ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Endpoint Detection and Response»

Руководство администратора

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Определение
АС	Автоматизированная Система
Заказчик	Зарегистрированный пользователь в системе заказчика передавший третьим лицам все необходимы данные и реквизиты для управления приложением или выполняющий указания третьих лиц за вознаграждение.
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО БУДУЩЕЕ; • Компанией-интегратором, по выбору Заказчика
ОС	Операционная Система
ПО	Программное обеспечение F6 Endpoint Detection and Response.
ТС	(«Технический Сервис») Система взаимодействия Заказчика, позволяющая обмениваться сообщениями и создавать цепочки обращений, которая представляет из себя отдельный раздел «Службу Поддержки» в панели управления «F6 Endpoint Detection and Response». В случае недоступности указанных систем формат взаимодействия осуществляется через электронный почтовый ящик.
APT	Advanced Persistent Threat, постоянная угроза повышенной сложности
DLP	Data Leak Prevention, Предотвращение утечек
IP	Internet Protocol
MAC	Media Access Control
MDP	F6 Malware Detonation Platform
MFT	Master File Table
MXDR	Программный комплекс Managed Extended Detection and Response (Managed XDR)

MXDR Console	F6 XDR, MXDR
NTFS	New Technology File System
pytest	Фреймворк для тестирования кода на Python.
RPM	RPM Package Manager
selenium	Инструмент для автоматизации действий веб-браузера.
SIEM	Security Information and Event Management
UEFI	Extensible Firmware Interface
USB	Universal Serial Bus

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ описывает процесс установки экземпляра программного обеспечения «F6 Endpoint Detection and Response» (далее – ПО, Endpoint Detection and Response, EDR).

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

1.2 Назначение ПО

«F6 Endpoint Detection and Response» — это модуль системы MXDR (Managed XDR) который специализируется на обнаружении, расследовании и реагировании на угрозы, направленные на конечные точки, такие как рабочие станции. ПО обеспечивает защиту от различных киберугроз, включая вредоносное ПО, программы-вымогатели и сложные атаки, такие как APT (Advanced Persistent Threat). При обнаружении угрозы ПО предлагает инструменты для быстрого реагирования на инциденты, что включает изоляцию, расследование и устранение угрозы. Решение также обладает мощными функциями форензики и анализа инцидентов, что помогает понять коренные причины атаки и предотвратить повторные инциденты. ПО поддерживает автоматизацию процессов защиты и позволяет настраивать политики безопасности в соответствии с потребностями организации, а также интегрируется с SIEM и другими системами для комплексного управления инцидентами. ПО доступно в виде клиента для операционных систем Windows, Linux и macOS.

2 ТРЕБОВАНИЯ К СИСТЕМЕ

ПО устанавливается на конечную точку (рабочую машину) или сервер.

2.1 Минимальные технические требования для физического сервера

2.1.1 Минимальные технические требования для оборудования на базе ОС семейства Microsoft Windows

Поддерживаемые операционные системы:

Тип ОС	Версии ОС
Компьютер	Windows 7 SP1 Windows 8 Windows 8.1 Windows 10 Windows 11
Сервер	Windows Server 2008 R2 x64 Windows Server 2012 x64 Windows Server 2012 R2 x64 Windows Server 2016 Windows Server 2019 Windows Server 2022

Минимальные системные требования:

Компонент	Требование
ОЗУ	Не менее 4 Гб
Процессор	Многоядерный процессор Intel® x86-64 не ниже intel **Core i3** или аналогичный
Жесткий диск	не менее **60Gb**, со скоростью не ниже **7200RPM**

2.1.2 Минимальные технические требования для оборудования на базе ОС ядра Linux

Проверенные интеграции:

- Canonical

  - Ubuntu 18.04, Ubuntu 20+

  - `dpkg`: cold installation, hot updating

- Ubuntu Server 18.04, Ubuntu Server 20+

  - `dpkg`: cold installation, hot updating

- Astra Linux 1.7.2, 1.7.3, 1.7.5 SE, 2.12.45, 2.12.46

  - `dpkg`: cold installation, hot updating

- Linux Mint 21*

  - `dpkg`: cold installation, hot updating

- Kali

  - `apt`: cold installation, hot updating

- Debian 11+

  - `dpkg`: cold installation, hot updating

- Kubuntu

  `dpkg`: cold installation, hot updating

- Red Hat

  - CentOS 7.9

    - `yum`: cold installation, hot updating

  - CentOS Stream 8+

    - `yum`: cold installation, hot updating

  - Fedora 33+

    - `dnf`: cold installation, hot updating

  - Oracle 8.6+

    - `dnf`: cold installation, hot updating

  - Oracle Server

  - `dnf`: cold installation, hot updating

- Alt Linux 9+

  - `apt-get`: cold installation, hot updating

- RHEL 7.9+

  - `rpm`: cold installation, hot updating

- Red OS 7.2+

  - `rpm`: cold installation, hot updating

- Arch

  - Arch Linux

    - `pacman`: cold installation, hot updating

  - Manjaro Linux

    - `pacman`: cold installation, hot updating

Минимальные системные требования:

Компонент	Требование
ОЗУ	Не менее 4 Гб
Процессор	Многоядерный процессор Intel® x86-64 не ниже intel **Core i3** или аналогичный
Жесткий диск	не менее **60Gb**, со скоростью не ниже **7200RPM**

2.1.3 Минимальные технические требования для оборудования на базе ОС семейства macOS

Компонент	Требование
ОС	MacOS 10.15.0 Catalina и выше
ОЗУ	Не менее 4 Гб
Процессор	Многоядерный процессор Intel® x86-64 не ниже intel **Core i3** или аналогичный или Apple Silicon (с тактовой частотой не менее 2 ГГц и SSE 4.2 или более поздней версии)
Жесткий диск	не менее **60Gb**, со скоростью не ниже **7200RPM**

.

3 УСТАНОВКА ТЕСТОВОЙ ВЕРСИИ ПО

3.1 Установка Windows EDR

В начале работы с **Windows EDR** могут быть выявлены конфликты с установленным программным обеспечением. Рекомендуется производить последовательную установку ПО на конечные точки инфраструктуры. Достаточно начать с 20 устройств и постепенно увеличивать число установок.

3.1.1 Скачивание пакета с Windows EDR

Скачивание установочных и конфигурационных файлов **Windows EDR** доступно в меню настроек при работе локального **MXDR Console** в 3-м и 4-м режимах, либо при использовании **MXDR Console** в облачном варианте поставки. За консультацией по другим вариантам установки необходимо обращаться к ответственным инженерам нашей компании или инженерам партнеров.

1. Перейдите в раздел **Настройки - Модули** и выберите необходимую группу хостов с Windows EDR.

2. Нажмите на кнопку **Инструкция по установке**и скачайте архив с установочным и конфигурационными файлами **Windows EDR**:

- `gibep.msi`,

- `gibep_config.txt`,

- `gibep_config.sign.txt`.

3. Разархивируйте содержимое в любую директорию (например, в `C:\EDR`).

Полный путь до директории не должен содержать кириллических символов и пробелов.

3.1.2 Установка Windows EDR

Для установки Windows EDR необходимо выполнить следующие действия:

1. Запустите командную строку - `cmd.exe` - от имени Администратора.

2. Перейдите в директорию с установочным и конфигурационными файлами и выполните команду установки **Windows EDR**:

msiexec /i gibep.msi /L*V install.log

3.1.3 Установка для VDI-решений и аналогов

Windows EDR можно использовать для VDI-решений и их аналогов. Для этого выполните следующие действия:

1. Установите все необходимое ПО на мастер-образ.

2. Выполните команду `msiexec` для установки **Windows EDR** с дополнительным ключом `CHGMID=1`:

msiexec /i gibep.msi /L*V install.log CHGMID=1

3. Завершите создание мастер-образа.

В случае возникновения проблем с установкой агента необходимо прислать лог, полученный в результате выполнения команды установки **Windows EDR** `msiexec`.

Мастер-образ в некоторых нотациях принято называть **золотой образ**.

3.1.4 Установка с помощью групповых политик - GPO

Чтобы установить **Windows EDR** через с помощью групповых политик необходимо выполнить следующие действия:

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

2. Откройте консоль **DPM** и создайте политику на нужном уровне. В поле **Security filtering**` уберите **Authenticated Users** и добавьте у/з компьютеров или группы компьютеров, на которых требуется поставить ПО. Правой кнопкой мыши кликните по политике и выберите **Edit**.

3. По адресу **Computer Configuration** → **Polices** → **Software settings** найдите пункт **Software Installation**, правой кнопкой мыши кликните на него и выберите **New** → **Package**:

4. В появившемся окне откройте сетевую папку, в которую ранее положили установщик агента **Windows EDR** и выберите его.

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

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

3.1.5 Проверка установки Windows EDR

1. Запустите командную строку - `cmd.exe` - от имени Администратора.

2. Выполните следующие команды:

"C:\Program Files\... \THF Huntpoint\gibepcli.exe" driver-version

sc queryex "gibthfhuntpoint" | find "STATE"

TASKLIST | find "gibep"

Если системным языком установлен русский, то вторая команда для проверки установки будет следующей: `sc queryex "gibthfhuntpoint" | find "Состояние"`.

В версиях **Windows EDR** ранее 1.1.21 необходимое ПО расположено в папке `TDS Huntpoint`.

После выполнения команд в реестре должны появиться ключи:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GIB*

3.1.6 Структура папки с Windows EDR

Архив с **Windows EDR** будет распакован на устройстве Windows в папку THF Huntpoint:

В версиях ранее 1.1.21 **Windows EDR** устанавливается в папку TDS Huntpoint.

3.2 Установка Linux EDR

3.2.1 Скачивание пакета с Linux EDR

Пакет для установки можно скачать на странице **Настройки** – **Модули** в описании **группы хостов с EDR**, на которых должны быть установлено ПО.

Для этого в таблице модулей выберите нужный модуль с типом **Группа хостов с Linux EDR** и в открывшемся сайдбаре нажмите кнопку **Инструкция по установк**`.

В открывшемся окне нажмите кнопку **Скачать** и выберите из выпадающего списка пакет для необходимого дистрибутива Linux:

Актуальная инструкция для установки пакета зависит от версии и используемого дистрибутива Linux. Она входит в комплект поставки и доступна на портале в разделе ***Инструкция по установке***.

3.2.2 Установка Linux EDR

Все команды выполняются с привилегиями root-пользователя.

Для установки модуля и плагинов **Linux EDR** выполните команды для используемого дистрибутива.

3.2.2.1 Debian-based and RH-based

- установка пакета:

<package manager> install ./<path_to_package>

Начиная с версии агента 2.6.__ необходимые плагины уже включены в установочный пакет. Установка дополнительных плагинов не требуется.

Большинство дистрибутивов выполняют установку через маску: **<package manager> install ./<path_to_linep-*version*>**.

3.2.2.2 Arch-based

- установка пакета:

pacman -U ./<path to package>

Начиная с версии агента 2.6.__ необходимые плагины уже включены в установочный пакет. Установка дополнительных плагинов не требуется.

Большинство дистрибутивов выполняют установку через маску: **<package manager> install ./<path_to_linep-*version***`.

3.2.3 Действия после установки

После установки пакета и плагинов выполните следующие действия:

- Установите конфигурационные файлы:

linepctl config apply <path to config> <path to signature>

- Запустите все сервисы:

systemctl start linep.service

- Проверьте статус работы агента:

systemctl status linep.service

3.2.4 Проверка корректности установки

3.2.4.1 Автоматические проверки

Все команды выполняются с привилегиями root-пользователя.

- Проверка состояния сервисов при помощи терминальной утилиты выполняется с помощью команды:

linepctl status

- Для вывода отчета в определенном формате используйте флаги:

- `--json` для JSON,

- `-c` для текста.

3.2.4.2 Ручные проверки

- Проверка состояния сервисов выполняется с помощью команды:

systemctl status linep.service

- Проверка логов сервиса выполняется с помощью команды:

journalctl -fu linep.service

3.3 Установка MacOS EDR

3.3.1 Скачивание пакета с MacOS EDR

Пакет для установки можно скачать на странице **Настройки** → **Модули** в описании **группы хостов с EDR**, на которых должны быть установлено ПО.

3.3.2 Установка macOS EDR

Для установки MacOS EDR необходимо выполнить следующие действия:

1. Смонтировать образ `edr-macos-installer-any.dmg`.

2. Перенести файл `Group-IB XDR.app` в директорию **Программы**.

3. Запустить `Group-IB XDR.app` из директории **Программы** через **Finder**.

4. В открывшемся предупреждении **Системное расширение заблокировано** перейти в **Системные настройки** и разрешить запуск системного расширения.

5. Вернуться в окно установки **MacOS EDR** и нажать **Продолжить**.

6. Перейти по кнопке **Конфиденциальность и безопасность** и при помощи ползунка разрешить полный доступ к диску для приложения `Group-IB XDR System Extension` в меню **Доступ к диску**.

7. Вернуться в окно установки **MacOS EDR** и нажать **Продолжить**.

8. В окне **Настройка конфигурации** нажать **Выбрать файл** и выбрать файл config.gibedrcondig из скачанного архива. Нажать **Продолжить**.

9. Разрешить приложению фильтровать сетевой трафик в открывшемся окне предупреждения.

10. Нажать **Продолжить** для завершения установки. Приложение будет доступно в отдельной иконке в правой части строки меню.

4 Сценарии проверки работоспособности ПО

4.1.1 Запуск ПО применительно к конечным станциям на базе ОС семейства Microsoft Windows

4.1.1.1 Проверка корректности установки агента на Стенде для проведения тестирования

Для проверки корректности установки агента на конечной станции выполняют следующее тестирование:

1. Проверить, что конечная станция, используемая для тестирования, (далее – Стенд) представляет собой виртуальное окружение и удовлетворяет всем системным требованиям.

2. Проверить, что у Стенда отсутствует сетевой доступ к корпоративной сети организации Заказчика.

3. После установки агента Стенд необходимо перезагрузить.

4. После перезагрузки Стенда перейти в интерфейсе в раздел Моя компания → Активы, выставить быстрый фильтр “Компьютер” и убедиться, что актив Стенда в статусе онлайн (индикатор актива зеленый).

5. Если на Стенде используются снимки файловой системы и был произведен откат, необходимо вернуться на пункт 4.

4.1.1.2 Проверка корректности настроек модуля EDR

1. Перейти в раздел **Настройки** → **Модули** → **Группа хостов с Windows EDR** → **Основные настройки** и активировать опцию **Удаленного терминального доступа**.

2. Проверить, что в разделе **Настройки** → **Модули** → **Группа хостов с Windows EDR** → **Основные настройки** в блоке **События с хостов** для всех категорий событий в колонке **Статус** выставлено значение **Все включены**, кроме категории событий *userModeHooks*, которая должна иметь в колонке **Статус** значение *Отключены: userModeHooks*.

3. Проверить, что на Стенде отключены все сторонние или встроенные средства защиты конечных устройств (Антивирусы, EDR, DLP и т.д.).

4. После применения всех настроек необходимо проверить корректность применения этих настроек на уровне клиента EDR. Для этого необходимо зайти в папку с

агентом, открыть файл Config.txt и проверить, что параметры выставлены в соответствии с настройками в веб-интерфейсе.

5. Далее перейти в раздел **Профиль пользователя → Безопасность и доступ → Двухфакторная аутентификация** и убедиться в наличии статуса *Аккаунт защищен двухфакторной аутентификацией*.

4.1.1.3 Проверка работоспособности функции блокировки ВПО

1. Перейти в раздел **Настройки → Модули → Группа хостов с Windows EDR → Основные настройки** и в блоке **Анализ файлов** включить опцию **Блокировать вредоносные файлы**.

2. Перейти в раздел **Расследование → Проверенные файлы**, выполнить поиск файлов, признанных вредоносными и загрузить один из таких экземпляров и перенести на Стенд.

3. Для корректного и безопасного проведения данного этапа теста крайне не рекомендуется заходить в веб-интерфейс консоли напрямую со Стенда.

4. После того, как загруженный вредоносный файл был помещен на Стенд, его необходимо извлечь из архива, в который он упаковывается для выгрузки из Web-интерфейса (пароль для извлечения указывается при скачивании). Далее необходимо осуществить попытку запуска загруженного вредоносного файла (открыть документ/запустить исполняемый файл/открыть архив).

5. Перейти в раздел **Атаки → Алерты**, выставить фильтр **Система интеграции → Huntpoint**, **Классификатор → Polygon**, выполнить поиск по имени Стенда и найти алерт о попытке открытия заблокированного файла.

4.1.1.4 Проверка работоспособности функции сбора криминалистических артефактов

Для корректного проведения данного тестирования, необходимо убедиться, что роль пользователя аналитик или админ.

1. Перейти в раздел **Моя компания → Активы** выполнить поиск по *machine_id* Стенда → раскрыть в правом верхнем углу меню **Реагирование** → выбрать опцию **Собрать артефакты на хосте**.

2. В открывшемся диалоговом окне выбрать опцию сбора базовых (отладочных) данных.

3. Перейти во вкладку **Реагирование** в раскрытом сайдбаре с информацией о Стенде, выбрать пункт **Артефакты**. Будет доступно отображение всех запрошенных

артефактов со статусом выполнения. По итогу сбора запрошенных на предыдущем шаге данных будет доступна карточка для просмотра и скачивания собранных артефактов.

4.1.1.5 Проверка работоспособности функций удаленного терминального доступа

1. Перейти в раздел **Моя компания** → **Активы** выполнить поиск по *machine_id Стенда* → раскрыть в правом верхнем углу меню **Реагирование** → выбрать опцию **Подключиться удаленно**.

2. В открывшемся диалоговом окне ввести одноразовый код 2FA.

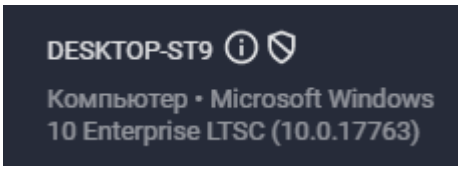
3. Далее по доступности терминала для ввода команды выполнить *ipconfig*, дождаться результата выполнения команды и после этого завершить сессию.

4.1.1.6 Проверка работоспособности функции изоляции конечной станции

1. Перейти в раздел **Моя компания** → **Активы** выполнить поиск по *machine_id* Стенда → раскрыть в правом верхнем углу меню **Реагирование** → выбрать опцию **Изолировать хост**.

2. В открывшемся диалоговом окне ввести имя компьютера, который необходимо изолировать, комментарий о причинах блокировки по необходимости и далее нажать на кнопку **Отправить**.

3. Далее в Web-интерфейсе в таблице активов рядом с записью, которая относится к Стенду, появится индикатор изоляции хоста – значок щита (скриншот ниже):



4. Далее на Стенде выполнить команду *ping 8.8.8.8* (или любой другой IP адрес, к которому компьютер имеет сетевой доступ) непосредственно на Стенде (либо через удаленный терминальный доступ). Результат выполнения команды – *все пакеты потеряны*.

5. Далее провести разблокировку хоста аналогичным блокировке способом и выполнить команду пинг повторно.

4.1.1.7 Проверка работоспособности функций выявления угроз с помощью поведенческого анализа на конечной станции

1. Перейти в раздел **Настройки** → **Модули** → **Группа хостов с Windows EDR** → **Основные настройки** и в блоке **Анализ файлов** проверить, что опции **Блокировать вредоносные файлы** и **Перемещать вредоносные файлы в карантин** выключены.

2. Перейти в раздел **Настройки → Модули → Группа хостов с Windows EDR → Основные настройки** и выключить использование модуля **Политики предотвращения угроз**.

3. Далее непосредственно на Стенде (или с помощью опции удаленного терминального доступа) запустить предоставленный вендором вредоносный экземпляр.

4. Перейти в раздел **Атаки → Алерты**, выставить фильтр **Система интеграции → Huntpoint**, **Классификатор → Huntpoint**, выполнить поиск по имени Стенда и найти алерт о вредоносной активности на хосте.

4.1.2 Запуск ПО применительно к конечным станциям на базе ОС ядра Linux

4.1.2.1 Проверка корректности установки агента на Стенде для проведения тестирования

1. Проверить, что конечная станция, используемая для проведения тестирования, представляет собой виртуальное окружение и удовлетворяет всем системным требованиям.

2. Проверить, что у Стенда отсутствует сетевой доступ к корпоративной сети организации Заказчика.

3. После установки агента Стенд необходимо перезагрузить.

4. Проверить, что на Стенде установлена рекомендуемая вендором версия агента в соответствии с инструкциями по установке. Для этого необходимо выполнить через терминал команду *systemctl status linep* и получить результат выполнения: *loaded: enabled; active: active*;

5. После перезагрузки Стенда перейти в интерфейсе в раздел **Моя компания → Активы**, выставить быстрый фильтр **Компьютер** и убедиться, что актив Стенда в статусе онлайн (индикатор актива зеленый).

4.1.2.2 Проверка корректности настроек модуля EDR

1. Перейти в раздел **Настройки → Модули → Группа хостов с Linux EDR → Основные настройки** и активировать опцию **Удаленного терминального доступа**.

2. Задать пароль контроля доступа (далее этот пароль нигде отображаться не будет, поэтому крайне важно этот пароль сохранить в менеджере паролей).

3. Проверить, что на Стенде отключены все сторонние или встроенные средства защиты конечных устройств (Антивирусы, EDR, DLP и т.д.).

4. Далее перейти в раздел **Профиль пользователя → Безопасность и доступ → Двухфакторная аутентификация** и убедиться в наличии статуса **Аккаунт защищен двухфакторной аутентификацией**.

4.1.2.3 Проверка работоспособности функции сбора криминалистических артефактов

Для корректного проведения данного тестирования, необходимо убедиться, что роль пользователя аналитик или админ.

1. Перейти в раздел **Моя компания → Активы** выполнить поиск по *machine_id* Стенда, раскрыть в правом верхнем углу меню **Реагирование**, выбрать опцию **Собрать артефакты на хосте**.

2. В открывшемся визарде выбрать опцию сбора данных обо всех залогиненных пользователей (logged users).

3. Перейти во вкладку Реагирование в раскрытом сайдбаре с информацией о Стенде, выбрать пункт **Артефакты**. Будет доступно отображение всех запрошенных артефактов со статусом выполнения. По итогу сбора запрошенных на предыдущем шаге данных будет доступна карточка для просмотра и скачивания собранных артефактов.

4.1.2.4 Проверка работоспособности функций удаленного терминального доступа

1. Перейти в раздел **Моя компания → Активы** выполнить поиск по *machine_id* Стенда, раскрыть в правом верхнем углу меню **Реагирование**, выбрать опцию **Подключиться удаленно**.

2. В открывшемся диалоговом окне ввести одноразовый код 2FA.

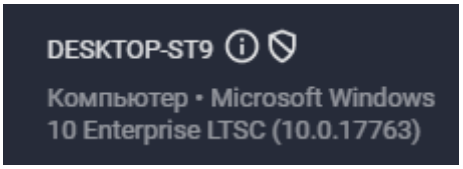
3. Далее по доступности терминала для ввода команды выполнить *whoami*, дождаться результата выполнения команды и после этого завершить сессию.

4.1.2.5 Проверка работоспособности функции изоляции конечной станции

1. Перейти в раздел **Моя компания → Активы** выполнить поиск по *machine_id* Стенда, раскрыть в правом верхнем углу меню **Реагирование**, выбрать опцию **Изолировать хост**.

2. В открывшемся диалоговом окне ввести имя компьютера, который необходимо изолировать, комментарий о причинах блокировки по необходимости и далее нажать на кнопку **Отправить**.

3. Далее в Web-интерфейсе в таблице активов рядом с записью, которая относится к Стенду, появится индикатор изоляции хоста - значок щита (скриншот ниже):



4. Далее на Стенде выполнить команду ***ping 8.8.8.8*** (или любой другой IP адрес, к которому компьютер имеет сетевой доступ) непосредственно на Стенде (либо через удаленный терминальный доступ). Результат выполнения команды – все пакеты потеряны.

5. Далее провести разблокировку хоста аналогичным блокировке способом и выполнить команду пинг повторно.

5 Администрирование Endpoint Detection and Response

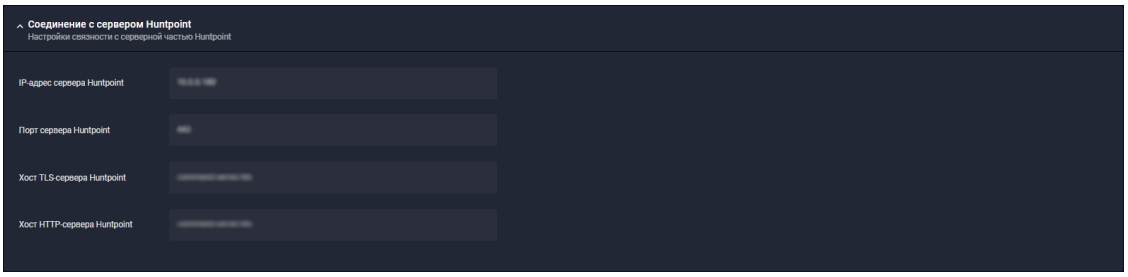
5.1.1 Администрирование конечной точки на базе ОС семейства Microsoft Windows

5.1.1.1 Основные настройки

Для перехода к настройкам перейдите в **Настройки** → **Модули** откройте карточку нужной группы хостов, нажмите **Основные настройки**.

5.1.1.2 Соединение с сервером Windows EDR

В данном разделе описаны настройки связности с серверной частью **Windows EDR**.



5.1.1.2.1 Основная информация

- **IP-адрес сервера Windows EDR** – IP-адрес или DNS имя управляющего **MXDR Console**. В случае использования облачного **MXDR Console** адрес будет установлен по умолчанию.

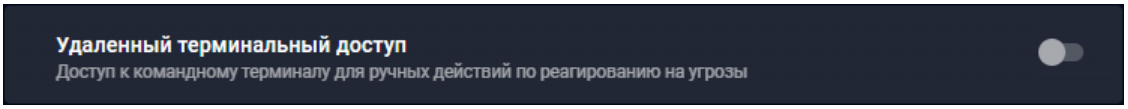
- **Порт сервера Windows EDR** – порт, используемый при обращении по адресу сервера Endpoint Detection and Response (см. пункт выше),

- **Хост TLS-сервера Windows EDR** – имя сервера для Server Name Indication (SNI) при реализации TLS handshake. Данная настройка установлена по умолчанию. Не рекомендуется ее изменение.

- **Хост HTTP-сервера Windows EDR** – имя виртуального хостинга внутри TLS туннеля для отправки событий **Windows EDR**. Данная настройка установлена по умолчанию. Не рекомендуется ее изменение.

5.1.1.3 Удаленный терминальный доступ

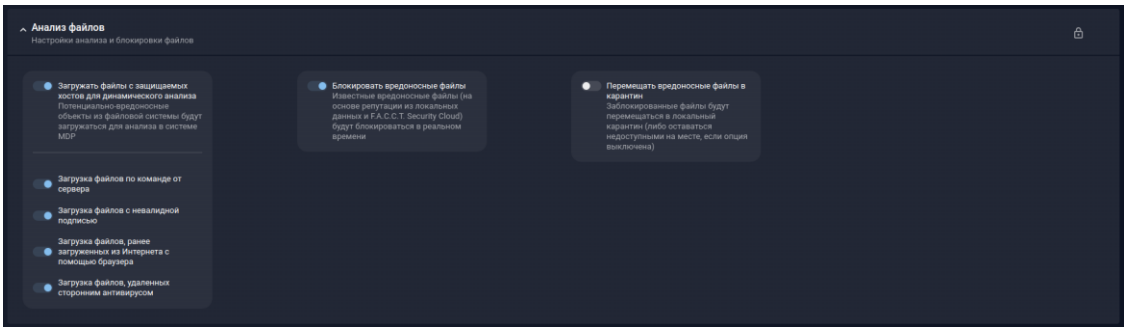
Настройка позволяет активировать удаленный терминальный доступ до конечной станции средствами веб-интерфейса без использования сторонних инструментов вне зависимости от статуса сетевой изоляции.



Интерфейс подключения предоставляется в разделе **Моя компания** → **Активы** в сайдбаре отдельного конечного устройства.

5.1.1.4 Анализ файлов

Блок настроек позволяет задавать политики анализа и блокировки потенциально вредоносных и заведомо вредоносных файлов на конечном устройстве. Пользователь может включить несколько настроек одновременно.



Доступны следующие настройки:

- **Загружать файлы с защищаемых хостов для динамического анализа** – потенциально-вредоносные файлы будут загружаться в подсистему поведенческого анализа файлов **Malware Detonation Platform**. Вы можете настроить загрузку файлов по следующим критериям:
  - ***Загрузка файлов по команде от сервера*** - при обнаружении системой подозрительного процесса, связанный с ним файл будет загружаться на анализ;
  - ***Загрузка файлов с невалидной подписью*** - файл с недействительной, недоверенной либо отсутствующей цифровой подписью отправится на анализ;
  - ***Загрузка файлов, ранее загруженных из Интернета с помощью браузера*** - все файлы, загруженные и загружаемые из браузера автоматически отправляются на анализ;
  - ***Загрузка файлов, удаленных сторонним антивирусом*** - дополнительный анализ файлов, обнаруженных сторонним антивирусом и отмеченных как вредоносные (для обнаружения дополнительных индикаторов).
- **Блокировать вредоносные файлы** – известные вредоносные файлы (на основе репутации из локальных данных и Security Cloud) будут блокироваться в реальном времени. Функция работает независимо от функции детонации ВПО следующим образом:

Windows EDR периодически запрашивает у головного **MXDR Console** список хеш-сумм ранее проанализированных и признанных подсистемой поведенческого анализа вредоносными файлов. Обращение за хеш-суммами производится в локальный головной **MXDR Console** и, если настроены режимы работы выше второго Режимы работы, в облачный **MXDR Console**.

- Перемещать вредоносные файлы в карантин – заблокированные файлы будут перемещаться в локальный карантин (либо оставаться недоступными на месте, если опция выключена).

Файлы, признанные вредоносными и удаленные EDR, можно найти в папке:

C:\Program Files (x86)\...\...\Quarantine

5.1.1.5 События Windows EDR

В данном разделе можно настроить, какие типы событий будут собираться **Windows EDR** для дальнейшей отправки в **MXDR Console**. Типы событий разделены на следующие категории:

- Связанные с процессами события;
- Связанные с файлами события;
- Связанные с системными логами события;
- Связанные с реестром события;
- Связанные с сетью события;
- Связанные с агентом события;
- События User mode hooks.

Категория типов событий **События User mode hooks** является экспериментальной и не рекомендуется к включению в настройках сбора событий.

Чтобы настроить сбор типов событий:

1. Нажмите на строку соответствующей категории.
2. В появившемся сайдбаре выберите необходимые типы событий при помощи переключателя напротив каждого из типов (по умолчанию включены все).

Исключение любых типов событий увеличивает риск не выявления вредоносной активности. Для восстановления настроек по умолчанию нажмите **Настроить по умолчанию**.

3. Нажмите **Сохранить** в правом верхнем углу сайдбара.
4. Нажмите **Сохранить** в правом верхнем углу панели настройки **События EDR**.

5.1.1.6 Политики предотвращения угроз

После активации данного блока будут доступны настройки раздела *Конструктор произвольных политик*.

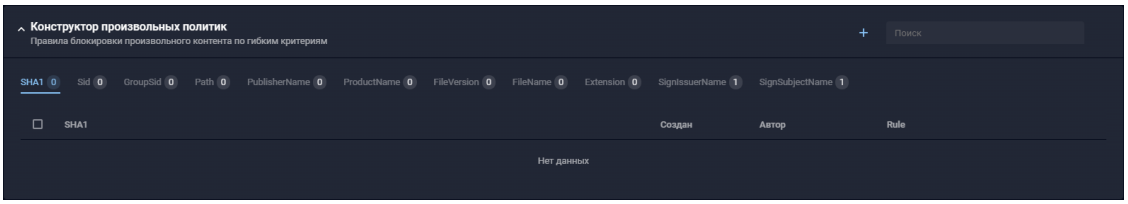
5.1.1.7 Конструктор произвольных политик

Раздел доступен только после активации настройки **Политики предотвращения угроз**.

В данном разделе осуществляется настройка черных и белых списков запуска файлов/кода по частным свойствам и критериям.

Файлы, подписанные нашей компанией и **Microsoft** не блокируются (если это не попытка обхода **Application Control**).

Разрешающие правила имеют приоритет над запрещающими.



Свойства и критерии черных и белых списков:

- **SHA1** – значение хеш-суммы (SHA1) исполняемого файла,
- **Sid** – идентификатор безопасности пользователя,
- **GroupSid** – идентификатор безопасности группы пользователей,
- **Path** – путь к исполняемому файлу,
- **PublisherName** – имя издателя,
- **ProductName** – наименование продукта,
- **FileVersion** – версия файла,

- **FileName** – наименование файла,
- **Extension** – расширение файла.

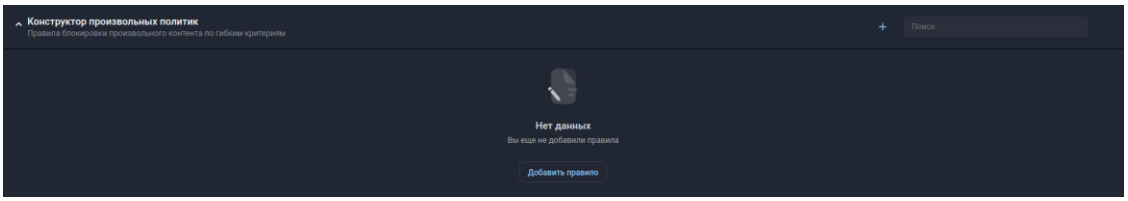
Указание сида пользователя или сида группы позволяет разрешать/блокировать события типа **Создание процесса** от лица указанных юзера или группы юзеров.

Кастомные политики работают со следующими форматами файлов:

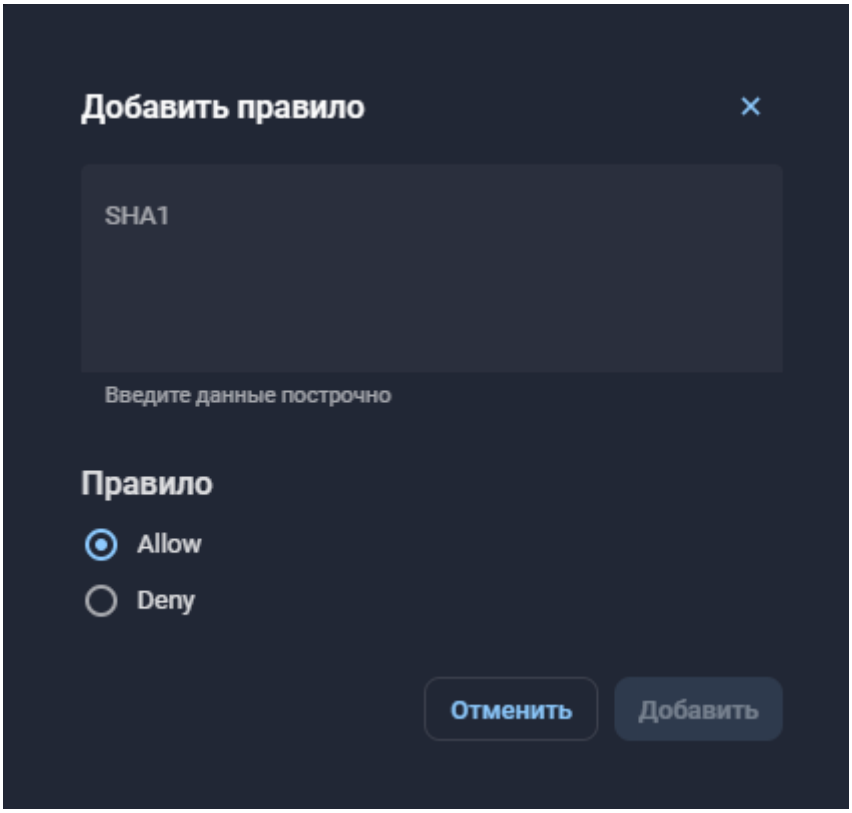
- exe
- msi
- dll
- скрипты

Для добавления нового правила необходимо нажать на значок  , а затем из раскрывающегося списка меню выбрать опцию, по которой будет настраиваться правило.

Нельзя указывать в одном правиле два разных значения, к примеру: *Sid* / *GroupSid* и *Path*.

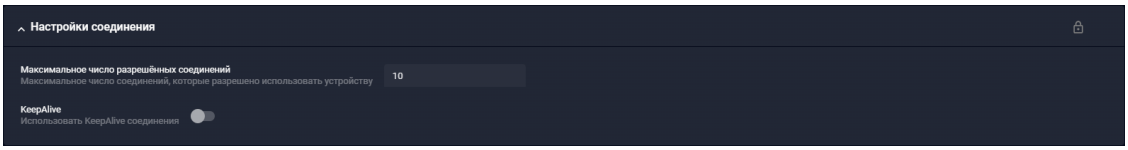


Чтобы добавить правило нажмите кнопку **Добавить**.



5.1.1.8 Настройки соединения

В данном разделе можно указать максимальное число разрешённых соединений для каждого хоста, на котором установлено ПО Endpoint Detection and Response, и настроить использование **KeepAlive-соединений**.



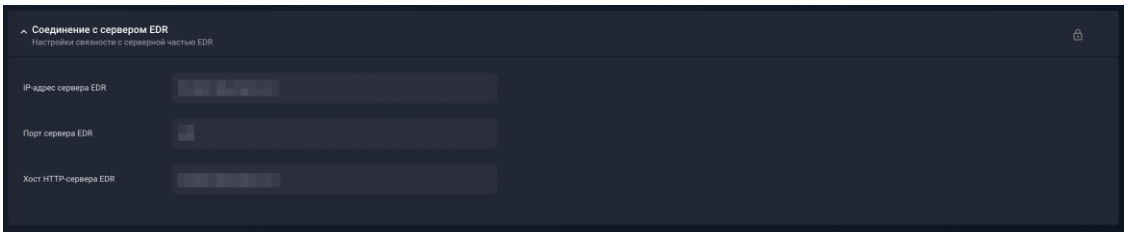
При необходимости укажите максимальное число разрешённых соединений (`10-65000`) в соответствующем поле и включите использование **KeepAlive-соединений** при помощи соответствующего переключателя. Затем нажмите **Сохранить**.

5.1.2 Администрирование конечной точки на базе ядра Linux EDR

5.1.2.1 Основные настройки

Для перехода к настройкам перейдите в **Настройки** → **Модули**, откройте карточку нужной группы хостов, нажмите **Основные настройки.**

5.1.2.2 Соединение с сервером Linux EDR



- **IP-адрес сервера Linux EDR** – IP-адрес или DNS имя управляющего **MXDR Console**. В случае использования облачного **MXDR Console** адрес будет установлен по умолчанию.

- **Порт сервера Linux EDR** – порт, используемый при обращении по адресу сервера Endpoint Detection and Response.

- **Хост HTTP-сервера Linux EDR** – имя виртуального хостинга внутри TLS туннеля для отправки событий Linux EDR. Данная настройка установлена по умолчанию. Не рекомендуется ее изменение.

5.1.2.3 Удаленный терминальный доступ

Настройка позволяет активировать удаленный терминальный доступ до конечной станции средствами веб-интерфейса без использования сторонних инструментов вне зависимости от статуса сетевой изоляции.

Интерфейс подключения предоставляется в разделе `Моя компания` → `Активы` в карточке отдельного актива или сервера.

5.1.2.4 События с хостов

В данном разделе можно настроить, какие типы событий будут собираться **Linux EDR** для дальнейшей отправки в **MXDR Console**. Типы событий разделены на следующие категории:

- **Agent related events —** События Агента
- **Filesystem related events —** События файловой системы
- **Process related events —** События процессов
- **Network related events —** События сети
- **Devise related events —** События устройств

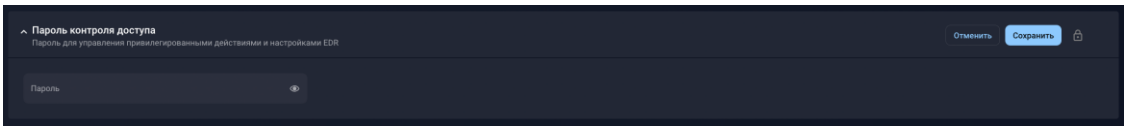
- **System user related events —** Пользовательские системные события
- **System group related events —** Групповые системные события
- **Services related events —** Сервисные системные события

Чтобы настроить сбор типов событий:

1. Нажмите на строку соответствующей категории.
2. В появившемся сайдбаре выберите необходимые типы событий при помощи переключателя напротив каждого из типов (по умолчанию включены все). Исключение любых типов событий увеличивает риск не выявления вредоносной активности. Для восстановления настроек по умолчанию нажмите **Настроить по умолчанию**.
3. Нажмите **Сохранить** в правом верхнем углу сайдбара. Для применения всех настроек потребуется ввести **PKI-ключ**.

5.1.2.5 Пароль контроля доступа

В данной настройке можно установить пароль для доступа к управлению привилегированными действиями и настройками **Linux EDR** в локальном режиме.



Не забудьте нажать кнопку **Сохранить** чтобы пароль стал активным.

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 Endpoint Detection and Response»: 115088, г. Москва, ул. Шарикоподшипниковская, д. 1