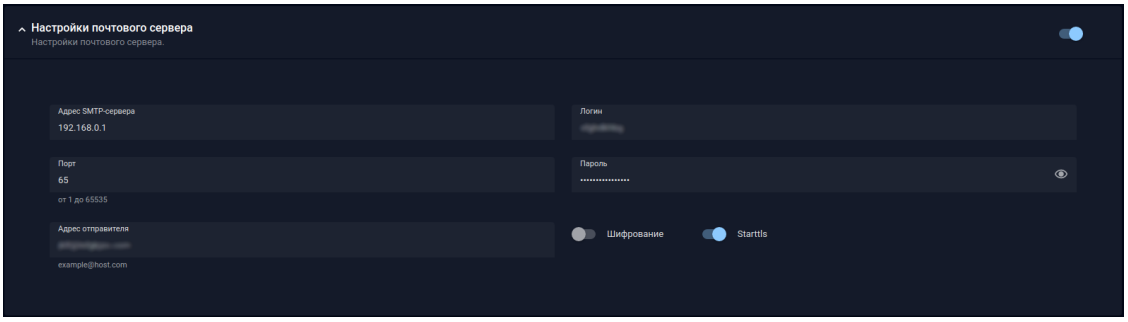
Данная настройка задаёт почтовый сервер и аккаунт для рассылки сообщений для аналитиков комплекса. Рассылка осуществляется индивидуально по сработанным инцидентам. Рассылка настраивается в соответствующих настройках аккаунта пользователей в разделе **Пользователи**.

- **Адрес SMTP-сервера** – Domain или IP адрес внутреннего сервера клиента, от имени которого будет производиться рассылка оповещений;
- **Логин** – для пользователя на локальном SMTP сервере;
- **Порт** – порт, используемый для подключения к SMTP серверу.

*Примечание – обратите внимание на используемые директивы **Шифрование** и **Strarttls** ниже в настройках. В зависимости от настроек SMTP сервера порты могут быть различаться.*

- **Пароль** – аутентификационные данные для логина на SMTP сервере

- **Адрес отправителя** – почтовый адрес в формате **name@domain**, чья запись будет подставляться в поле mail from при рассылке оповещений
- **Шифрование** – активация использования SMTP over TLS
- **Starttls** – использование директивы STARTLS на этапе согласования SMTP.



5.10 Сервер событий EDR

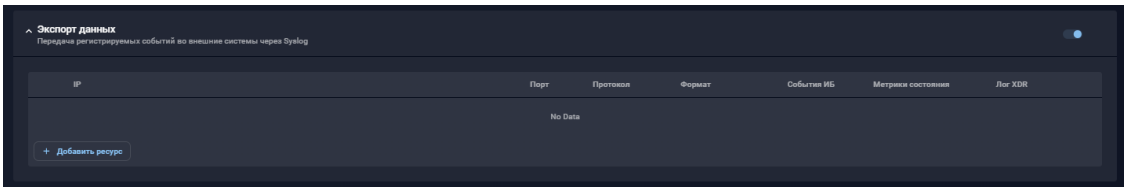
Сервер управления **Endpoint Detection and Response**.

Активирует сервер для агентов на конечных станциях с ОС Windows, следящих за системной активностью и отправляющих события на **MXDR Console** для анализа и последующей реакции. Является решением типа Behavior Inspection & Host Forensics.

5.11 Экспорт данных (только для MXDR Console On-prem)

В **MXDR Console On-prem События ИБ** и **Метрики состояния** экспортируются аналогично экспорту данных в настройках модуля **NTA**.

В **MXDR Console On-prem** доступна опция экспорта **Логи XDR**.



5.11.1 Лог XDR в формате JSON

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

Поле	Описание
`date_time`	Дата и время события.
`type`	Тип события.
`email`	Email адрес.

Поле	Описание
ip	IP адрес.
url	URL адрес.

Пример лога XDR в формате JSON приведен ниже:


```
{
    "date_time": "2024-04-25T16:16:47.699288+00:00",
    "type": "attachment analyzed",
    "message": "Романова_апрель2024_21.pdf: The file has been analyzed in 181 seconds.
Verdict: Benign (0.0%)",
    "email": "",
    "ip": "",
    "url": ""
}
```


5.11.2 Лог XDR в формате CEF

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

Поле	Описание
timestamp	Дата и время создания события в формате UTC.
hostname	UUID устройства в системе MXDR, проводящего анализ письма.
src	Порт источника события.
suser	Отправитель.
duser	Получатель.
cs1	Тип события.
cs1Label	Всегда имеет значение type
cs2	Описание события.
cs2Label	Всегда имеет значение message
cs3	Ссылка.
cs3Label	Всегда имеет значение link
rt	Дата и время отправки текущего сообщения в формате UTC.

Пример лога XDR в формате CEF приведен ниже:


```
 <timestamp> <hostname> CEF:0| company_name|XDR|1.1|0|LOGS|0|src= suser= duser=None cs
1=attachment analyzed cs1Label=type cs2=<file>: The file has been analyzed in 181 seco
nds. Verdict: Benign (0.0%) cs2Label=message cs3= cs3Label=link rt=<time>
```


Примечание – в режиме **On-prem MXDR Console** экспортирует события безопасности от модулей **NTA** и **EDR**.

5.12 SNMP-мониторинг

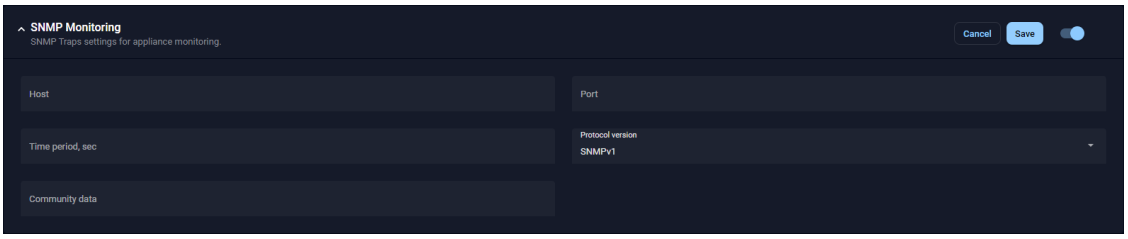
Настройка позволяет обеспечивать мониторинг состояния оборудования, а также мониторинг статистических данных используемых модулей в **MXDR Console**.

Поддерживаемые версии протокола SNMP:

- SNMPv1
- SNMPv2
- SNMPv3

Примечание – при выборе версии протокола появляется возможность задать дополнительные параметры – специфичные для выбранного протокола.

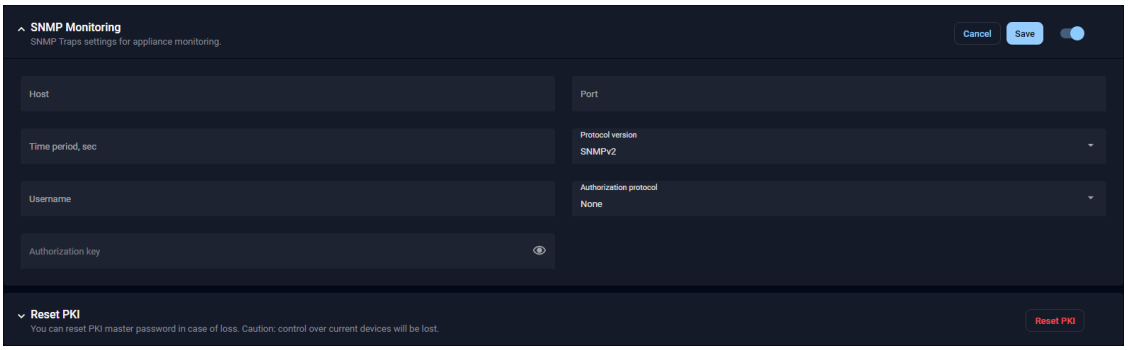
5.12.1 SNMPv1



Доступные настройки:

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

5.12.2 SNMPv2



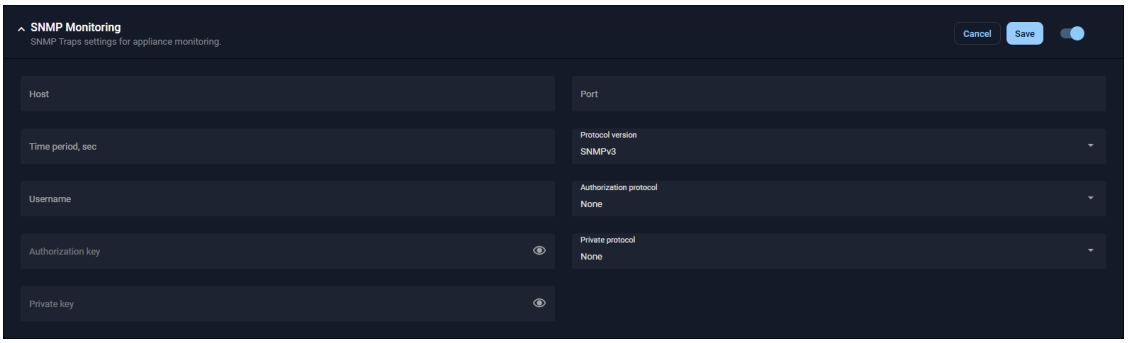
Доступные настройки:

- Адрес сервера
- Порт
- Временной период
- Версия протокола
- Имя пользователя
- Протокол авторизации:
    - None
    - MD5
    - SHA

- SHA224
- SHA256
- SHA384
- SHA512

- Ключ авторизации

5.12.3 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

5.13 Сброс PKI (только для MXDR Console On-prem)

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

6 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка осуществляется в соответствии с условиями контракта следующими способами:

- Приоритетный способ осуществления техподдержки через создание запросов во вкладке «Поддержка» по ссылке https://xdr.f6.security/service-desk
- по электронной почте: info@f6.ru;
- по номеру телефона: +7 495 984-33-64;

В рамках технической поддержки оказываются следующие услуги:

- консультация по фактическому наличию имеющегося функционала в системе;
- помощь в настройке и интеграции ПО;
- помощь в эксплуатации ПО;
- решение технических проблем;
- пояснение принципов работы имеющихся механизмов ПО;
- поиск, тестирование и фиксирование найденных ошибок;
- предоставление актуальной документации по настройке, эксплуатации и работе ПО.

Время работы технической поддержки: с понедельника по пятницу с 9:00 до 18:00 UTC+3.

Фактический адрес размещения службы поддержки ПО «F6 XDR»: 115088, г. Москва, ул. Шарикоподшипниковская, д. 1