MaxPatrol EDR версия 5.0

Руководство администратора

Дата редакции документа: 04.10.2023

Содержание

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по развертыванию, настройке и администрированию MaxPatrol Endpoint Detection and Response (далее также — MaxPatrol EDR).

Руководство адресовано специалистам, выполняющим установку, первоначальную настройку и администрирование MaxPatrol EDR.

Комплект документации MaxPatrol EDR включает в себя следующие документы:

— Этот документ.

— Начало работы — содержит информацию и инструкции для первоначальной настройки MaxPatrol EDR.

— Руководство разработчика — содержит справочную информацию и инструкции для специалистов, разрабатывающих модули агентов в MaxPatrol EDR.

2. О MaxPatrol EDR

MaxPatrol Endpoint Detection and Response — система на базе платформы MaxPatrol 10, предназначенная для защиты конечных устройств от киберугроз. Собирая и анализируя данные из множества систем, MaxPatrol EDR выявляет в IT-инфраструктуре организации сложные целевые атаки и автоматически реагирует на них. MaxPatrol EDR встроен в экосистему продуктов Positive Technologies и позволяет:

— отправлять подозрительные файлы на проверку в PT Sandbox и использовать полученные вердикты одновременно на всех конечных устройствах;

— запускать на конечных устройствах сканирование в режиме аудита и отправлять результаты в MaxPatrol VM;

— использовать для выявления и расследования кибератак данные и экспертизу из других продуктов.

При обнаружении угроз MaxPatrol EDR имеет возможность выполнить следующие автоматические действия:

— удалить файл;

— завершить один или несколько процессов;

— заблокировать сетевой трафик;

— запустить проверку файлов и процессов на основе YARA-правил;

— отправить файл на проверку в PT Sandbox;

— отправить данные о событиях ИБ на syslog-сервер.

Кроме того, администратор или оператор системы может в любой момент времени вручную запустить на конечном устройстве реагирование на угрозу.

3. Архитектура и алгоритм работы MaxPatrol EDR

MaxPatrol EDR состоит из серверной части и агентов, устанавливаемых на конечные устройства. Серверная часть MaxPatrol EDR состоит из двух программных компонентов — управляющего сервера и сервера агентов.

Управляющий сервер — основной компонент системы, который позволяет конфигурировать ее через веб-интерфейс. Сервер агентов — приложение для управления агентами и модулями, а также для взаимодействия с внешними системами (MaxPatrol SIEM, MaxPatrol VM, PT Sandbox, syslog-сервер).

Агент — приложение, которое устанавливается на конечное устройство для обеспечения работы модулей и связи с сервером агентов. Модуль — приложение, которое запускается на конечном устройстве для выполнения основных функций продукта.

Существуют две конфигурации MaxPatrol EDR — односерверная и многосерверная. Многосерверную конфигурацию вы можете использовать для распределения нагрузки при большом количестве конечных устройств в вашей организации. В этой конфигурации на основном сервере устанавливаются все компоненты, а на других только сервер агентов, СУБД PostgreSQL и объектное хранилище MinIO.

Алгоритм работы MaxPatrol EDR:

1. Сервер агентов передает на агенты модули и их конфигурацию (см. раздел 18.1).
2. Модули доставки и установки устанавливают и настраивают приложения на конечном устройстве, например Sysmon.
3. Модули сбора собирают данные о системных событиях, кэшируют их в памяти агента, передают в модули обнаружения и при необходимости на сервер агентов и в MaxPatrol SIEM.
4. Модули обнаружения анализируют файлы, процессы, собранные события, обнаруживают подозрительную активность на конечном устройстве — и регистрируют события ИБ.
5. Модули реагирования пресекают подозрительную и вредоносную активность, выполняя действия в соответствии с политикой или по команде пользователя (см. раздел 20).
6. Модули интеграции обеспечивают интеграцию с внешними системами.
7. Данные о событиях ИБ кэшируются в памяти агента, сервера агентов и пересылаются в базу данных MaxPatrol SIEM.
8. Агент передает метрики и данные трассировки (см. раздел 21.3) на сервер агентов.
9. Управляющий сервер получает обновления продукта и пакетов экспертизы с сервера обновлений.

В этом разделе

3.1. Взаимодействие компонентов в односерверной конфигурации

В этой конфигурации все компоненты MaxPatrol EDR устанавливаются на одном сервере.

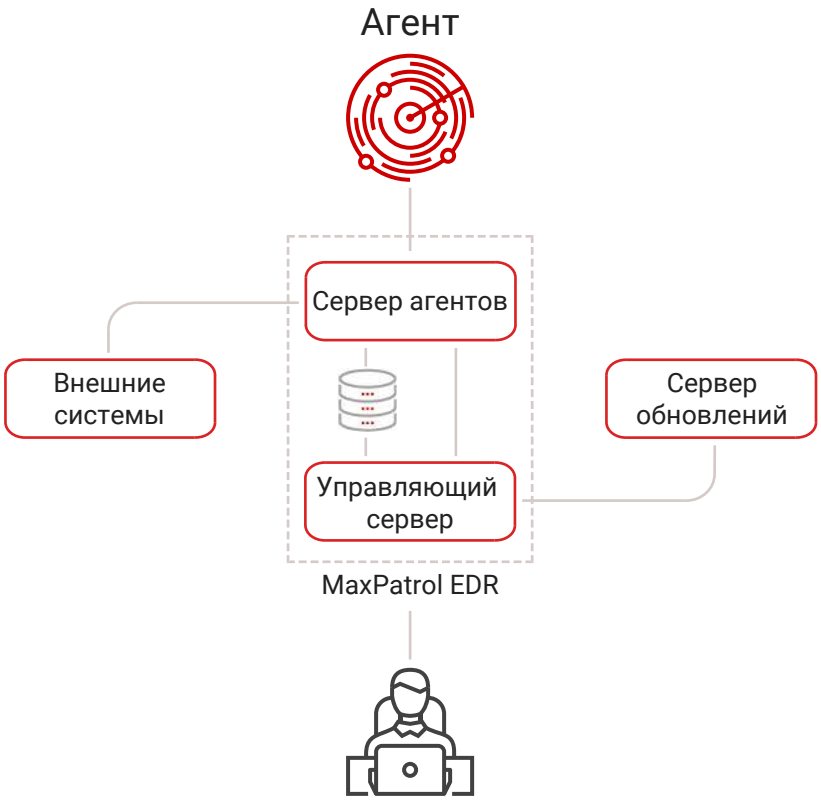

Рисунок 1. Взаимодействие компонентов MaxPatrol EDR

Для обеспечения сетевого взаимодействия компонентов MaxPatrol EDR должны быть доступны перечисленные ниже порты.

Примечание. В таблице приведены порты, используемые по умолчанию.

Таблица 1. Компоненты и порты взаимодействия

Порт	Протокол	Соединение	Описание
Сервер MaxPatrol EDR			
8444	HTTPS	Входящее	Взаимодействие управляющего сервера с внешними источниками
8443	HTTPS	Входящее	Взаимодействие управляющего сервера с сервером агентов и сервера агентов с агентами
443	HTTPS	Исходящее	Взаимодействие с PT Sandbox

Порт	Протокол	Соединение	Описание
5671	AMQP	Исходящее	Взаимодействие с MaxPatrol SIEM
5671	AMQP	Исходящее	Взаимодействие с MaxPatrol VM
3334	HTTPS	Исходящее	Взаимодействие с компонентом MP 10 Core
443	HTTPS	Исходящее	Взаимодействие с сервером лицензирования
443	HTTPS	Исходящее	Взаимодействие с сервером обновлений
9000	S3	Входящее	Доступ к объектному хранилищу MinIO
5431	PostgreSQL	Входящее	Доступ к СУБД PostgreSQL
3000	HTTPS	Входящее	Веб-интерфейс Grafana
8148	gRPC	Входящее	Веб-интерфейс OpenTelemetry
16686	HTTP	Входящее	Веб-интерфейс Jaeger
8428	HTTPS	Входящее	Веб-интерфейс VictoriaMetrics
9443	HTTPS	Входящее	Доступ к сервису интеграции с сервером лицензирования
22	SSH	Входящее	Доступ к серверу по протоколу SSH
Агент			
8443	WSS	Исходящее	Взаимодействие с сервером агентов

3.2. Взаимодействие компонентов в многосерверной конфигурации

В этой конфигурации на основном сервере устанавливаются все компоненты MaxPatrol EDR, а на других только сервер агентов, СУБД PostgreSQL и объектное хранилище MinIO.

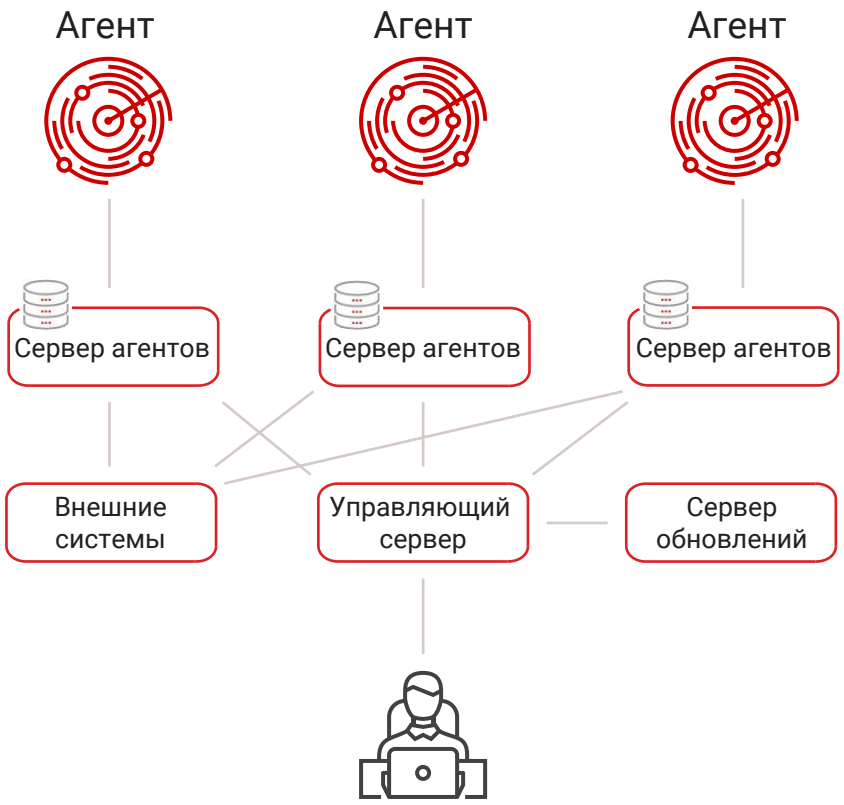

Рисунок 2. Взаимодействие компонентов MaxPatrol EDR

Для обеспечения сетевого взаимодействия компонентов MaxPatrol EDR должны быть доступны перечисленные ниже порты.

Примечание. В таблице приведены порты, используемые по умолчанию.

Таблица 2. Компоненты и порты взаимодействия

Порт	Протокол	Соединение	Описание
Управляющий сервер			
8444	HTTPS	Входящее	Взаимодействие управляющего сервера с внешними источниками
8443	HTTPS	Исходящее	Взаимодействие с серверами агентов
9000	S3	Исходящее	Доступ к объектным хранилищам MinIO на серверах агентов
5431	PostgreSQL	Исходящее	Доступ к СУБД PostgreSQL на серверах агентов
3334	HTTPS	Исходящее	Взаимодействие с компонентом MP 10 Core
443	HTTPS	Исходящее	Взаимодействие с сервером лицензирования

Порт	Протокол	Соединение	Описание
443	HTTPS	Исходящее	Взаимодействие с сервером обновлений
9000	S3	Входящее	Доступ к объектному хранилищу MinIO
5431	PostgreSQL	Входящее	Доступ к СУБД PostgreSQL
3000	HTTPS	Входящее	Веб-интерфейс Grafana
8148	gRPC	Входящее	Веб-интерфейс OpenTelemetry
16686	HTTP	Входящее	Веб-интерфейс Jaeger
8428	HTTPS	Входящее	Веб-интерфейс VictoriaMetrics
9443	HTTPS	Входящее	Доступ к сервису интеграции с сервером лицензирования
22	SSH	Входящее	Доступ к управляющему серверу по протоколу SSH
Сервер агентов			
8443	WSS	Входящее	Взаимодействие с управляющим сервером и агентами
8148	HTTPS	Исходящее	Отправка данных трассировки на управляющий сервер
9000	S3	Входящее	Доступ к объектному хранилищу MinIO для управляющего сервера
5431	PostgreSQL	Входящее	Доступ к СУБД PostgreSQL для управляющего сервера
443	HTTPS	Исходящее	Взаимодействие с PT Sandbox
5671	AMQP	Исходящее	Взаимодействие с MaxPatrol SIEM
5671	AMQP	Исходящее	Взаимодействие с MaxPatrol VM
22	SSH	Входящее	Доступ к серверу агентов по протоколу SSH
Агент			
8443	WSS	Исходящее	Взаимодействие с сервером агентов

4. Лицензирование

Для работы MaxPatrol EDR и его защиты от нелегального использования нужно активировать лицензию.

В MaxPatrol EDR есть два типа лицензий: платная для полноценного использования и пробная, предназначенная для демонстрационных целей. Для каждой лицензии указываются срок ее действия, максимальное количество авторизованных агентов и возможность установки MaxPatrol EDR на виртуальных машинах.

После истечения срока действия пробной лицензии работа с системой будет недоступна. Если истек срок действия платной лицензии, то будут ограничены обновление системы, ее настройка и работа агентов.

Просмотреть параметры лицензий вы можете на странице **Лицензии EDR**.

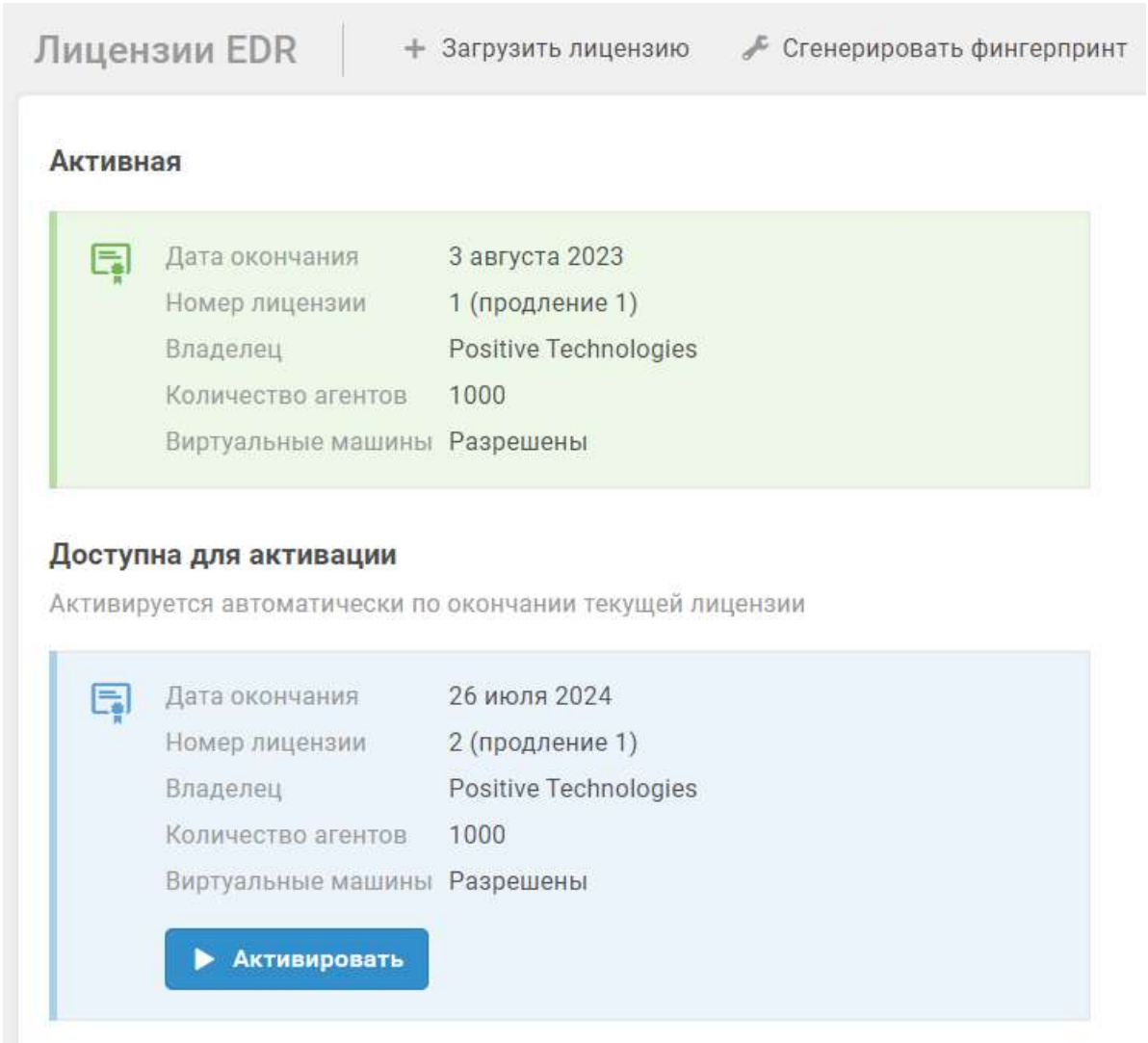

Рисунок 3. Страница **Лицензии EDR**

Процесс лицензирования состоит из следующих шагов:

1. В веб-интерфейсе MaxPatrol EDR вы генерируете фингерпринт.
2. Вы отправляете фингерпринт вашему менеджеру Positive Technologies по электронной почте, он создает файл лицензии и присылает его вам.
3. Вы загружаете файл лицензии через веб-интерфейс MaxPatrol EDR.

   Примечание. Если в системе уже есть активная лицензия, то загруженная лицензия не активируется и помещается в блок **Доступна для активации**. Лицензия активируется автоматически по окончании срока действия текущей лицензии или по нажатию кнопки **Активировать**.

5. Программные и аппаратные требования

В этом разделе приведены требования к программному и аппаратному обеспечению серверов MaxPatrol EDR и конечных устройств.

В этом разделе

5.1. Программные требования

Управляющий сервер MaxPatrol EDR необходимо устанавливать на сервер с компонентом MP 10 Core системы MaxPatrol 10 версии 26.1 или выше. Сервер агентов MaxPatrol EDR рекомендуется устанавливать на чистую 64-разрядную операционную систему. Поддерживаются следующие операционные системы:

- Debian 10, 11;
- Astra Linux Special Edition 1.3, 1.7;
- Astra Linux Common Edition 2.12 («Орел»);
- «РЕД ОС Сервер» 7.1, 7.2, 7.3;
- AlterOS Desktop 7.5;
- «ОСнова» Onyx 2.0;
- «Альт Сервер» 10.1;
- «Альт Рабочая станция» 9, 10.1;
- «Альт Линукс Сервер» 7.0;
- «Альт Линукс Рабочая станция» 7.0.

Для работы управляющего сервера и сервера агентов MaxPatrol EDR в операционной системе должнен быть установлен компонент Docker CE версии 20.10 или выше. Если при установке MaxPatrol EDR в многосерверной конфигурации для подключения к удаленным серверам не используется SSH-ключ (см. раздел 6.2), то на сервере, с которого выполняется установка, должна быть установлена утилита sshpass.

5.2. Требования к аппаратному обеспечению сервера MaxPatrol EDR в односерверной конфигурации

Требования, предъявляемые к аппаратным ресурсам серверов с MaxPatrol EDR, зависят от количества активных агентов.

Таблица 3. Аппаратные требования к серверу MaxPatrol EDR

Активных агентов	Количество событий в секунду	Центральный процессор	ОЗУ	Жесткий диск
До 1000	5000	Суммарно 16 логических ядер	64 ГБ	SSD, 2 ТБ
До 3000	15 000	Суммарно 48 логических ядер	96 ГБ	SSD, 5,5 ТБ
До 5000	25 000	Суммарно 48 логических ядер	128 ГБ	SSD, 10 ТБ
До 10 000	50 000	Суммарно 104 логических ядра	256 ГБ	SSD, 16 ТБ

5.3. Требования к аппаратному обеспечению серверов MaxPatrol EDR в многосерверной конфигурации

Требования, предъявляемые к аппаратным ресурсам серверов с MaxPatrol EDR, зависят от количества активных агентов.

Таблица 4. Аппаратные требования к управляющему серверу MaxPatrol EDR

Активных агентов	Количество событий в секунду	Центральный процессор	ОЗУ	Жесткий диск
До 5000	25 000	Суммарно 16 логических ядер	32 ГБ	SSD, 1 ТБ
До 10 000	50 000	Суммарно 48 логических ядер	64 ГБ	SSD, 2 ТБ
До 50 000	250 000	Суммарно 56 логических ядер	128 ГБ	SSD, 8 ТБ
До 100 000	500 000	Суммарно 104 логических ядра	256 ГБ	SSD, 15 ТБ

Таблица 5. Аппаратные требования к серверу агентов MaxPatrol EDR

Активных агентов	Количество событий в секунду	Центральный процессор	ОЗУ	Жесткий диск
До 1000	5000	Суммарно 8 логических ядер	32 ГБ	SSD, 1,5 ТБ
До 3000	15 000	Суммарно 16 логических ядер	64 ГБ	SSD, 3,5 ТБ
До 5000	25 000	Суммарно 24 логических ядра	112 ГБ	SSD, 6 ТБ
До 10 000	50 000	Суммарно 36 логических ядер	192 ГБ	SSD, 12 ТБ

5.4. Требования к программному и аппаратному обеспечению конечного устройства

Агент поддерживает установку на конечные устройства под управлением следующих операционных систем:

- Windows 7, 8, 8.1, 10;
- Windows Server 2012, 2012R2, 2016, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 2019;
- macOS: 11, 12;
- Debian 10, 11;
- Ubuntu 18.04 LTS, 20.04 LTS;
- CentOS 7, 8;
- Red Hat Enterprise Linux 7, 8;
- Astra Linux Special Edition 1.3, 1.7;
- Astra Linux Common Edition 2.12 («Орел»);
- «РЕД ОС Рабочая станция» 7.2, 7.3;
- AlterOS Desktop 7.5;
- «ОСнова» Onyx 2.0;
- «Альт Сервер» 10.1;
- «Альт Рабочая станция» 9, 10.1;
- «Альт Линукс Сервер» 7.0;
- «Альт Линукс Рабочая станция» 7.0.

Примечание. Для корректной работы модулей в Linux должен быть установлен пакет libpthread.

Агенты необходимо устанавливать на конечные устройства, удовлетворяющие приведенным ниже аппаратным требованиям.

Таблица 6. Аппаратные требования к конечному устройству

Компонент	Минимальные требования	Рекомендуемые требования
Центральный процессор	Тактовая частота 2,2 ГГц, суммарно 2 логических ядра	Тактовая частота 2,2 ГГц, суммарно 2 логических ядра
ОЗУ (доступная память)	150 МБ	200 МБ
Сетевой адаптер	От 100 Кбит/с	От 200 Кбит/с
Жесткий диск, свободное дисковое пространство	HDD или SSD, от 500 МБ	HDD или SSD, от 1000 МБ

6. Развертывание MaxPatrol EDR

В этом разделе приводятся инструкции по установке MaxPatrol EDR.

В этом разделе

6.1. Распаковка архива с дистрибутивом MaxPatrol EDR

Перед установкой или обновлением MaxPatrol EDR вам нужно распаковать архив с дистрибутивом MaxPatrol EDR на сервере с компонентом MP 10 Core.

- Чтобы распаковать архив с дистрибутивом MaxPatrol EDR:

  1. Скопируйте архив с дистрибутивом MaxPatrol EDR в любой каталог.
  2. Перейдите в каталог со скопированным архивом:
     ```
     cd <Имя каталога>
     ```
  3. Создайте каталог, в который будет распакован установочный комплект. Например, `edr-installer`:
     ```
     mkdir edr-installer
     ```
  4. Распакуйте архив в созданный каталог:
     ```
     tar xvf edr-installer.<Версия продукта>.tar.gz -C edr-installer/
     ```
     Например:
     ```
     tar xvf edr-installer.v5.0.0.1111.tar.gz -C edr-installer/
     ```

  Архив с установщиком MaxPatrol EDR распакован.

Теперь вы можете перейти к установке или обновлению MaxPatrol EDR.

6.2. Манифест установки MaxPatrol EDR

Манифест установки — это специальный JSON-файл, которой задает параметры установки MaxPatrol EDR. Манифест состоит из двух блоков параметров. В блоке параметров `hosts` задаются параметры серверов и учетные данные пользователей операционных систем. В блоке параметров `param` — параметры учетных записей для доступа к базам данных и служебные параметры. Вы можете не использовать манифест, если MaxPatrol EDR

устанавливается в односерверной конфигурации и в MaxPatrol 10 один конвейер обработки событий. В этом случае установка будет выполнена с параметрами по умолчанию. Описание параметров приведено в таблице ниже.

Примечание. Изменять значения служебных параметров не рекомендуется.

Таблица 7. Параметры в манифесте установки MaxPatrol EDR

Параметр	Описание
`hosts → <IP-адрес сервера> → components`	Список устанавливаемых компонентов MaxPatrol EDR. Список компонентов управляющего сервера должен содержать `dbms`, `observability` и `ui`, остальных — `agent_server`. Вы также можете установить компонент `agent_server` на управляющем сервере
`hosts → <IP-адрес сервера> → credentials`	Учетные данные пользователя операционной системы. Пользователи удаленных серверов должны иметь права суперпользователя (root) и им должен быть разрешен доступ по протоколу SSH. Учетные данные могут быть заданы в одном из следующих форматов: — `<Логин>:<Пароль>`; — `<Логин>:<Пароль>:<SSH-ключ>`; — `<Логин>::<SSH-ключ>`.
`hosts → <IP-адрес сервера> → service_name`	Название сервера агентов в системе
`hosts → <IP-адрес сервера> → mp_rmq → auto`	Автоматическое или ручное определение компонента MaxPatrol SIEM Server, на котором будут обрабатываться события. Если в MaxPatrol 10 один конвейер обработки событий, необходимо задать значение `true`. Если несколько — `true` и определить параметр `siem_server_name`. Если в MaxPatrol 10 используются пользовательские сертификаты безопасности, то необходимо задать значение `false`, а также определить параметры `siem_server_name`, `ssl_ca`, `ssl_cert` и `ssl_key`. Если при этом сервер RabbitMQ установлен отдельно от компонента MaxPatrol SIEM Server, то вместо параметра `siem_server_name` нужно определить параметры `rmq_host`, `rmq_port` и `rmq_vhost`
`hosts → <IP-адрес сервера> → mp_rmq → siem_server_name`	Компонент MaxPatrol SIEM Server, на котором будут обрабатываться события
`hosts → <IP-адрес сервера> → mp_rmq → ssl_ca`	Путь до файла корневого SSL-сертификата на сервере, на котором планируется установить сервер агентов

Параметр	Описание
hosts → <IP-адрес сервера> → mp_rmq → ssl_cert	Путь до файла публичного SSL-сертификата на сервере, на котором планируется установить сервер агентов
hosts → <IP-адрес сервера> → mp_rmq → ssl_key	Путь до файла закрытого ключа SSL-сертификата, на котором планируется установить сервер агентов
hosts → <IP-адрес сервера> → mp_rmq → rmq_host	IP-адрес или FQDN сервера RabbitMQ
hosts → <IP-адрес сервера> → mp_rmq → rmq_port	Порт сервера RabbitMQ
hosts → <IP-адрес сервера> → mp_rmq → rmq_vhost	Имя виртуального узла RabbitMQ
param → agent_server → POSTGRES_USER	Логин для подключения к базе данных в PostgreSQL на сервере агентов
param → dbms→ POSTGRES_USER	Логин для подключения к базе данных в PostgreSQL на управляющем сервере
param → agent_server → POSTGRES_PASSWORD	Пароль для подключения к базе данных в PostgreSQL на сервере агентов
param → dbms→ POSTGRES_PASSWORD	Пароль для подключения к базе данных в PostgreSQL на управляющем сервере
param → agent_server → MINIO_ACCESS_KEY	Ключ доступа к объектному хранилищу MinIO на сервере агентов
param → dbms → MINIO_ACCESS_KEY param → ui → MINIO_ACCESS_KEY	Ключ доступа к объектному хранилищу MinIO на управляющем сервере. Значения обоих параметров должны совпадать
param → agent_server → MINIO_SECRET_KEY	Секретный ключ доступа к объектному хранилищу MinIO на сервере агентов
param → dbms → MINIO_SECRET_KEY param → ui → MINIO_SECRET_KEY	Секретный ключ доступа к объектному хранилищу MinIO на управляющем сервере. Значения обоих параметров должны совпадать

Примеры конфигураций

Вариант 1. Установка MaxPatrol EDR в односерверной конфигурации, в MaxPatrol 10 несколько конвейеров обработки событий.

```
"hosts":
{
"127.0.0.1": {
"components": ["agent_server", "dbms", "observability", "ui"],
```

```
"credentials": "login:password",
"service_name": "First server",
"mp_rmq": { "auto": true, "siem_server_name": "SiemServer1" }
}
```

Вариант 2. Установка MaxPatrol EDR в многосерверной конфигурации, в MaxPatrol 10 несколько конвейеров обработки событий, события с каждого сервера агентов будут обрабатываться отдельным конвейером.

```
"hosts":
{
"127.0.0.1": {
"components": ["agent_server", "dbms", "observability", "ui"],
"credentials": "login:password",
"service_name": "Management server",
"mp_rmq": { "auto": true, "siem_server_name": "SiemServer1" }
},
"192.0.2.5": {
"components": ["agent_server],
"credentials": "login:password",
"service_name": "Agent server north",
"mp_rmq": { "auto": true, "siem_server_name": "SiemServer2" }
},
"203.0.113.34": {
"components": ["agent_server"],
"credentials": "login:password",
"service_name": "Agent server east",
"mp_rmq": { "auto": true, "siem_server_name": "SiemServer3" }
}
},
```

6.3. Редактирование манифеста установки MaxPatrol EDR

Перед редактированием манифеста вам нужно распаковать архив (см. раздел 6.1) с дистрибутивом MaxPatrol EDR.

- Чтобы отредактировать манифест:

  1. Перейдите в каталог с установочным комплектом:
     `cd /edr-installer/`
  2. Скопируйте файл `manifest_template.json` в файл `manifest.json`:
     `cp manifest_template.json manifest.json`
  3. Откройте файл `manifest.json` для редактирования:
     `nano manifest.json`

4. Задайте параметры установки MaxPatrol EDR в манифесте (см. раздел 6.2).
5. Нажмите клавишу F2 и сохраните изменения в файле.

Манифест сохранен.

6.4. Установка MaxPatrol EDR

Установку необходимо проводить с сервера, на котором установлен компонент MP 10 Core. Перед этим нужно распаковать архив с дистрибутивом (см. раздел 6.1), при необходимости задать параметры установки в манифесте (см. раздел 6.2) и убедиться, что все серверы соответствуют аппаратным и программным требованиям (см. раздел 5).

Внимание! Перед установкой серверов агентов в «РЕД ОС» измените на всех серверах режим работы модуля безопасности SELinux на Permissive с помощью команды `sudo setenforce permissive` — и перезагрузите их.

- Чтобы установить MaxPatrol EDR:

1. Перейдите в каталог с установочным комплектом:
   ```
   cd /edr-installer/
   ```
2. Запустите установочный скрипт с параметром `--use-manifest` (если вы задавали параметры установки в манифесте) или без него (если манифест не используется):
   ```
   sudo ./edr_installer --use-manifest manifest.json
   ```

   Начнется установка MaxPatrol EDR. После завершения установки службы MaxPatrol EDR будут запущены автоматически.

   Примечание. Вы можете настроить установку MaxPatrol EDR, используя другие параметры установочного скрипта (см. раздел 6.5).
3. Удалите установочный комплект и архив с ним:
   ```
   cd <Имя каталога>
   rm -rf edr-installer
   rm edr-installer.<Версия продукта>.tar.gz
   ```
4. Если требуется обновить список псевдонимов команд (см. приложение А), выполните на всех серверах команду, которая указана в сообщениях установщика (например, `source /home/<Логин>/.bashrc`).

MaxPatrol EDR установлен. Вы можете просмотреть журнал с помощью команды `sudo journalctl -u edr`.

6.5. Параметры установочного скрипта

В таблице ниже приведены допустимые параметры установочного скрипта.

Таблица 8. Параметры установочного скрипта

Параметр	Описание	Значение по умолчанию
`--api-server-external-port`	Задает порт управляющего сервера для взаимодействия с внешними источниками	`8444`
`--mgmt-ip`	Задает локальный IP-адрес, по которому будет доступен веб-интерфейс. Если параметр не задан, то веб-интерфейс будет доступен по любому IP-адресу сервера	`0.0.0.0`
`--wan-ip`	Задает локальный IP-адрес сервера агентов. Если параметр не задан, то для подключения агентов вы можете использовать любой IP-адрес сервера	`0.0.0.0`
`--update-server`	Задает IP-адрес или доменное имя сервера обновлений MaxPatrol EDR	`update.ptsecurity.com`
`--download-updates`	Включает автоматическое обновление набора модулей, пакета экспертизы и скачивание новой версии MaxPatrol EDR	Используется
`--only-create-inventory`	Создает инвентарный файл Ansible	Не используется
`--use-manifest`	Задает имя конфигурационного файла, который будет использоваться при распределенной установке компонентов MaxPatrol EDR	Не используется
`--clean`	Запускает удаление службы MaxPatrol EDR	Не используется
`--purge`	Запускает полное удаление MaxPatrol EDR	Не используется

6.6. Установка дополнительного сервера агентов

Вы можете добавить в систему дополнительный сервер агентов для распределения нагрузки. Установку необходимо выполнять с сервера, с которого выполнялась первоначальная установка MaxPatrol EDR. Перед установкой нужно убедиться, что дополнительный сервер соответствует аппаратным и программным требованиям (см. раздел 5.1), и распаковать архив с дистрибутивом (см. раздел 6.1).

Внимание! Перед установкой серверов агентов в «РЕД ОС» измените на всех серверах режим работы модуля безопасности SELinux на Permissive с помощью команды `sudo setenforce permissive` — и перезагрузите их.

► Чтобы установить дополнительный сервер агентов:

1. Перейдите в каталог `opt/edr/`.
   ```
   cd /opt/edr/
   ```
2. Откройте файл `manifest.json` для редактирования:
   ```
   nano manifest.json
   ```
3. В блоке параметров `hosts` добавьте параметры дополнительных серверов агентов и учетные данные пользователей операционных систем (см. раздел 6.2).

   Внимание! Не удаляйте параметры текущих серверов.

   Примечание. Пользователи удаленных серверов должны иметь права суперпользователя (root) и им должен быть разрешен доступ по протоколу SSH.
4. Нажмите клавишу F2 и сохраните изменения в файле.
5. Перейдите в каталог с установочным комплектом:
   ```
   cd /edr-installer/
   ```
6. Запустите установочный скрипт с параметром `--use-manifest`.
   ```
   sudo ./edr_installer --use-manifest /opt/edr/manifest.json
   ```

   Примечание. Вы можете настроить установку MaxPatrol EDR, используя другие параметры установочного скрипта (см. раздел 6.5).

   Начнется установка MaxPatrol EDR. После завершения установки службы MaxPatrol EDR будут запущены автоматически.
7. Удалите установочный комплект и архив с ним:
   ```
   cd <Имя каталога>
   rm -rf edr-installer
   rm edr-installer.<Версия продукта>.tar.gz
   ```
8. Если требуется обновить список псевдонимов команд (см. приложение А), выполните на всех серверах команду, которая указана в сообщениях установщика (например, `source /home/<Логин>/.bashrc`).

Дополнительный сервер агентов установлен. Вы можете просмотреть журнал с помощью команды `sudo journalctl -u edr`.

7. Обновление MaxPatrol EDR с версий 4.0 и 4.1 до версии 5.0

Обновление MaxPatrol EDR до версии 5.0 по основному сценарию (см. раздел 8) невозможно. Для обновления с версий 4.0 и 4.1 до версии 5.0 вам нужно:

1. На управляющем сервере версии 4.0 или 4.1 создать резервную копию конфигурации с помощью утилиты `backup`.
2. Установить MaxPatrol 10 и MaxPatrol EDR версии 5.0 (см. раздел 6).
3. Восстановить созданную резервную копию в MaxPatrol EDR версии 5.0 с помощью утилиты `backup`.

Создание резервной копии

- Чтобы создать резервную копию конфигурации MaxPatrol EDR версии 4.0 или 4.1:

  1. Скопируйте на сервер с установленным управляющим сервером утилиту `backup`.
  2. Перейдите в каталог с утилитой:
     ```
     cd <Имя каталога>
     ```
  3. Запустите создание резервной копии:
     ```
     sudo backup create
     ```
     Начнется создание резервной копии в виде архива формата ZIP. Файл будет сохранен в каталоге `/opt/edr/backups`.

Восстановление резервной копии

Вы можете восстановить резервную копию конфигурации с версий 4.0 и 4.1 как на пустом сервере MaxPatrol EDR версии 5.0, так и на сервере с данными. При восстановлении конфигурации данные MaxPatrol EDR не будут утеряны и дополнятся данными из резервной копии.

- Чтобы восстановить резервную копию конфигурации в MaxPatrol EDR версии 5.0:

  1. На управляющем сервере перейдите в каталог `/opt/edr/`.
     ```
     cd /opt/edr/
     ```
  2. Запустите скрипт для генерации токена доступа к конфигурации управляющего сервера:
     ```
     sudo ./register_client --privileges
     pt.edr.ui.services.api.view,pt.edr.ui.modules.api.view,pt.edr.ui.modules.control.import,pt
     .edr.ui.agents.downloads,pt.edr.ui.groups.api.view,pt.edr.ui.groups.api.create,pt.edr.ui.p
     olicies.api.view,pt.edr.ui.policies.api.create,pt.edr.ui.policies.control.link,pt.edr.ui.p
     olicies.api.edit,pt.edr.ui.agents.api.view,pt.edr.ui.agents.api.edit,pt.edr.ui.agents.api.
     create --client-id backup
     ```

Запустится создание токена. По завершении работы скрипта будет выведен токен, который понадобится вам на шаге 5.

3. Скопируйте на сервер утилиту `backup` и архив с резервной копией конфигурации.
4. Перейдите в каталог с утилитой:

   ```
   cd <Имя каталога>
   ```

5. Запустите восстановление конфигурации:

   ```
   sudo backup restore --backup-file <Путь к архиву с резервной копией> --client-token <Токен доступа>
   ```

Конфигурация восстановлена.

8. Обновление MaxPatrol EDR

Для обновления MaxPatrol EDR потребуется архив с установочным комплектом новой версии продукта. При выходе новой версии MaxPatrol EDR архив автоматически загружается с сервера обновлений Positive Technologies в каталог `/opt/edr/updates/EDR/<Версия продукта>`. Проверка обновлений выполняется каждый день. Если автоматическая проверка и скачивание новой версии MaxPatrol EDR были отключены при установке (см. раздел 6.5), вы можете запустить проверку вручную с помощью команды `edr-update`.

Перед обновлением нужно убедиться, что серверы соответствует аппаратным и программным требованиям (см. раздел 5), и распаковать архив с дистрибутивом (см. раздел 6.1). Обновление MaxPatrol EDR в многосерверной конфигурации рекомендуется проводить с сервера, с которого выполнялась установка.

> **Внимание!** Обновлять MaxPatrol EDR версий 4.0 и 4.1 до версии 5.0 нужно по другому сценарию (см. раздел 7).

► Чтобы обновить MaxPatrol EDR:

1. Перейдите в каталог с установочным комплектом:

   ```
   cd edr-installer/
   ```

   > **Внимание!** Имя каталога с установочным комплектом новой версии MaxPatrol EDR должно совпадать с именем каталога, из которого осуществлялась первоначальная установка продукта.

2. Запустите установочный скрипт и дождитесь завершения обновления:

   ```
   sudo ./edr_installer
   ```

3. Удалите установочный комплект и архив с ним:

   ```
   cd <Имя каталога>
   rm -rf edr-installer
   rm edr-installer.<Версия продукта>.tar.gz
   ```

MaxPatrol EDR обновлен.

9. Обновление набора модулей и пакета экспертизы MaxPatrol EDR

Обновление набора модулей и пакета экспертизы MaxPatrol EDR выполняется автоматически с помощью сервера обновлений Positive Technologies. Проверка обновлений и их установка выполняются каждый час. В набор модулей могут входить новые модули, новые версии уже используемых модулей и измененные конфигурации стандартных политик, в пакет экспертизы — новые правила YARA и правила корреляции.

> **Примечание.** Обновление модулей и экспертизы доступно при наличии действующей лицензии (см. раздел 4).

Если при установке MaxPatrol EDR было отключено автоматическое обновление модулей и экспертизы (см. раздел 6.5), то вы можете запустить проверку и установку обновлений вручную.

- Чтобы обновить модули и экспертизу вручную,

  на сервере с установленным MaxPatrol EDR выполните команду `edr-update`.

Если обновление прошло успешно, в журнале контейнера `vx_edr_modules` последнее сообщение будет `done`. Вы можете проверить его с помощью команды `sudo docker logs -n 1 vx_edr_modules`.

10. Настройка обновления MaxPatrol EDR с локального зеркала

MaxPatrol EDR может работать на сервере в изолированном от интернета сегменте сети. В этом случае для получения обновлений продукта нужно настроить локальное зеркало обновлений. Оно должно располагаться в демилитаризованной зоне (ДМЗ) и загружать обновления с сервера обновлений Positive Technologies.

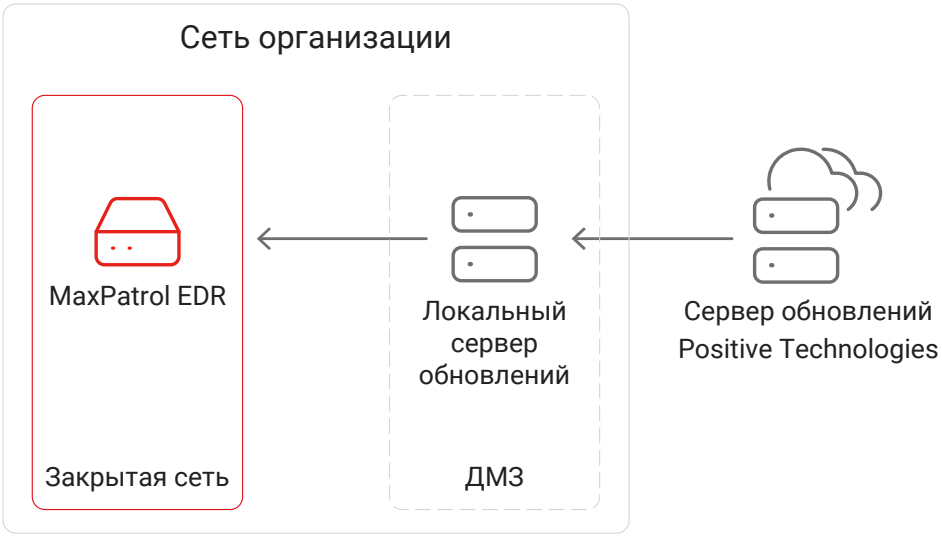

Рисунок 4. Обновление MaxPatrol EDR в закрытом сегменте сети

Для обновления MaxPatrol EDR через локальное зеркало вам нужно:

1. Установить локальный сервер обновлений (см. раздел 10.3).
2. Настроить локальный сервер обновлений (см. раздел 10.4).
3. Активировать лицензию на локальном сервере обновлений (см. раздел 10.5).
4. Настроить подключение продукта к локальному серверу обновлений (см. раздел 10.6).

В этом разделе

Настройка подключения MaxPatrol EDR к локальному серверу обновлений (см. раздел 10.6)

Добавление самоподписанных сертификатов в список доверенных на управляющем сервере MaxPatrol EDR (см. раздел 10.7)

10.1. Аппаратные и программные требования для локального сервера обновлений

Локальный сервер обновлений может быть установлен как на физическом сервере, так и в виртуальной среде.

Аппаратные требования

Для работы локального сервера обновлений потребуются следующие минимальные аппаратные ресурсы:

— 2 ядра процессора;

— 4 ГБ оперативной памяти;

— 200 ГБ свободного места на диске.

Программные требования

Локальный сервер обновлений рекомендуется устанавливать на чистую 64-разрядную серверную версию Ubuntu 18.04, Debian 10 или Debian 11.

10.2. Распаковка архива с установщиком локального сервера обновлений

► Чтобы распаковать архив с установщиком локального сервера обновлений:

1. Скопируйте архив с установщиком локального сервера обновлений в любой каталог на сервере или виртуальной машине, на которые вы планируете устанавливать локальный сервер обновлений.

   Примечание. Архив имеет название `pt-update-mirror-<Версия продукта>.tar.gz`, например `pt-update-mirror-0.1.111.tar.gz`.

2. Перейдите в каталог со скопированным архивом.

   Например:

   ```
   cd /home/user/pt-update-mirror
   ```

3. Распакуйте скопированный архив:

   ```
   tar pxf pt-update-mirror-<Версия продукта>.tar.gz
   ```

Например:

```
tar pxf pt-update-mirror-0.1.111.tar.gz
```

Архив с установщиком локального сервера обновлений распакован.

10.3. Установка локального сервера обновлений

В этом разделе приводится инструкция по установке локального сервера обновлений.

Перед выполнением инструкции нужно:

— Убедиться, что физический сервер или виртуальная машина, на которые вы планируете устанавливать локальный сервер обновлений, удовлетворяет аппаратным и программным требованиям (см. раздел 10.1).

— Распаковать архив с установщиком локального сервера обновлений (см. раздел 10.2).

► Чтобы установить локальный сервер обновлений:

1. Перейдите в каталог с распакованным установщиком локального сервера обновлений:

   ```
   cd /home/user/pt-update-mirror
   ```

2. Запустите установку локального сервера обновлений:

   ```
   sudo dpkg -i pt-update-mirror-<Версия продукта>.deb
   ```

   Например:

   ```
   sudo dpkg -i pt-update-mirror-0.1.111.deb
   ```

   Локальный сервер обновлений установлен и запущен в виде службы подсистемы systemd. Вы можете проверять состояние сервера с помощью команды `systemctl status pt-update-mirror.service` и просматривать его журналы с помощью команды `journalctl -u pt-update-mirror.service`.

10.4. Настройка локального сервера обновлений

Перед настройкой локального сервера обновлений вам нужно получить файлы `cert.crt` и `cert.key` сертификата, выданного центром сертификации вашей организации для локального сервера обновления.

► Чтобы настроить локальный сервер обновлений:

1. Скопируйте файлы `cert.crt` и `cert.key` сертификата локального сервера обновлений в каталог `/etc/pt-update-mirror/https_certs` на этом сервере.

2. Откройте файл `/etc/pt-update-mirror/config.json`:

   ```
   sudo nano /etc/pt-update-mirror/config.json
   ```

3. Замените содержимое блока параметров `products` на следующее:

   ```
   {
           "EDR":
               {
   ```

```
            "synchronizer": "ComponentSynchronyzer",
            "count_number_on_version_parse": 3,
            "store_release_versions": 2
        },
    "EDR.KB":
        {
            "synchronizer": "DockerSynchronizer",
            "count_number_on_version_parse": 3,
            "store_release_versions": 2
        },
    "EDR.*Rules":
        {
            "synchronizer": "ComponentSynchronizer",
            "count_number_on_version_parse": 3,
            "store_release_versions": 3
        }
},
```

4. Если локальный сервер обновлений должен подключаться к интернету через прокси-сервер, в качестве значения параметра `proxy` введите адрес (и при необходимости) порт прокси-сервера.
5. Если прокси-сервер требует аутентификации, укажите логин и пароль для подключения в параметрах `proxy-user` и `proxy-password` соответственно.
6. Сохраните изменения в файле `/etc/pt-update-mirror/config.json`.
7. Перезапустите локальный сервер обновлений:

   ```
   sudo systemctl restart pt-update-mirror.service
   ```

Локальный сервер обновлений настроен.

10.5. Активация лицензии на локальном сервере обновлений

После установки локального сервера обновлений нужно активировать на нем лицензию, приобретенную организацией. Лицензия нужна для аутентификации локального сервера обновлений на публичном сервере обновлений Positive Technologies. Активация выполняется с помощью файла лицензии `license-access-token.key`. Вы можете найти этот файл в архиве, который вам прислали при заказе лицензии.

- Чтобы активировать лицензию на локальном сервере обновлений,

  выполните команду:

  ```
  sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --license-token
  <Полный путь к файлу лицензии>
  ```

Например:

```
sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --license-token /home/user/license-access-token.key
```

Лицензия активирована.

10.6. Настройка подключения MaxPatrol EDR к локальному серверу обновлений

Для получения обновлений в изолированном от интернета сегменте сети вам нужно настроить подключение управляющего сервера MaxPatrol EDR к локальному серверу обновлений.

- Чтобы настроить подключение:

  1. Откройте файл `/opt/edr/update.env`:

     ```
     sudo nano /opt/edr/update.env
     ```

  2. Для параметра `UPDATE_SERVER` задайте значение `<IP-адрес или доменное имя локального сервера обновлений>:8743`.

     Например:

     ```
     UPDATE_SERVER=update.example.com:8743
     ```

  3. Сохраните изменения в файле `/opt/edr/update.env`.

  4. Если для работы локального сервера обновлений вы используете самоподписанные сертификаты, добавьте их в список доверенных на управляющем сервере (см. раздел 10.7).

  Подключение MaxPatrol EDR к локальному серверу обновлений настроено.

10.7. Добавление самоподписанных сертификатов в список доверенных на управляющем сервере MaxPatrol EDR

Если для работы локального сервера обновлений вы используете самоподписанные сертификаты, вам нужно добавить их в список доверенных на управляющем сервере MaxPatrol EDR.

- Чтобы добавить самоподписанные сертификаты в список доверенных:

  1. Скопируйте файлы сертификатов в каталог `/usr/local/share/ca-certificates` на управляющем сервере MaxPatrol EDR.

  2. Создайте каталог `/etc/docker/certs.d/<IP-адрес или доменное имя локального сервера обновлений>:8743`.

3. Скопируйте файлы сертификатов в созданный каталог.
4. Перезапустите компонент Docker:

   `systemctl restart docker`.

Сертификаты добавлены в список доверенных.

11. Удаление MaxPatrol EDR

Удаление MaxPatrol EDR в многосерверной конфигурации рекомендуется проводить с сервера, с которого выполнялась установка.

- Чтобы удалить MaxPatrol EDR:

  1. На сервере с установленным MaxPatrol EDR выполните команду `edr-purge`.
  2. Подтвердите удаление.

  MaxPatrol EDR удален.

См. также

Удаление MaxPatrol EDR завершилось с ошибкой (см. раздел 22.5)

12. Вход в MaxPatrol EDR через PT MC

Сервис управления пользователями и доступом PT MC обеспечивает механизм единого входа (технология single sign-on) в приложения Positive Technologies. Перед входом в MaxPatrol EDR запросите у администратора PT MC логин и пароль вашей учетной записи и убедитесь, что в браузере разрешены всплывающие окна.

► Чтобы войти в MaxPatrol EDR:

1. В адресной строке браузера введите ссылку для входа в интерфейс MaxPatrol EDR.

   Откроется страница входа в PT MC.

2. Выполните одно из следующих действий:

   - Если вы входите под локальной учетной записью, то на вкладке **Локальный** укажите логин локальной учетной записи.
   - Если вы входите под доменной учетной записью, то на вкладке **LDAP** укажите логин доменной учетной записи.

3. В поле **Пароль** введите пароль вашей учетной записи.

   Примечание. Стандартная сессия пользователя в MaxPatrol EDR длится 12 часов. Вы можете продлить сессию, установив флажок **Запомнить меня**: тогда она завершится только через 7 дней бездействия.

4. Нажмите кнопку **Войти**.

PT MC проверяет введенные вами учетные данные. Если вы указали верные данные, откроется стартовая страница с системным дашбордом MaxPatrol EDR. Если вы указали неверные данные, отобразится сообщение об ошибке.

13. О ролях пользователей

В MaxPatrol EDR используется ролевая модель управления доступом. После установки MaxPatrol EDR пользователь может иметь одну из стандартных ролей: администратор, оператор, разработчик. Вы также можете создавать и настраивать свои роли в PT MC.

Таблица 9. Стандартные роли пользователей и доступные функции

Страница продукта	**Администратор**	**Оператор**	**Разработчик**
	Доступные функции		
Агенты EDR	Просмотр списка агентов и их карточек		
	Ручное реагирование на угрозы		
	Операции с агентами		—
Политики EDR	Просмотр списка политик и их карточек		
	Назначение и снятие политики с группы агентов		
	Конфигурирование модулей в политике		
	Изменение параметров политики		
	Создание и копирование политики		—
	Удаление политики		—
Группы агентов EDR	Просмотр списка групп агентов и их карточек		
	Операции с группами агентов		—
Модули	Просмотр списка модулей и их карточек		
	Импорт модуля		
	—		Создание, редактирование, экспорт и удаление модуля
Лицензии EDR	Просмотр загруженных лицензий		
	Генерация фингерпринта	—	
	Загрузка и активация лицензии	—	
Резервное копирование и восстановление	Создание резервной копии, импорт и восстановление конфигурации	—	
Дистрибутивы агентов	Скачивание дистрибутивов	—	

14. Интерфейс MaxPatrol EDR

MaxPatrol EDR встроен в интерфейс системы MaxPatrol 10. После установки MaxPatrol EDR в главном меню появляется раздел **EDR**, меню которого содержит пункты для перехода ко всем страницам продукта.

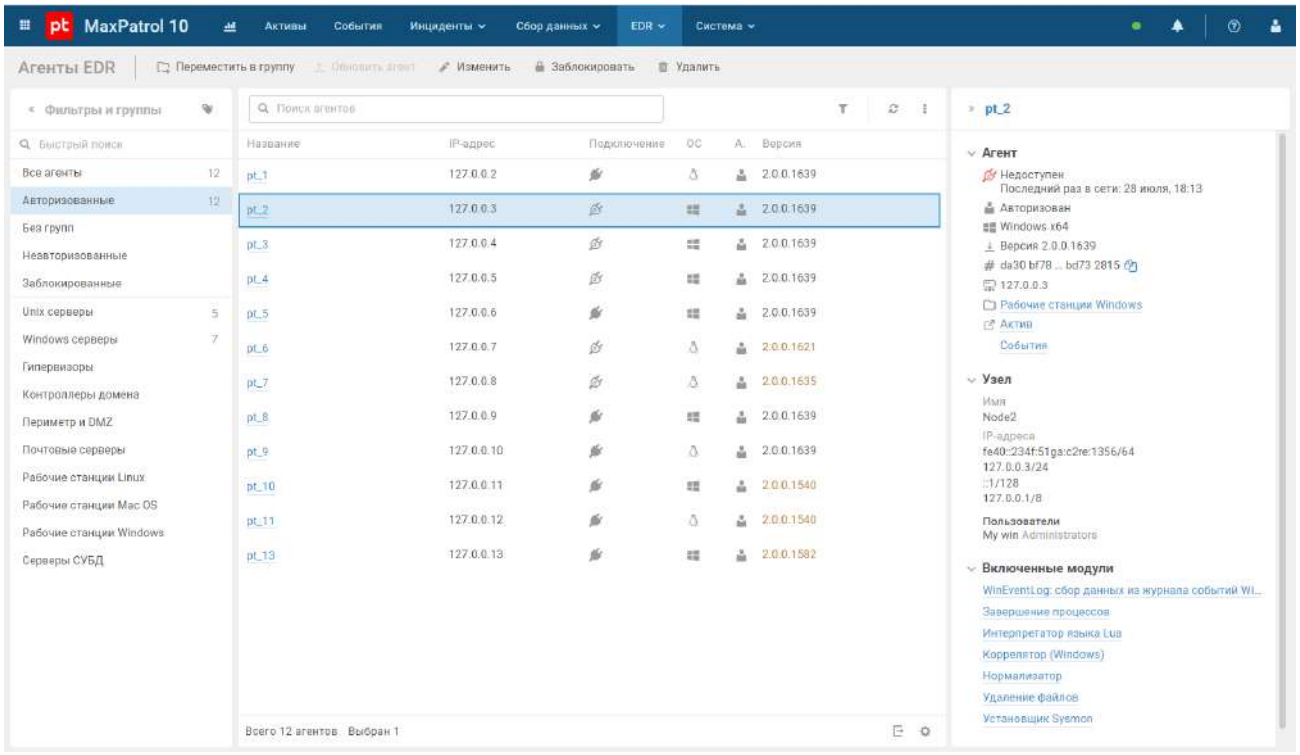

Рисунок 5. Страница **Агенты EDR**

Страницы продукта содержат панель инструментов и рабочую область. Панель инструментов содержит кнопки, с помощью которых вы можете выполнять действия (в том числе групповые) с данными, представленными в рабочей области.

15. Выбор сервера агентов

Если в системе используется несколько серверов агентов, вы можете переключаться между ними в веб-интерфейсе. Для каждого сервера агентов уникален набор агентов, групп и политик. Выбор сервера агентов не сбрасывается при выходе из системы: при следующем входе вы сразу продолжите работу с ним.

- Чтобы выбрать сервер агентов,

  в главном меню в разделе **EDR** в раскрывающемся списке **Сменить сервер агентов** выберите нужный вам сервер.

16. Работа с агентами EDR

Далее приведена основная информация об агентах в MaxPatrol EDR, а также даны инструкции по установке и работе с ними.

В этом разделе

16.1. Об агентах EDR

Агент EDR (далее также — агент) — это приложение, которое необходимо установить на конечном устройстве (см. раздел 16.2) для обнаружения угроз и реагирования на них. После установки вам необходимо авторизовать агент (см. раздел 16.3) и добавить его в группу, на которую назначена хотя бы одна политика (см. раздел 18).

Агент в MaxPatrol EDR может иметь один из двух статусов:

— **Подключен**. У агента есть связь с сервером агентов, все функции продукта выполняются штатно.

— **Отключен**. У агента нет связи с сервером агентов, конечное устройство отключено или служба агента остановлена. В частности, возможен такой вариант, при котором устройство включено, служба выполняется (все модули (см. раздел 19.1) работают локально), но данные на сервер агентов и в сторонние системы не отправляются. Все операции с агентом будут выполнены после восстановления связи. Кроме того, этот статус имеют заблокированные агенты.

Список агентов и информация о них отображаются в веб-интерфейсе продукта на странице **Агенты EDR**. При нажатии на название агента откроется карточка агента. В карточке агента вы можете изменять название агента, добавлять агенту метки для быстрого поиска и просматривать установленные модули, их конфигурацию и зависимости. Из карточки агента вы также можете перейти к соответствующему активу и его событиям.

См. также

Управление политиками EDR (см. раздел 18)

Установка агента на конечное устройство (см. раздел 16.2)

Авторизация агента (см. раздел 16.3)

16.2. Установка агента на конечное устройство

Вы можете установить агент на конечных устройствах под управлением операционных систем Windows, Linux и macOS. Для установки агента вам потребуется перенести на конечное устройство либо пакет установки, либо бинарный файл агента.

Для корректного подключения версия устанавливаемого агента должна поддерживаться на сервере MaxPatrol EDR. Список поддерживаемых сервером версий агентов отображается на странице **Дистрибутивы агентов**.

- Чтобы скачать бинарный файл агента:

  1. Перейдите в веб-интерфейс MaxPatrol EDR.
  2. В главном меню в разделе **EDR** выберите пункт **Управление** → **Дистрибутивы агентов**.

     Откроется страница **Дистрибутивы агентов**.
  3. Нажмите кнопку, соответствующую версии ОС и архитектуре.

  Бинарный файл сохранен на вашем компьютере.

Далее приведены инструкции по установке агента на конечное устройство.

В этом разделе

Установка агента в Windows (см. раздел 16.2.1)

Установка агента в Linux (см. раздел 16.2.2)

Установка агента в macOS (см. раздел 16.2.3)

Установка агента с помощью бинарного файла (см. раздел 16.2.4)

16.2.1. Установка агента в Windows

- Чтобы установить агент в Windows:

  1. Откройте интерфейс командной строки Windows от имени администратора.
  2. Перейдите в папку с установочным пакетом:
     ```
     cd <Имя папки>
     ```
  3. Запустите установку агента:
     ```
     msiexec /quiet /i vxagent-<Номер версии>_<Архитектура>.msi VXSERVER_CONNECT=wss://<Адрес сервера агентов>:<Порт>
     ```
     Примечание. Порт сервера агентов по умолчанию — 8443.

  Агент установлен.

16.2.2. Установка агента в Linux

В зависимости от используемого дистрибутива Linux вы можете установить агент либо из deb-пакета, либо из RPM-пакета. При установке агента в Debian 10, 11 и CentOS 8 рекомендуется использовать дистрибутив с именем `vxagent-<Номер версии>_<Архитектура>`, в остальных ОС — `vxagent-bundle-<Номер версии>_<Архитектура>`.

Примечание. В операционных системах «Альт Сервер», «Альт Рабочая станция», «Альт Линукс Сервер» и «Альт Линукс Рабочая станция» установку агента необходимо выполнять с помощью бинарного файла (см. раздел 16.2.4).

- Чтобы установить агент из deb-пакета:

  1. Перейдите в каталог с deb-пакетом:
     ```
     cd <Имя каталога>
     ```
  2. Запустите установку агента:
     ```
     sudo VXSERVER_CONNECT=wss://<Адрес сервера агентов>:<Порт> dpkg -i ./vxagent-<Номер версии>_<Архитектура>.deb
     ```
     Примечание. Порт сервера агентов по умолчанию — 8443.

  Агент установлен.

- Чтобы установить агент из RPM-пакета:

  1. Перейдите в каталог с RPM-пакетом:
     ```
     cd <Имя каталога>
     ```
  2. Если пакет `initscripts` не установлен, установите его:
     ```
     yum install -y initscripts
     ```
  3. Запустите установку агента:
     ```
     sudo VXSERVER_CONNECT=wss://<Адрес сервера агентов>:<Порт> rpm -i ./vxagent-<Номер версии>.<Архитектура>.rpm
     ```

Примечание. Порт сервера агентов по умолчанию — 8443.

Агент установлен.

16.2.3. Установка агента в macOS

- Чтобы установить агент в macOS:

1. Откройте приложение «Терминал».
2. Перейдите в каталог с установочным пакетом:
   ```
   cd <Имя каталога>
   ```
3. Запустите установку агента:
   ```
   sudo bash -c "launchctl setenv VXSERVER_CONNECT wss://<Адрес сервера агентов>:<Порт> &&
   installer -pkg ./vxagent-<Номер версии>.pkg -target /Library/"
   ```
   Примечание. Порт сервера агентов по умолчанию — 8443.

Агент установлен.

16.2.4. Установка агента с помощью бинарного файла

В этом разделе приводится информация об установке агента с помощью бинарного файла в Windows. Процесс установки в других ОС не отличается. Перед установкой необходимо создать папку, в которую будет установлен агент, и скопировать в нее файл `vxagent.exe`. Имя папки не должно содержать букв русского алфавита.

Внимание! Установку агента в Windows необходимо выполнять от имени администратора, в Linux — от имени суперпользователя (root). В macOS установку может выполнять любой пользователь.

- Чтобы установить агент с помощью бинарного файла:

1. Откройте интерфейс командной строки Windows от имени администратора.
2. Перейдите в папку с файлом `vxagent.exe`.
   ```
   cd <Имя папки>
   ```
3. Запустите файл с аргументами `connect` и `command install`:
   ```
   vxagent -connect wss://<Адрес сервера агентов>:<Порт> -command install
   ```
   Примечание. Порт сервера агентов по умолчанию — 8443.
4. Запустите службу vxagent:
   ```
   vxagent -command start
   ```

Агент установлен.

16.3. Авторизация агента

После установки агента он отображается в MaxPatrol EDR со статусом **Неавторизован**. Для дальнейшей работы с агентом вам нужно авторизовать его. При авторизации агент добавляется в группу (см. раздел 17).

- Чтобы авторизовать агент:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Выберите фильтр **Неавторизованные**.

  3. Выберите агент.

     Примечание. Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.

  4. Нажмите кнопку **Переместить в группу**.

     Откроется всплывающее окно со списком групп.

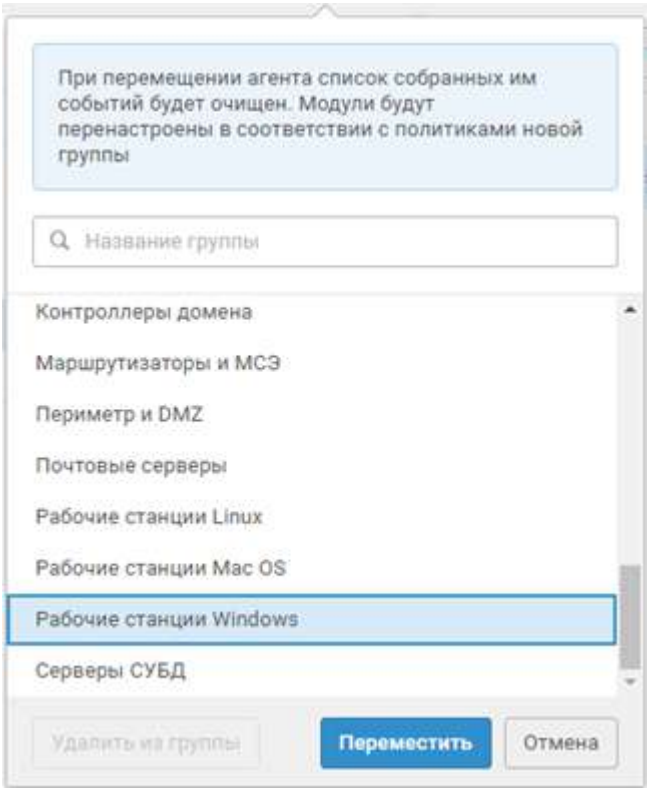

Рисунок 6. Выбор группы

5. Выберите группу, в которую вы хотите добавить агент, или введите название новой группы.
6. Нажмите кнопку **Переместить**.

Агент авторизован.

16.4. Изменение параметров агента

Вы можете изменять название агента в MaxPatrol EDR и добавлять для агента метки, облегчающие поиск.

- Чтобы изменить параметры агента:

1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

   Откроется страница **Агенты EDR**.
2. Выберите агент.
3. Нажмите кнопку **Изменить**.

   Откроется окно **Агент**.
4. Измените параметры агента.
5. Нажмите кнопку **Сохранить**.

Параметры агента изменены.

16.5. Обновление агента

Если для агента доступно обновление, то его версия в таблице будет выделена желтым цветом. Вы можете обновлять только авторизованные агенты.

- Чтобы обновить агент:

1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

   Откроется страница **Агенты EDR**.
2. Выберите агент.

   Примечание. Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.
3. Нажмите кнопку **Обновить агент**.

   Запустится обновление агента. После успешного обновления в таблице будет указана его новая версия.

   Примечание. Если агент отключен, то он будет обновлен после подключения.

16.6. Блокировка агента

Если в систему добавляется неизвестный агент или поведение авторизованного агента стало подозрительным, вы можете заблокировать агент. При блокировке авторизованного агента на нем удаляются все модули. В дальнейшем вы можете авторизовать заблокированные агенты, добавив их в группу (см. раздел 17.7).

- Чтобы заблокировать агент:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Выберите агент.

     Примечание. Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.

  3. Нажмите кнопку **Заблокировать**.

  Агент заблокирован.

См. также

Добавление агента в группу (см. раздел 17.7)

16.7. Удаление агента в MaxPatrol EDR

Вы можете удалить агент из системы, например если он продолжительное время отключен или был добавлен в группу по ошибке. При удалении агента из MaxPatrol EDR он не удаляется с конечного устройства. Если после удаления агент начнет присылать данные, то он автоматически будет добавлен обратно со статусом **Неавторизован**. При удалении агента на нем удаляются все модули.

- Чтобы удалить агент:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Выберите агент.

     Примечание. Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.

  3. Нажмите кнопку **Удалить** и подтвердите удаление.

  Агент удален.

16.8. Удаление агента с конечного устройства

Этот раздел содержит инструкции по удалению агента с конечного устройства.

В этом разделе

16.8.1. Удаление агента в Windows

- Чтобы удалить агент в Windows:

  1. В контекстном меню кнопки **Пуск** выберите пункт **Приложения и возможности**.
  2. В списке установленных программ выберите **Positive Technologies MaxPatrol EDR Agent** и нажмите кнопку **Удалить**.

     Откроется окно мастера удаления агента.
  3. Нажмите кнопку **Удалить**.

  Агент удален.

16.8.2. Удаление агента в Linux

- Чтобы удалить агент, который был установлен из deb-пакета,

  выполните команду `dpkg -r vxagent`.

  Агент удален.

- Чтобы удалить агент, который был установлен из RPM-пакета,

  выполните команду `rpm -e vxagent`.

  Агент удален.

16.8.3. Удаление агента в macOS

- Чтобы удалить агент в macOS,

  выполните команду `sudo /Library/vxagent/uninstall.sh`.

  Агент удален.

16.8.4. Удаление агента, установленного с помощью бинарного файла

В этом разделе приводится информация об удалении агента в Windows, установленного с помощью бинарного файла. Процесс удаления в других ОС не отличается.

- Чтобы удалить агент, который был установлен с помощью бинарного файла:

  1. Откройте интерфейс командной строки Windows от имени администратора.
  2. Перейдите в папку с файлом `vxagent.exe`.
  3. Остановите и удалите службу vxagent:

     ```
     vxagent -command stop
     vxagent -command uninstall
     ```

  4. Удалите папку, в которой находится файл `vxagent.exe`:

     ```
     rd /s /q <Путь к папке>
     ```

  Агент удален.

17. Управление группами агентов EDR

Далее приведена основная информации о группах агентов и даны инструкции по работе с ними.

В этом разделе

17.1. О группах агентов EDR

Группа агентов EDR (далее также — группа агентов) — это один или несколько агентов, объединенных по определенному принципу для назначения им одних и тех же политик. Каждый агент может находиться только в одной группе или быть без группы. По умолчанию в системе создано несколько стандартных групп агентов. Вы можете создавать свои группы и перемещать агенты из одной группы в другую. Если агент находится в группе, то к нему применяются все политики (см. раздел 18), назначенные на группу.

Список всех групп агентов отображается на странице **Группы агентов EDR**.

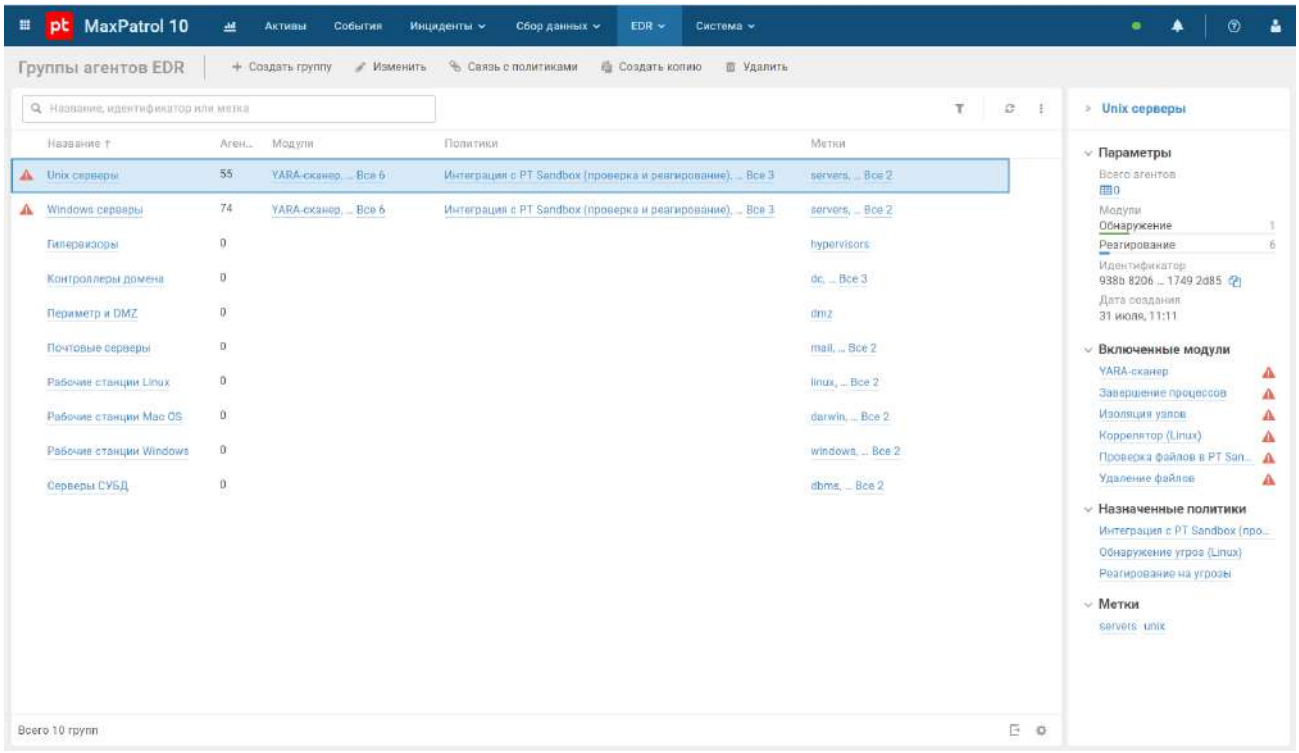

Рисунок 7. Страница **Группы агентов EDR**

При нажатии на название группы откроется карточка группы, в которой вы можете просматривать списки:

— модулей со всех политик, назначенных на группу;

— зависимостей модулей со всех политик, назначенных на группу;

— агентов группы;

— политик, назначенных на группу.

17.2. Создание группы

► Чтобы создать группу:

1. В главном меню в разделе **EDR** выберите пункт **Группы агентов**.

   Откроется страница **Группы агентов EDR**.

2. Нажмите кнопку **Создать группу**.

   Откроется окно **Новая группа агентов**.

3. В поле **Название** введите название группы.

4. В поле **Метки** выберите существующие метки для быстрого поиска группы или задайте свои.

5. В блоке параметров **Отправлять системные события** выберите, куда нужно отправлять системные события со всех агентов группы.
6. В поле **Кэш на агенте** укажите максимальный размер кэша событий на агенте.
7. В поле **Время хранения событий в кэше** укажите максимальное время хранения событий в кэше на агенте.
8. В поле **Макс. скорость передачи событий с агента** укажите максимальную скорость передачи событий с агента на сервер агентов.
9. Нажмите кнопку **Добавить**.

Группа создана.

Вы также можете копировать группы (см. раздел 17.4) или создавать их при перемещении агентов (см. раздел 17.5).

17.3. Настройка хранения и передачи системных событий

Системные события (телеметрия), которые собирают модули «WinEventLog: сбор данных из журнала событий Windows», «Драйвер сбора данных и реагирования» и «Сбор данных из файлов журналов», кэшируются в памяти агента. Вы можете настроить передачу системных событий в кэш сервера агентов и в MaxPatrol SIEM, а также параметры хранения событий в кэше агента.

> **Примечание.** События ИБ всегда отправляются в MaxPatrol SIEM. Если у агента нет соединения с сервером агентов, то события ИБ будут хранится в кэше агента и будут отправлены в MaxPatrol SIEM после восстановления соединения.

► Чтобы настроить хранение и передачу системных событий:

1. В главном меню в разделе **EDR** выберите пункт **Группы агентов**.

   Откроется страница **Группы агентов EDR**.
2. Выберите группу.
3. Нажмите кнопку **Изменить**.

   Откроется окно **Группа агентов**.
4. В блоке параметров **Отправлять системные события** выберите, куда нужно отправлять системные события со всех агентов группы.
5. В поле **Кэш на агенте** укажите максимальный размер кэша событий на агенте.
6. В поле **Время хранения событий в кэше** укажите максимальное время хранения событий в кэше на агенте.
7. В поле **Макс. скорость передачи событий с агента** укажите максимальную скорость передачи событий с агента на сервер агентов.
8. Нажмите кнопку **Сохранить**.

17.4. Копирование группы

Вы можете создавать новые группы агентов на основе имеющихся. Для этого нужно скопировать исходную группу. При этом на новую группу назначаются те же политики, которые были назначены исходной группе. Это полезно в тех случаях, когда нужно незначительно изменить набор политик для новой группы.

- Чтобы скопировать группу:

  1. В главном меню в разделе **EDR** выберите пункт **Группы агентов**.

     Откроется страница **Группы агентов EDR**.

  2. Выберите группу.
  3. Нажмите кнопку **Создать копию**.

     Откроется окно **Копия группы агентов**.

  4. В поле **Название** введите название группы.
  5. В поле **Метки** выберите существующие метки для быстрого поиска группы или задайте свои.
  6. Если требуется, измените параметры хранения и передачи системных событий (см. раздел 17.3).
  7. Нажмите кнопку **Создать**.

  Группа скопирована.

17.5. Перемещение агента из одной группы в другую

Если на агенте требуется изменить набор модулей или их конфигурацию, вы можете переместить агент в другую группу. При этом с него удаляются все модули из политик, назначенных на исходную группу. Затем на агент будут установлены модули из политик, назначенных на группу, в которую его переместили.

- Чтобы переместить агент в другую группу:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Выберите агент.

     Примечание. Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.

  3. Нажмите кнопку **Переместить в группу**.

     Откроется всплывающее окно со списком групп.

4. Выберите группу, в которую вы хотите добавить агент, или введите название новой группы.
5. Нажмите кнопку **Переместить**.

Агент перемещен в другую группу.

17.6. Исключение агента из группы

Если агент был добавлен в группу по ошибке или работа модулей вызвала нарушения в работе конечного устройства (например, чрезмерно высокую загрузку центрального процессора), вы можете исключить агент из группы. При этом на агенте удаляются все модули.

- Чтобы исключить агент из группы:

1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

   Откроется страница **Агенты EDR**.
2. Выберите агент.

   Примечание. Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.
3. Нажмите кнопку **Переместить в группу**.

   Откроется всплывающее окно со списком групп.
4. Нажмите кнопку **Удалить из группы**.

Агент исключен из группы.

17.7. Добавление агента в группу

Если агент был исключен из группы или заблокирован, то основные функции MaxPatrol EDR на нем не выполняются. Для установки и работы модулей нужно добавить агент в группу.

- Чтобы добавить агент в группу:

1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

   Откроется страница **Агенты EDR**.
2. Выберите фильтр **Агенты без группы** или **Заблокированные**.
3. Выберите агент.

   Примечание. Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.
4. Нажмите кнопку **Переместить в группу**.

   Откроется всплывающее окно со списком групп.

5. Выберите группу, в которую вы хотите добавить агент, или введите название новой группы.
6. Нажмите кнопку **Переместить**.

Агент добавлен в группу.

17.8. Изменение названия группы и меток

Вы можете изменять название группы и добавлять для группы метки, облегчающие поиск.

- Чтобы изменить название группы и набор меток:

1. В главном меню в разделе **EDR** выберите пункт **Группы агентов**.

   Откроется страница **Группы агентов EDR**.
2. Выберите группу.
3. Нажмите кнопку **Изменить**.

   Откроется окно **Группа агентов**.
4. Измените название группы и набор меток.
5. Нажмите кнопку **Сохранить**.

Название группы и набор меток изменены.

17.9. Удаление группы

Если группа была создана по ошибке или больше не используется, вы можете удалить ее. При этом с агентов, которые находились в группе, будут удалены все модули.

- Чтобы удалить группу агентов:

1. В главном меню в разделе **EDR** выберите пункт **Группы агентов**.

   Откроется страница **Группы агентов EDR**.
2. Выберите группу.
3. Нажмите кнопку **Удалить** и подтвердите удаление.

Группа удалена.

18. Управление политиками EDR

Далее приведена основная информация о политиках и даны инструкции по работе с ними.

В этом разделе

18.1. О политиках EDR

Политика EDR (далее также — политика) — это механизм управления поставкой модулей агентов в той или иной конфигурации на конечные устройства. Политика состоит из перечня модулей, и после назначения политики на группу агентов эти модули автоматически устанавливаются на всех агентах группы.

> **Примечание.** В некоторых случаях модуль не будет установлен на агенте, например если он не поддерживается в ОС конечного устройства.

Вы можете создавать свои политики с помощью встроенных шаблонов (см. раздел 18.2). Список всех политик отображается на странице **Политики EDR**.

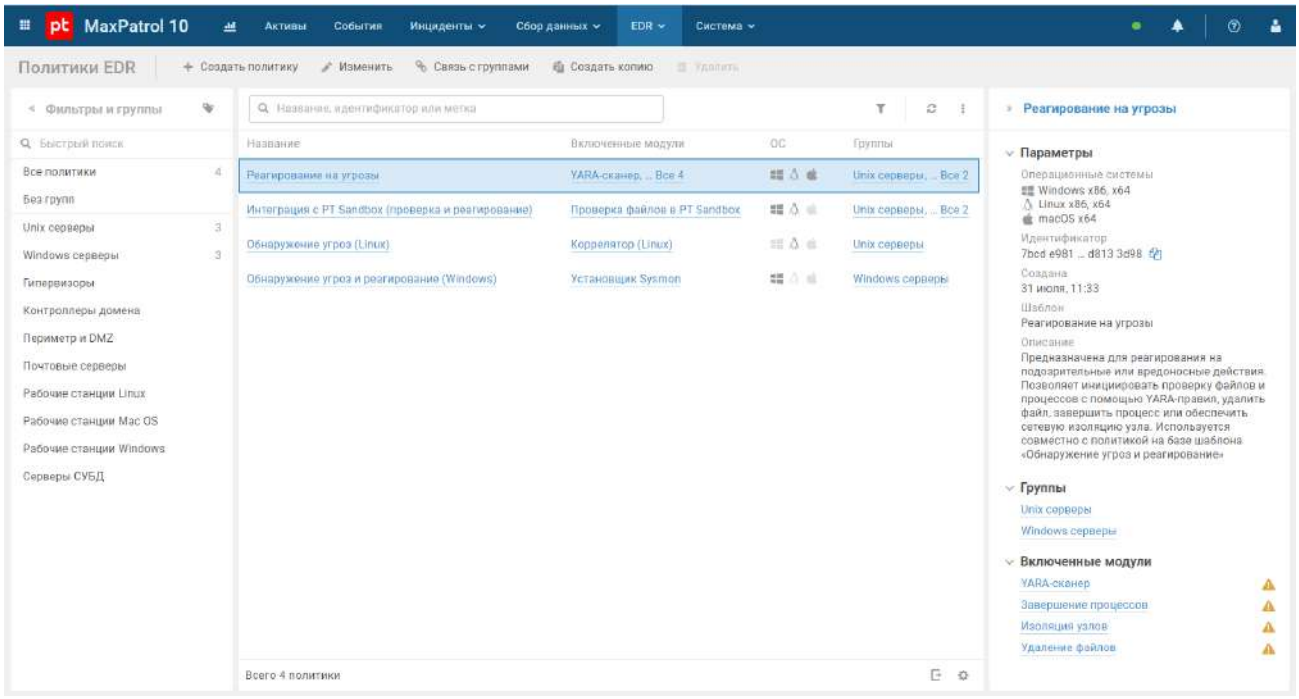

Рисунок 8. Страница **Политики EDR**

При нажатии на название политики откроется карточка политики, в которой вы можете управлять модулями агентов (см. раздел 19), а также просматривать списки:

— зависимостей модулей политики;

— агентов с этой политикой;

— групп, на которые назначена эта политика.

18.2. Шаблоны политик

В системе есть несколько встроенных шаблонов политик, которые сконфигурированы экспертами Positive Technologies. Вы можете создавать политики на базе этих шаблонов и управлять в них конфигурацией модулей (см. раздел 19).

Таблица 10. Шаблоны политик

Название	Описание	Модули
Обнаружение угроз и реагирование (Windows)	Политики на базе этого шаблона предназначены для обнаружения угроз на агентах под управлением Windows и автоматического реагирования на них. Для обнаружения угроз используются данные утилиты Sysmon (основной источник), журнала безопасности, Windows PowerShell и Windows Defender. При обнаружении подозрительных или вредоносных действий такие политики позволяют инициировать проверку	«Коррелятор (Windows)», «WinEventLog: сбор данных из журнала событий Windows»,

Название	Описание	Модули
	файлов и процессов с помощью YARA-правил, удалить файл, завершить процесс или обеспечить сетевую изоляцию узла. Эти политики используются совместно с политиками, в которые входят модули реагирования, например с политикой на базе шаблона «Реагирование на угрозы»	«Установщик Sysmon», «Нормализатор»
Обнаружение угроз (Windows)	Политики на базе этого шаблона предназначены для обнаружения угроз на агентах под управлением Windows. Для этого используются данные утилиты Sysmon (основной источник), журнала безопасности, Windows PowerShell и Windows Defender. Такие политики при совместном использовании с другими специальными политиками позволяют отправлять все события на syslog-сервер, а также проверять подозрительные файлы с помощью YARA-правил или в PT Sandbox	«Коррелятор (Windows)», «WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор»
Обнаружение угроз (Linux)	Политики на базе этого шаблона предназначены для обнаружения угроз на агентах под управлением Linux. Такие политики позволяют выявить нетипичные случаи аутентификации в системе и атаки методом подбора пароля. При совместном использовании этих политик с другой специальной политикой все события ИБ отправляются на syslog-сервер	«Коррелятор (Linux)», «Сбор данных из файлов журналов»
Интеграция с syslog-сервером	Политики на базе этого шаблона предназначены для отправки событий ИБ на syslog-сервер. Такие политики используются совместно с другими политиками	«Отправка событий на syslog-сервер»
Интеграция с PT Sandbox (проверка и реагирование)	Политики на базе этого шаблона предназначены для отправки подозрительных файлов на проверку в PT Sandbox и автоматического реагирования в зависимости от полученного вердикта. Такие политики используются совместно с политиками на базе шаблонов «Обнаружение угроз» и «Реагирование на угрозы»	«Проверка файлов в PT Sandbox»
Интеграция с PT Sandbox (только проверка)	Политики на базе этого шаблона предназначены для отправки подозрительных файлов на проверку в PT Sandbox. Используются совместно с политикой на базе шаблона «Обнаружение угроз»	«Проверка файлов в PT Sandbox»
Реагирование на угрозы	Политики на базе этого шаблона предназначены для реагирования на подозрительные или вредоносные действия. Такие политики позволяют инициировать проверку файлов и процессов с помощью YARA-правил, удалить файл, завершить процесс или обеспечить	«YARA-сканер», «Удаление файлов», «За-

Название	Описание	Модули
	сетевую изоляцию узла. Используются совместно с политикой на базе шаблона «Обнаружение угроз и реагирование»	вершение процессов», «Изоляция узлов»

18.3. Создание политики

Вы можете создавать политики на базе шаблонов (см. раздел 18.2) или пустые. В политиках, которые созданы на базе шаблонов, добавлены модули (см. раздел 19.1) для решения определенных задач и настроены автоматические действия. Политики на базе шаблонов для обнаружения угроз или реагирования можно сразу использовать на агентах. В политиках с модулями интеграции вам предварительно нужно настроить подключение к внешним системам. После создания пустой политики вам нужно добавить в нее модули (см. раздел 19.3), сконфигурировать их (см. раздел 19.4) и настроить автоматические действия (см. раздел 19.5).

- Чтобы создать политику:

  1. В главном меню в разделе **EDR** выберите пункт **Политики**.

     Откроется страница **Политики EDR**.

  2. Нажмите кнопку **Создать политику**.

     Откроется окно **Новая политика**.

  3. В раскрывающемся списке **Шаблон** выберите шаблон (см. раздел 18.2), на базе которого вы хотите создать политику.

     Примечание. Для создания пустой политики вы можете выбрать значение **Не выбран**.

  4. В поле **Название** введите название политики.

  5. В поле **Метки** выберите существующие метки для быстрого поиска политики или задайте свои.

  6. Нажмите кнопку **Создать**.

  Политика создана.

Вы также можете создавать копии существующих политик (см. раздел 18.4).

18.4. Копирование политики

Вы можете создавать новые политики на основе имеющихся. Это полезно в тех случаях, когда нужно незначительно изменить конфигурацию модулей в политике.

- Чтобы скопировать политику:

  1. В главном меню в разделе **EDR** выберите пункт **Политики**.

Откроется страница **Политики EDR**.

2. Выберите политику.
3. Нажмите кнопку **Создать копию**.

   Откроется окно **Копия политики**.

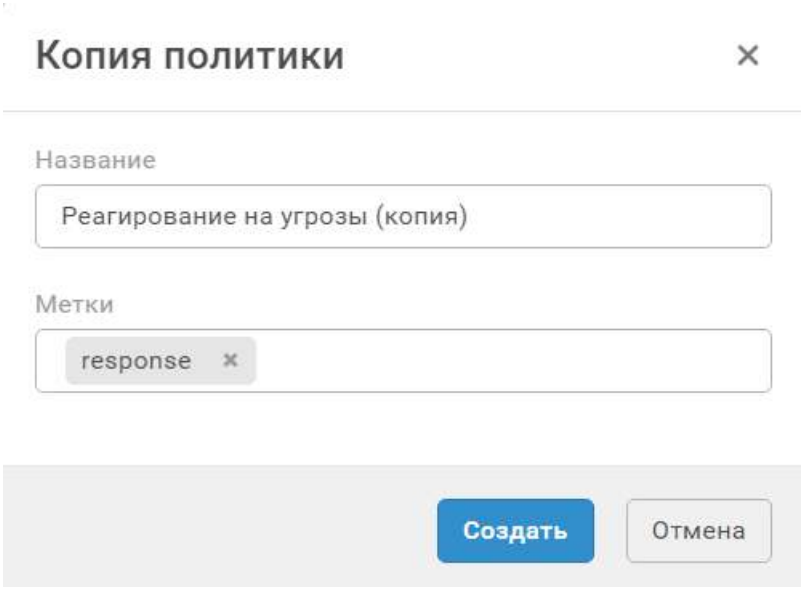

Рисунок 9. Копирование политики

4. В поле **Название** введите название политики.
5. В поле **Метки** выберите существующие метки для быстрого поиска политики или задайте свои.
6. Нажмите кнопку **Создать**.

Политика скопирована.

18.5. Назначение политики на группу агентов

Для установки модулей на агенты необходимо назначить политику на группу агентов. Одну политику можно назначить на множество групп. Вы не можете назначить политику на группу, если в этой политике есть модуль, который уже работает на агентах этой группы (входит в другую политику). В таких случаях вам нужно отключить модуль (см. раздел 19.6) в политике или снять политику (см. раздел 18.7) с группы.

- Чтобы назначить политику на группу:

  1. В главном меню в разделе **EDR** выберите пункт **Политики**.

     Откроется страница **Политики EDR**.

  2. Выберите политику.

3. Нажмите кнопку **Связь с группами**.

   Откроется всплывающее окно **Связи с группами агентов**.

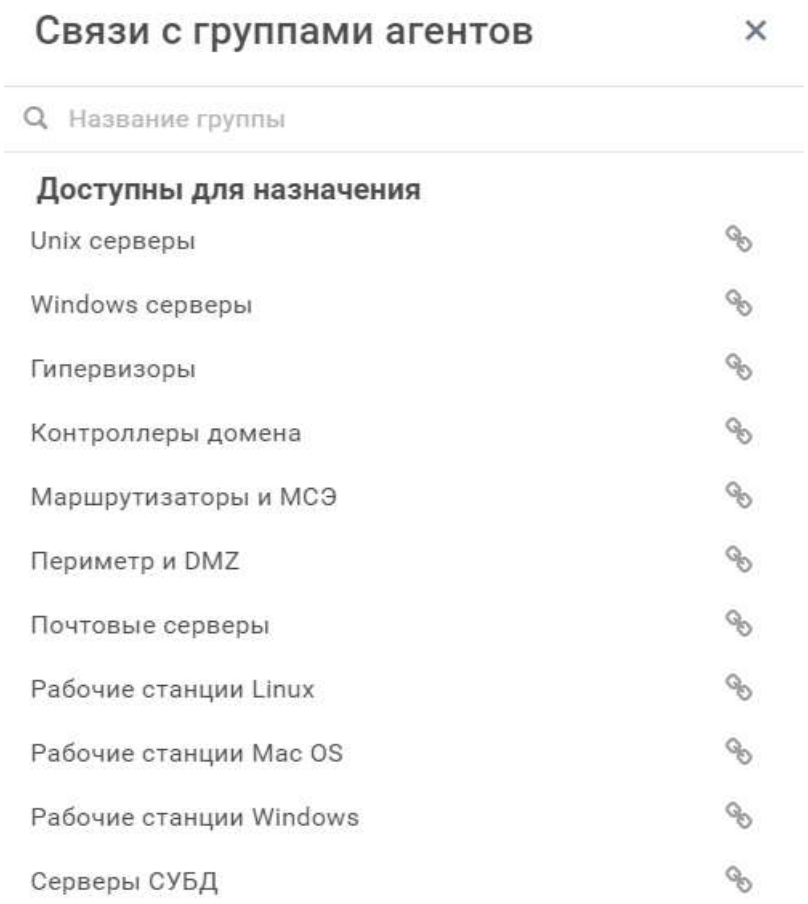

Рисунок 10. Назначение политики на группу агентов

4. Напротив группы, на которую вы хотите назначить политику, нажмите .

Политика назначена на группу.

18.6. Изменение параметров политики

Вы можете изменять название политики и добавлять для политики метки, облегчающие поиск.

- Чтобы изменить параметры политики:

  1. В главном меню в разделе **EDR** выберите пункт **Политики**.

     Откроется страница **Политики EDR**.

  2. Выберите политику.

  3. Нажмите кнопку **Изменить**.

Откроется окно **Политика**.

4. Измените параметры политики.
5. Нажмите кнопку **Сохранить**.

Параметры политики изменены.

18.7. Снятие политики с группы агентов

Вы можете снять политику с группы агентов, например чтобы отладить работу модулей. При снятии политики с группы на агентах удаляются все модули, которые в нее входили.

- Чтобы снять политику с группы агентов:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.
2. Выберите политику.
3. Нажмите кнопку **Связь с группами**.

   Откроется всплывающее окно **Связи с группами агентов**.
4. Напротив группы, с которой вы хотите снять политику, нажмите  .

Политика снята с группы.

18.8. Удаление политики

Вы можете удалить политику, например если она была добавлена по ошибке или больше не используется. Вы не можете удалить политику, назначенную на группу агентов.

- Чтобы удалить политику:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.
2. Выберите политику.
3. Нажмите кнопку **Удалить** и подтвердите удаление.

Политика удалена.

19. Управление модулями агента в политике

Далее приведена основная информация о модулях агента, а также даны инструкции по работе с ними.

В этом разделе

19.1. О модулях агента

Модуль агента — это приложение, которое запускается на агенте для выполнения основных функций продукта. Перечень модулей и описание их конфигураций содержится в политике. Вы можете добавлять и удалять модули из политики, а также отключать и включать их. Для корректной работы модулей на агенте вам нужно обеспечить их зависимости (см. раздел 19.2).

В MaxPatrol EDR есть пять типов модулей:

- **Модули доставки и установки.** Устанавливают и настраивают приложения и управляют конфигурацией ОС на конечном устройстве.
- **Модули сбора.** Собирают данные о событиях на конечном устройстве и передают их в модули обнаружения и в SIEM-системы.
- **Модули обнаружения.** Анализируют собранные события, обнаруживают подозрительную и вредоносную активность на конечном устройстве — и регистрируют события ИБ.
- **Модули реагирования.** Пресекают подозрительную и вредоносную активность на конечном устройстве, выполняя действия в соответствии с конфигурацией модулей обнаружения.
- **Модули интеграции.** Обеспечивают интеграцию с внешними системами.

Некоторые модули по своим функциям могут относиться к нескольким типам.

Таблица 11. Модули MaxPatrol EDR

Название	Описание
Модули доставки и установки	
Установщик Sysmon	Устанавливает и конфигурирует утилиту Sysmon. Удаление модуля с агента не повлияет на конфигурацию Sysmon на конечном устройстве
Модули сбора	
Драйвер сбора данных и реагирования	На уровне ядра ОС собирает данные о системных событиях, удаляет файлы и завершает процессы
WinEventLog: сбор данных из журнала событий Windows	Передает данные из журнала событий Windows в модули обнаружения и сторонние системы
Сбор данных из файлов журналов	Передает данные из заданных журналов в модули обнаружения и сторонние системы
Нормализатор	Выполняет нормализацию необработанных событий от модулей «WinEventLog: сбор данных из журнала событий Windows», «Драйвер сбора данных и реагирования» и «Сбор данных из файлов журналов» для последующей обработки и анализа в других модулях и в MaxPatrol SIEM
Модули обнаружения	
Коррелятор	Выполняет нормализацию, агрегацию и корреляцию потока необработанных событий от источников. При обнаружении вредоносных или подозрительных действий регистрирует события ИБ (корреляционные события). В системе есть два отдельных коррелятора для Windows и Linux
YARA-сканер	Выполняет сигнатурный анализ на основе YARA-правил. При обнаружении вредоносных или подозрительных файлов и процессов выносит вердикты и регистрирует события ИБ
Модули реагирования	
Удаление файлов	Удаляет файлы
Завершение процессов	Завершает процессы
Изоляция узлов	Блокирует сетевой трафик на узлах. Изолировать узел можно двумя способами — полностью, отключив все сетевые адаптеры, или частично, сохранив для него связь с сервером агентов и адресами из списка исключений
Блокировка по IP-адресу	Блокирует все сетевые соединения по IP-адресу. Адрес может быть заблокирован на уровне политики, агента или на обоих уровнях

Название	Описание
Перенаправление DNS-запросов (sinkholing)	Перенаправляет трафик с подозрительных и вредоносных доменов на заданный IP-адрес с помощью файла `hosts`
Интерпретатор языка Lua	Предоставляет возможность для выполнения произвольного кода на языке Lua на агенте
Модули интеграции	
Проверка файлов в PT Sandbox	Отправляет файлы на проверку в PT Sandbox и сохраняет результат проверки в локальные БД всех агентов с данной политикой. Перед отправкой файла на проверку проверяется наличие актуального результата проверки в локальной БД. Если актуальный результат есть, то файл в PT Sandbox не отправляется. Результат проверки считается актуальным в течение семи дней
Сканирование в режиме аудита (MaxPatrol VM)	Сканирует узлы в режиме аудита и отправляет результаты в MaxPatrol VM
Отправка событий на syslog-сервер	Отправляет записи о событиях ИБ на syslog-сервер
Отправка файлов	Отправляет файлы во внешние системы

19.2. Зависимости модулей

Модули могут иметь зависимости. Наличие зависимости у модуля означает, что для его корректной работы на агенте требуется выполнение определенного условия. Если такое условие выполняется, то зависимость считается обеспеченной. Вам нужно обеспечить зависимости всех модулей на агенте.

Зависимости бывают двух видов: от версии агента и от другого модуля. Зависимость от модуля может возникать в двух случаях: когда для работы модуля требуются данные от другого модуля и когда на события модуля назначено действие, которое выполняет другой модуль.

> **Примечание.** Некоторые модули могут иметь по несколько зависимостей от данных других модулей. Для работы каждого такого модуля вам достаточно обеспечить только одну из них, но часть функций MaxPatrol EDR будет при этом недоступна.

Отслеживать зависимости модулей агента вы можете в карточке агента или группы агентов. Если зависимость не обеспечена, то она будет отмечена значком ⚠.

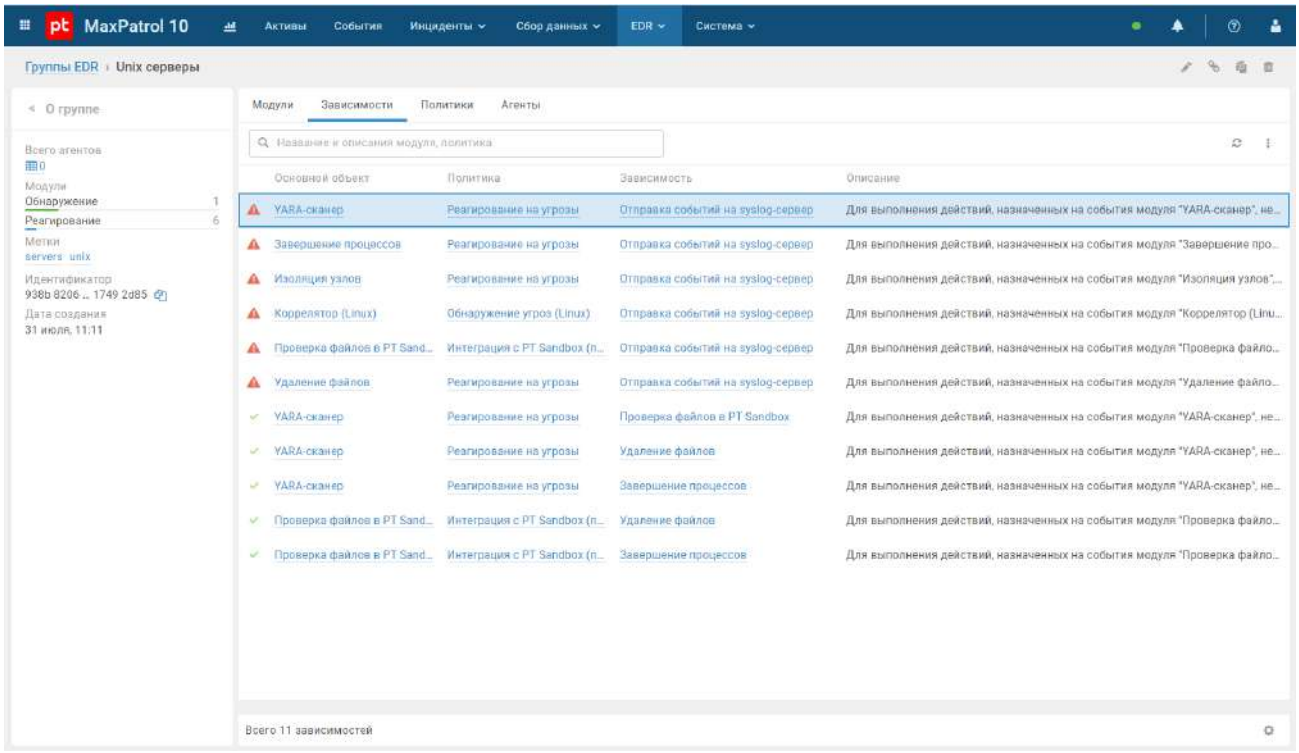

Рисунок 11. Зависимости модулей агента

Вы можете обеспечить зависимость от другого модуля двумя способами:

— добавив необходимый модуль (см. раздел 19.3) в политику, которая назначена на группу;

— назначив на группу (см. раздел 18.5) политику, в которой есть необходимый модуль.

Для обеспечения зависимости от версии агента вам нужно обновить агент (см. раздел 16.5).

19.3. Добавление модуля в политику

► Чтобы добавить модуль в политику:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

3. В списке **Доступны для добавления** выберите модуль.

4. Нажмите кнопку **Добавить**.

   Модуль добавлен в политику. Если политика назначена на группу (см. раздел 18.5), то сразу после добавления модуля он будет автоматически установлен на всех агентах группы.

19.4. Настройка модулей в политике

В разделе приведены инструкции по настройке некоторых модулей в политике. При настройке других модулей вы можете использовать описание их параметров (см. приложение Б).

> **Примечание.** В конфигурации модуля значком отмечены защищенные параметры: их значения передаются на агенты в зашифрованном виде. Просматривать и изменять защищенные параметры могут только пользователи с соответствующими правами.

В этом разделе

19.4.1. Настройка модуля «WinEventLog: сбор данных из журнала событий Windows»

- Чтобы настроить модуль «WinEventLog: сбор данных из журнала событий Windows»:

  1. В главном меню в разделе **EDR** выберите пункт **Политики**.

     Откроется страница **Политики EDR**.

  2. Нажмите на название политики.

     Откроется карточка политики.

  3. В списке **Включенные** выберите модуль «WinEventLog: сбор данных из журнала событий Windows».

     Отобразится список параметров модуля.

  4. Если требуется, в блоке параметров **Каналы журналов** добавьте каналы журнала событий Windows, которые будут обрабатываться модулем.

     Например, `Microsoft-Windows-Sysmon/Operational`.

  5. Нажмите кнопку **Сохранить**.

  Модуль настроен.

19.4.2. Настройка модуля «Проверка файлов в PT Sandbox»

Для проверки файлов с конечных устройств в PT Sandbox должны быть доступны образы win10-1803-x64 (для файлов из Windows) и redos-murom-x64 (для файлов из Linux).

► Чтобы настроить модуль «Проверка файлов в PT Sandbox»:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

3. В списке **Включенные** выберите модуль «Проверка файлов в PT Sandbox».

   Отобразится список параметров, событий и действия модуля.

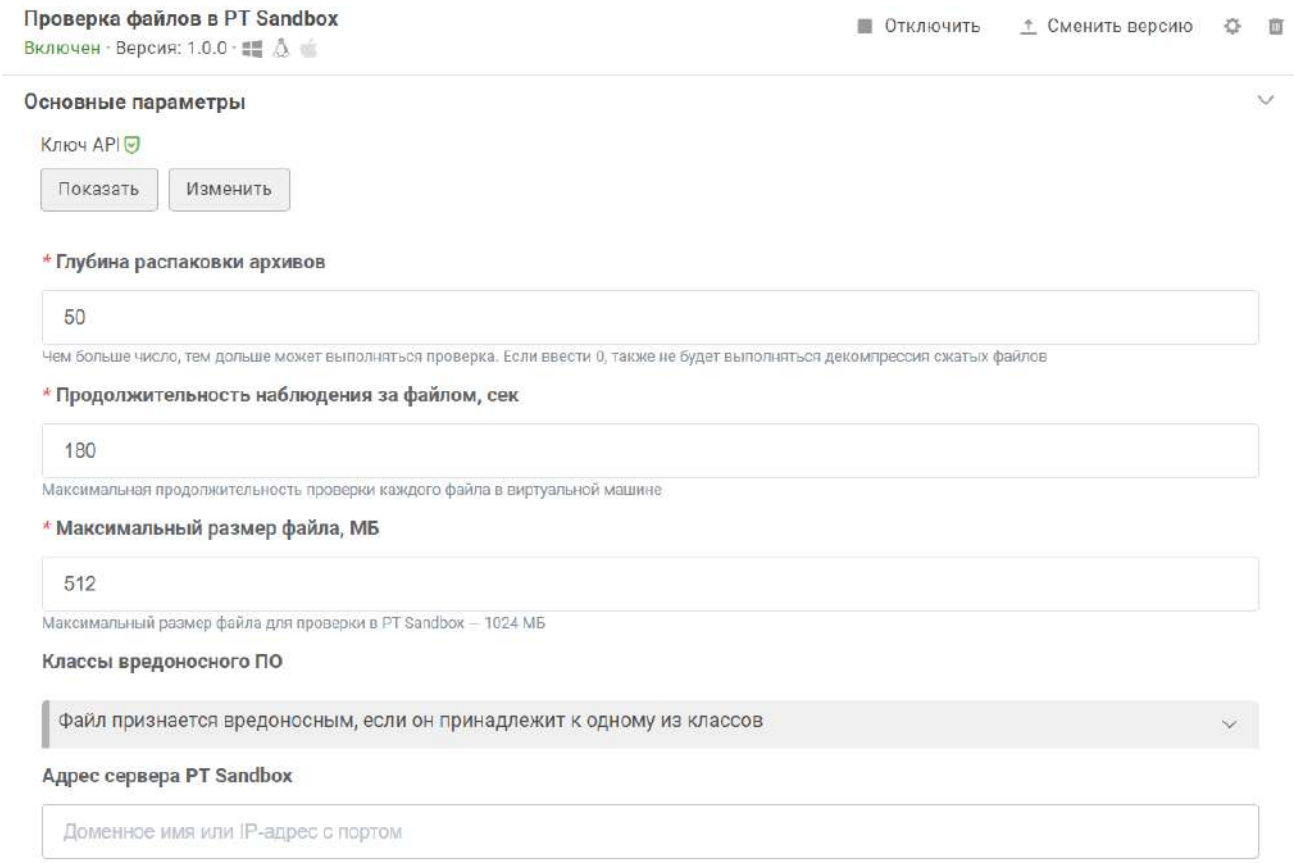

Рисунок 12. Настройка модуля «Проверка файлов в PT Sandbox»

4. В поле **Адрес сервера PT Sandbox** введите адрес сервера PT Sandbox, на который вы хотите отправлять файлы.

5. В поле **Ключ API** введите ключ для доступа к публичному API PT Sandbox.

   Примечание. Для генерации ключа API вам нужно выполнить команду `sudo ptmsctl api auth create <Название ключа API>` в консольной утилите PT Sandbox. Подробная инструкция по генерации ключа API приведена в разделе «Генерация токена доступа» в Справочном руководстве по публичному API из комплекта поставки PT Sandbox.

6. Если требуется, задайте дополнительные параметры модуля (см. приложение Б).
7. Если требуется, выберите действия, которые будут выполняться при регистрации событий ИБ (см. раздел 19.5).
8. Нажмите кнопку **Сохранить**.

Модуль настроен.

19.4.3. Настройка модуля «Сканирование в режима аудита (MaxPatrol VM)»

Вы можете настроить запуск сканирования в режиме аудита по расписанию или при регистрации события ИБ, а также запускать его вручную (см. раздел 20.10.1). Ориентировочное время сканирования около 10 минут, обработка результатов в MaxPatrol VM — до 30 минут. При сильной нагрузке на сервер MaxPatrol VM время обработки результатов может увеличиться.

При потере соединения между агентом и сервером MaxPatrol EDR сканирование по расписанию будет запускаться в обычном порядке. Результаты сканирования будут храниться в локальной базе данных агента и будут отправлены в MaxPatrol VM после восстановления связи.

Внимание! Сканирование в режиме аудита может существенно влиять на загрузку процессора конечного устройства. Не рекомендуется настраивать частый запуск сканирования по расписанию, а также назначать его на события ИБ, которые регистрируются постоянно.

► Чтобы настроить модуль «Сканирование в режиме аудита (MaxPatrol VM)»:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

3. В списке **Включенные** выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».

   Отобразится список параметров, событий и действия модуля.

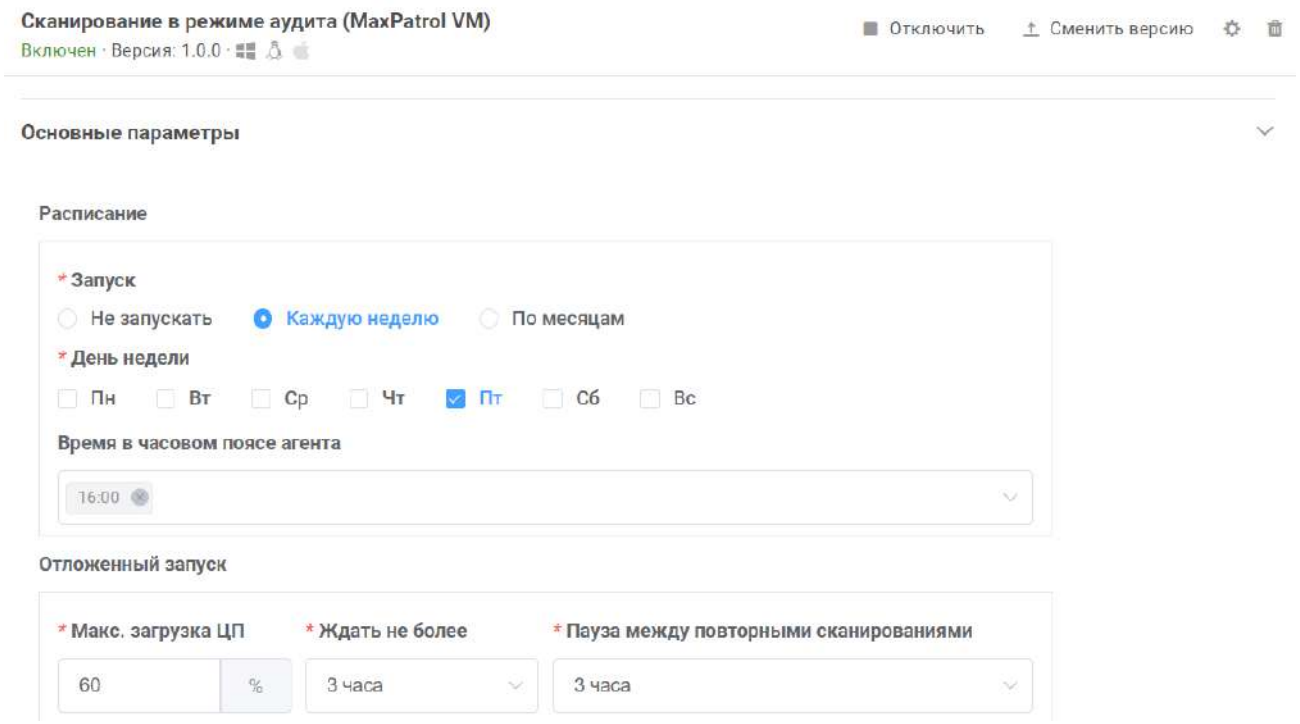

Рисунок 13. Настройка модуля «Сканирование в режиме аудита (MaxPatrol VM)»

4. В блоке параметров **Расписание** настройте запуск сканирования по расписанию.
5. Если требуется, задайте дополнительные параметры модуля (см. приложение Б).
6. Если требуется, выберите действия, которые будут выполняться при регистрации событий ИБ (см. раздел 19.5).
7. Нажмите кнопку **Сохранить**.

Модуль настроен.

19.4.4. Настройка модуля «Коррелятор»

Далее приведена информация о передаче данных в модули «Коррелятор» и «Коррелятор (Linux)», а также дана инструкция по добавлению исключений для правил корреляций.

В этом разделе

19.4.4.1. Передача данных в модуль «Коррелятор»

Модуль «Коррелятор» использует для работы данные из журнала событий Windows. Для корректной работы модуля вам нужно:

— назначить на группу агентов с модулем «Коррелятор» политику с модулями «WinEventLog: сбор данных из журнала событий Windows» и «Установщик Sysmon»;

— добавить канал `Microsoft-Windows-Sysmon/Operational` в список каналов, обрабатываемых модулем «WinEventLog: сбор данных из журнала событий Windows».

19.4.4.2. Передача данных в модуль «Коррелятор (Linux)»

Модуль «Коррелятор (Linux)» использует для работы данные из журналов auditd. Для корректной работы модуля вам нужно:

— вручную установить и настроить на конечных устройствах компонент auditd;

— назначить на группу агентов с модулем «Коррелятор (Linux)» политику с модулем «Сбор данных из файлов журналов».

19.4.4.3. Добавление исключений

Вы можете добавлять исключения для правил корреляций. Это позволит уменьшить количество ложных срабатываний правил, которые могут возникать из-за особенностей вашей инфраструктуры. Исключение состоит из нескольких условий в формате регулярного выражения (regex).

► Чтобы добавить исключение:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

3. В списке **Включенные** выберите модуль «Коррелятор».

   Отобразится список параметров, событий и действия модуля.

4. В блоке параметров **Список исключений** нажмите кнопку **Добавить**.

5. В поле **Переменные** укажите одну или несколько переменных для первого условия в регулярном выражении.

В регулярном выражении указанные переменные будут разделяться логическим оператором ИЛИ. Например, если вы хотите исключить срабатывания правила корреляции на внутреннюю утилиту, вы можете указать переменные, в которых передается имя исполняемого файла: `object.fullpath`, `object.process.cmdline`, `object.name`.

Примечание. Подробную информацию о событии модуля «Коррелятор» вы можете посмотреть на странице **События** в панели **Сводка**.

6. В поле **Регулярное выражение** введите регулярное выражение, которое будет применяться к списку заданных переменных.

   Например, вы можете ввести имя исполняемого файла вашей утилиты. В этом случае первое условие в исключении сработает, если хотя бы в одной заданной переменной будет содержаться указанное имя файла.

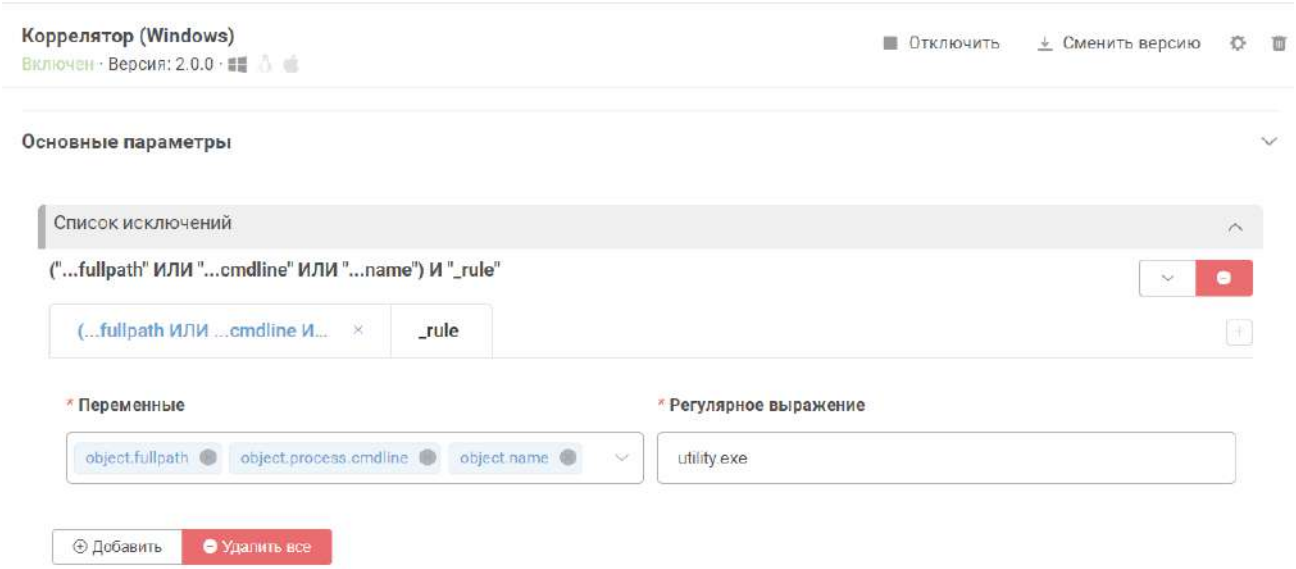

Рисунок 14. Добавление исключения

7. Если требуется, нажмите + и настройте второе условие, повторив шаги 5—6.

   В регулярном выражении условия будут разделяться логическим оператором И. Во втором условии вы можете указать правило, которое дает ложное срабатывание. Для этого в поле **Переменные** нужно ввести `_rule`, а в поле **Регулярное выражение** — имя правила.

8. Если требуется, настройте дополнительные условия.

   Например, вы можете добавить исключение только для одного узла. Для этого в поле **Переменные** нужно выбрать переменную `event_src.host`, а в поле **Регулярное выражение** ввести имя узла.

9. Нажмите кнопку **Сохранить**.

Исключение добавлено.

19.4.5. Настройка модуля «Перенаправление DNS-запросов (sinkholing)»

- Чтобы настроить модуль «Перенаправление DNS-запросов (sinkholing)»:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

3. В списке **Включенные** выберите модуль «Перенаправление DNS-запросов (sinkholing)».

   Отобразится список параметров, событий и действия модуля.

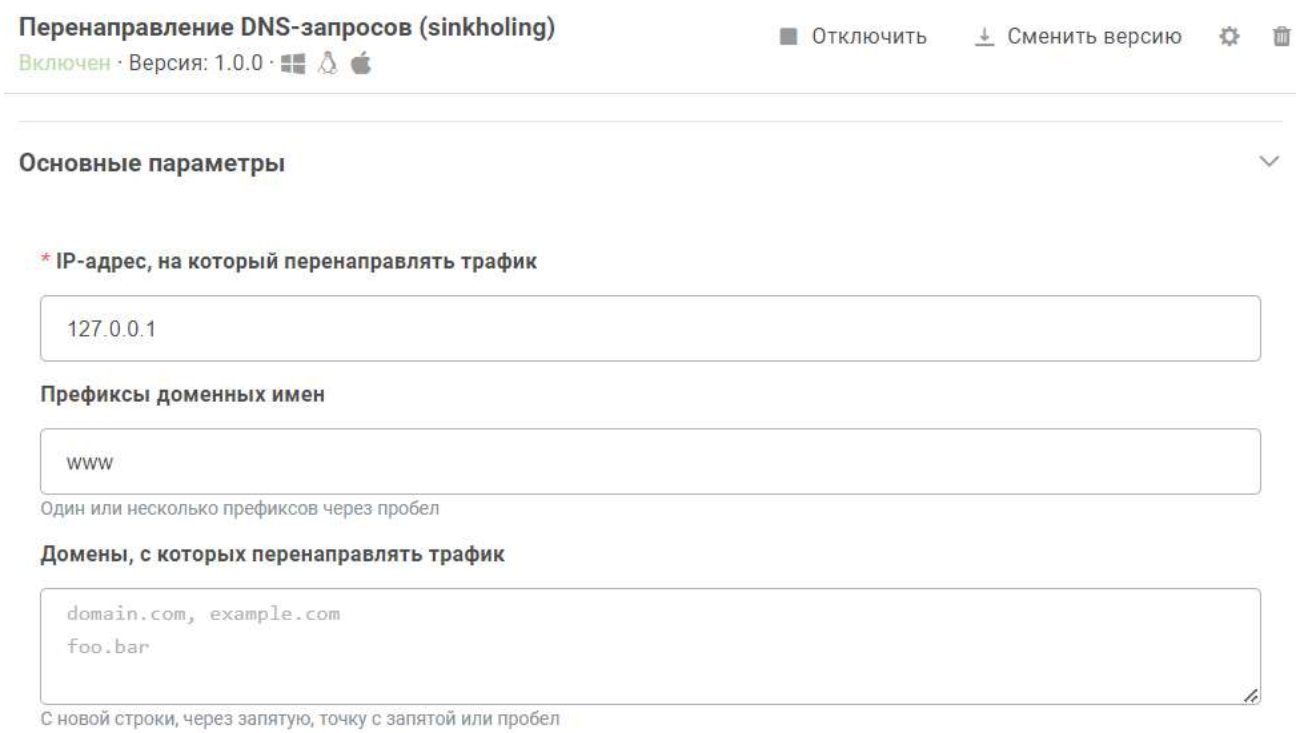

Рисунок 15. Настройка модуля «Перенаправление DNS-запросов (sinkholing)»

4. В поле **IP-адрес, на который перенаправлять трафик** введите IP-адрес, на который будет перенаправляться трафик.

   Это может быть адрес специального сервера, на котором входящие данные будут анализироваться, или неиспользуемый внутренний IP-адрес для блокировки трафика, например `127.0.0.1` или `0.0.0.0`.

5. В поле **Домены, с которых перенаправлять трафик** введите один или несколько доменов, трафик с которых будет перенаправляться.

Трафик будет перенаправляться со всех адресов заданных доменов.

6. Если требуется, в поле **Префиксы доменных имен** введите один или несколько префиксов, которые будут добавляться ко всем доменным именам.

   Например, если вы хотите перенаправлять трафик с адресов mail.example.com и mail.example.net, вам нужно добавить `example.com` и `example.net` в список доменов, а `mail` в список префиксов.

7. Нажмите кнопку **Сохранить**.

Модуль настроен.

19.5. Настройка автоматического реагирования

Для настройки автоматического реагирования вам нужно назначить действия, которые будут выполняться при регистрации того или иного события ИБ. После добавления модуля в политику для всех событий ИБ, которые он регистрирует, назначено только одно автоматическое действие — **Сохранить в БД**. Назначить действия на события модуля вы можете двумя способами:

— выбрав для события необходимые действия (см. раздел 19.5.1);

— выбрав для действия события, при регистрации которых его нужно выполнять (см. раздел 19.5.2).

Примечание. Для автоматического выполнения действий модулям требуются данные, которые передаются с помощью переменных в событиях. Вы не сможете назначить действие на событие, если это событие не содержит необходимых данных.

Если на одно событие назначено несколько действий, то порядок их выполнения определяется приоритетом. Каждое действие имеет приоритет от 1 до 100 в условных единицах. Если у двух действий одинаковый приоритет, то они будут выполняться в случайном порядке.

Далее приведены инструкции по назначению действий на события.

В этом разделе

19.5.1. Назначение действий на событие модуля

► Чтобы назначить действия на событие модуля:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

Откроется карточка политики.

3. В списке **Включенные** выберите модуль, на события которого вы хотите назначить действия.
4. В блоке параметров **События** напротив нужного события нажмите .

   Откроется окно **Назначение действий**.

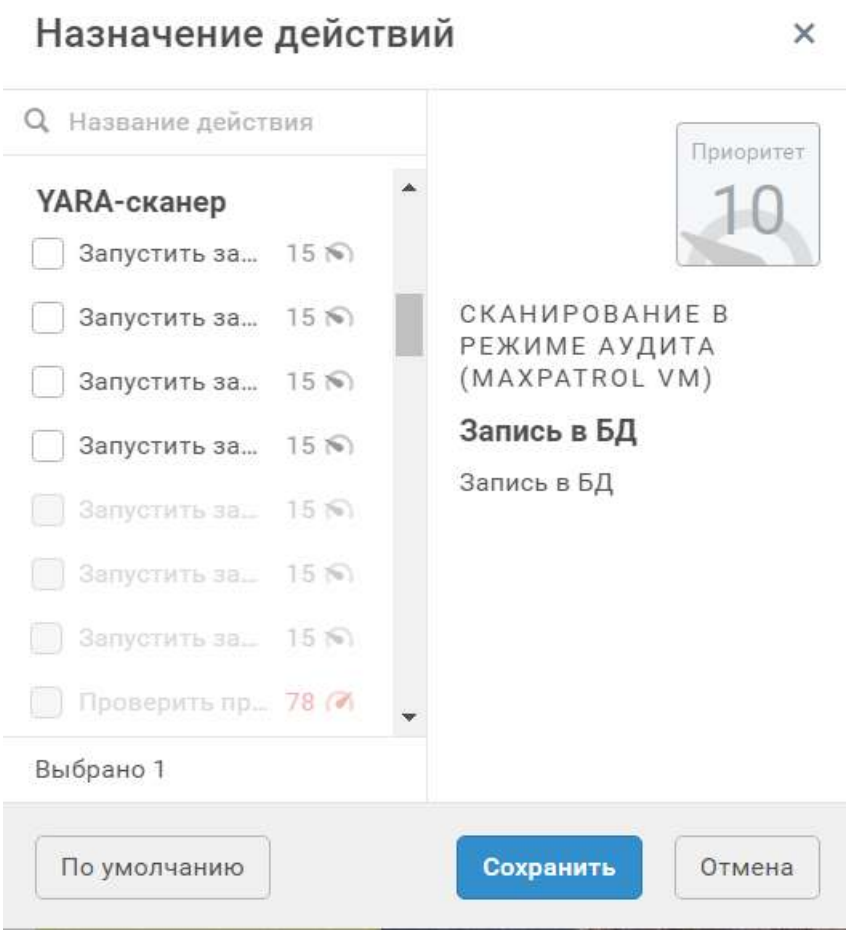

Рисунок 16. Назначение действий

5. Установите флажки напротив тех действий, которые нужно автоматически выполнять при регистрации этого события.
6. Нажмите кнопку **Сохранить**.

Действия назначены.

19.5.2. Массовое назначение действия на события модуля

Вы можете назначить конкретное действие на выбранные события модуля или сразу на все с помощью мастера назначения действий.

► Чтобы назначить действие на события модуля:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

3. В списке **Включенные** выберите модуль, на события которого вы хотите назначить действия.

4. В блоке параметров **События** нажмите кнопку **Мастер назначения действий**.

   Откроется окно **Мастер назначения действий**.

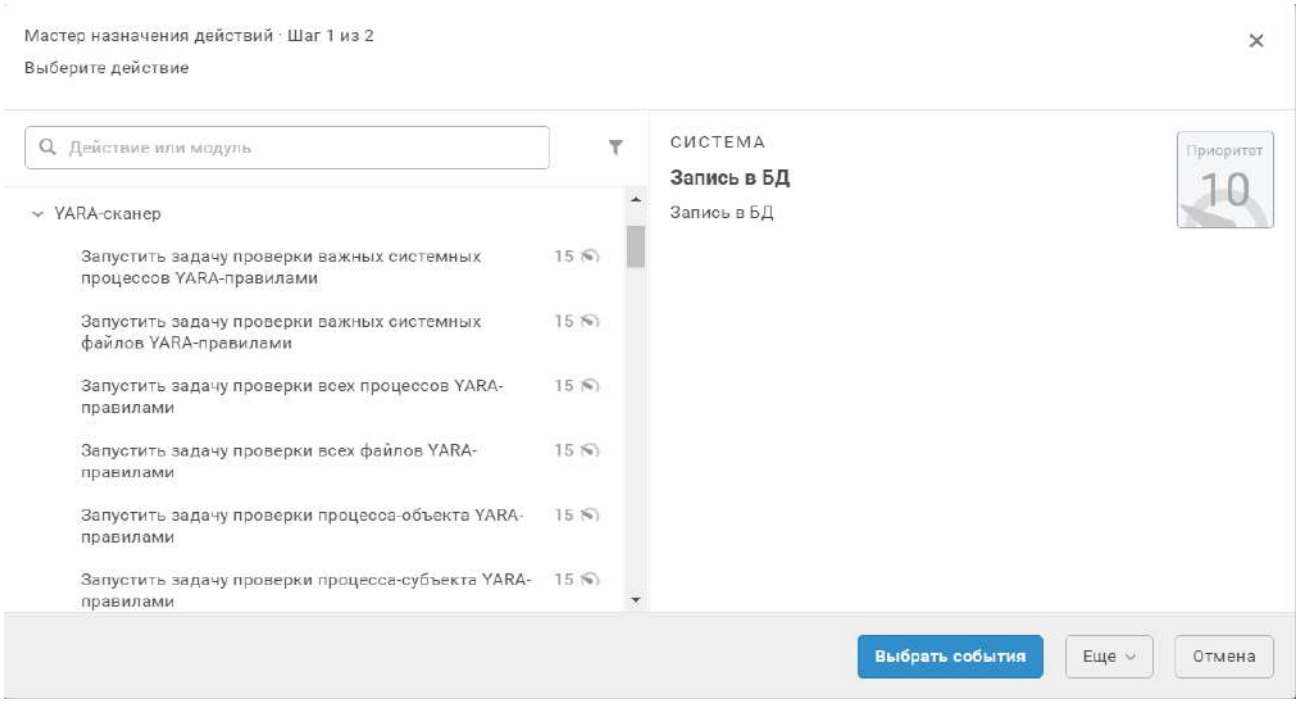

Рисунок 17. Выбор действия

5. Выберите действие, которое вы хотите назначить на события.

   Примечание. Вы можете отфильтровать действия и изменить их группировку по кнопке .

6. Нажмите кнопку **Выбрать события**.

   Примечание. Вы можете назначить действие на все доступные события модуля сразу, нажав кнопку **Еще** и в раскрывшемся меню выбрав пункт **Назначить на все доступные события**.

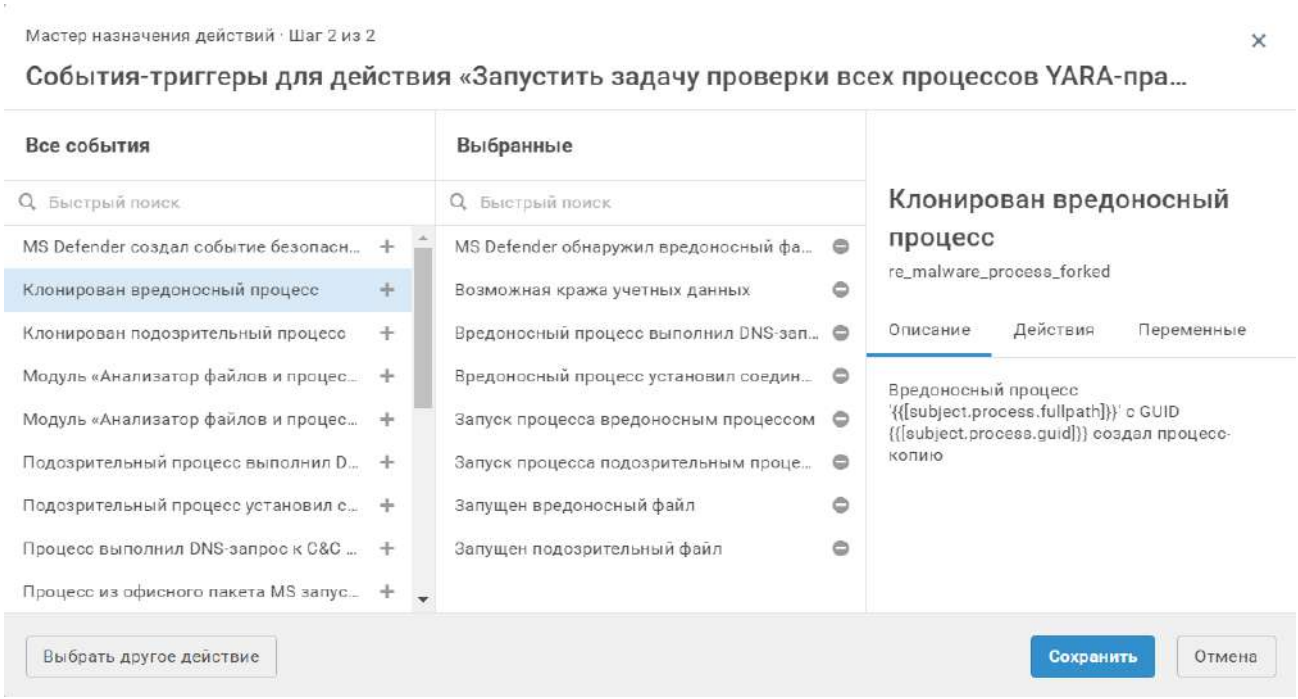

Рисунок 18. Выбор событий

7. Нажмите + напротив тех событий, при регистрации которых нужно выполнять выбранное действие.
8. Нажмите кнопку **Сохранить**.

Действие назначено на события модуля.

19.6. Отключение модуля

Вы можете убрать модуль из политики, сохранив его конфигурацию. Для этого вам нужно отключить модуль. В дальнейшем вы можете добавить модуль обратно, включив его (см. раздел 19.7).

► Чтобы отключить модуль в политике:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.
2. Нажмите на название политики.

   Откроется карточка политики.
3. В списке **Включенные** выберите модуль.
4. Нажмите кнопку **Отключить**.

Внимание! Если политика назначена на группу (см. раздел 18.5), то сразу после отключения модуль будет автоматически удален со всех агентов группы.

Модуль отключен.

См. также

Включение модуля (см. раздел 19.7)

19.7. Включение модуля

Ранее отключенный модуль (см. раздел 19.6) может быть включен в прежней конфигурации.

- Чтобы включить модуль:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

3. В списке **Отключенные** выберите модуль.

4. Нажмите кнопку **Включить**.

   Модуль включен. Если политика назначена на группу (см. раздел 18.5), то сразу после включения модуль будет автоматически установлен на всех агентах группы.

Если модуль уже установлен на агентах группы другой политикой, то в этой политике он останется в состоянии «Отключен».

19.8. Изменение версии модуля в политике

Вы можете установить на агентах любую версию модуля, доступную на сервере MaxPatrol EDR. Для этого вам нужно изменить версию модуля в политике. При установке версии ниже той, что используется сейчас, может быть сброшена часть конфигурации модуля и удалены некоторые события.

- Чтобы изменить версию модуля в политике:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

3. Выберите модуль.

4. Нажмите кнопку **Сменить версию**.

Откроется всплывающее окно с выбором версии.

5. Нажмите кнопку **Установить** напротив версии модуля.

Версия модуля изменена.

19.9. Удаление модуля из политики

Вы можете удалить модуль из политики.

Внимание! Если политика назначена на группу (см. раздел 18.5), то модуль будет автоматически удален со всех агентов группы.

► Чтобы удалить модуль из политики:

1. В главном меню в разделе **EDR** выберите пункт **Политики**.

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

3. Выберите модуль.

4. Нажмите  и подтвердите удаление.

Модуль удален из политики.

См. также

Назначение политики на группу агентов (см. раздел 18.5)

20. Ручное реагирование на угрозы

В некоторых случаях автоматическое реагирование на агентах недопустимо, например если заведомо известно, что это может привести к потере важной информации. В таких случаях вы можете реагировать на угрозы вручную. Набор доступных способов реагирования зависит от установленных на агенте модулей реагирования (см. раздел 19.1).

Далее приведены инструкции по ручному реагированию на угрозы.

В этом разделе

20.1. Реагирование на событие

При регистрации события вы можете вручную запустить реагирование на него. Список доступных действий для реагирования определяется модулями, которые установлены на узле, и данными, которые передаются в событии.

- Чтобы запустить реагирование:

  1. В главном меню выберите раздел **События**.

     Откроется страница **События**.
  2. Если требуется, отфильтруйте события в списке.
  3. В списке событий выберите событие, на которое вы хотите отреагировать.
  4. В панели **Сводка** нажмите кнопку **Реагировать**.

Откроется окно **Реагирование**.

5. Выберите необходимое действие.

Реагирование запущено.

20.2. Удаление файлов

Вы можете удалять файлы на конечном устройстве с помощью двух модулей — «Удаление файлов» и «Драйвер сбора данных и реагирования». Модуль «Драйвер сбора данных и реагирования» работает на уровне ядра ОС, поэтому имеет более высокий уровень привилегий для удаления файлов. Например, если файл задействован в процессе, то модуль «Драйвер сбора данных и реагирования» завершит процесс и удалит файл, тогда как модуль «Удаление файлов» не сможет его удалить.

Далее в разделе приведена инструкция по удалению файлов с помощью модуля «Удаление файлов». Удаление файлов с помощью модуля «Драйвер сбора данных и реагирования» выполняется таким же способом.

- Чтобы удалить файл на конечном устройстве:

1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

   Откроется страница **Агенты EDR**.

2. Нажмите на название агента, установленного на конечном устройстве.

   Откроется карточка агента.

3. Выберите модуль «Удаление файлов».

4. Нажмите .

   Откроется карточка модуля.

5. Нажмите кнопку **Выбрать действие** и в раскрывшемся меню выберите действие.

6. Введите путь к файлу.

7. Нажмите кнопку **Выполнить действие**.

Файл удален.

20.3. Завершение процессов

Вы можете завершать процессы на конечном устройстве с помощью двух модулей — «Завершение процессов» и «Драйвер сбора данных и реагирования». Модуль «Драйвер сбора данных и реагирования» работает на уровне ядра ОС, поэтому имеет более высокий уровень привилегий для завершения процессов. Например, в некоторых случаях модуль «Завершение процессов» не сможет завершить процесс из-за недостатка прав.

Вы можете завершить:

— все процессы, запущенные указанным исполняемым файлом;

— все процессы с указанным именем;

— процесс с указанными именем и идентификатором;

— родительские процессы с указанными именами и идентификаторами;

— дерево процессов (нужно указать имя и идентификатор родительского процесса);

— несколько деревьев процессов (нужно указать имя родительского процесса).

Далее приведена инструкция по завершению процессов с указанным именем с помощью модуля «Завершение процессов».

► Чтобы завершить процессы на конечном устройстве:

1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

   Откроется страница **Агенты EDR**.

2. Нажмите на название агента, установленного на конечном устройстве.

   Откроется карточка агента.

3. Выберите модуль «Завершение процессов».

4. Нажмите ⚙.

   Откроется карточка модуля.

5. Нажмите кнопку **Выбрать действие** и в раскрывшемся меню выберите **Завершить все процессы, используя имя**.

6. Введите имя процесса в формате `{"proc_name": "<Имя процесса>"}`.

7. Нажмите кнопку **Выполнить действие**.

Процессы завершены.

20.4. Изоляция узлов

Вы можете изолировать узел, на котором установлен агент, двумя способами — полностью, отключив все сетевые адаптеры, или частично, сохранив для него связь с сервером агентов и адресами из списка исключений.

► Чтобы изолировать узел, на котором установлен агент:

1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

   Откроется страница **Агенты EDR**.

2. Нажмите на название агента.

Откроется карточка агента.

3. Выберите модуль «Изоляция узлов».
4. Нажмите ⚙.

   Откроется карточка модуля.
5. Выберите способ изоляции узла.
6. Настройте время, через которое изоляция узла будет снята автоматически.
7. Нажмите кнопку **Изолировать**.

   Примечание. Вы можете обновить статус изоляции узла по кнопке ↻.

Узел изолирован.

- Чтобы досрочно снять частичную изоляцию узла,

  нажмите кнопку **Снять изоляцию**.

  Примечание. Для досрочного снятия полной изоляции узла вам нужно включить сетевые адаптеры на устройстве вручную.

20.5. Блокировка по IP-адресу

Вы можете заблокировать все сетевые соединения узла, на котором установлен агент, с заданным IP-адресом. Это может быть полезно, если вы обнаружили подозрительное соединение и хотите его прервать. Если этот IP-адрес уже заблокирован на уровне политики, вы можете дополнительно заблокировать его на агенте. В таком случае соединения узла с этим адресом не будут разблокированы даже после изменения конфигурации модуля в политике. Заблокировать IP-адрес сервера MaxPatrol EDR невозможно.

- Чтобы заблокировать IP-адрес на агенте:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.
  2. Нажмите на название агента, на котором вы хотите заблокировать IP-адрес.

     Откроется карточка агента.
  3. Выберите модуль «Блокировка по IP-адресу».
  4. Нажмите ⚙.

     Откроется карточка модуля.
  5. Введите IP-адрес в формате IPv4, IPv6 или подсеть в нотации CIDR.
  6. Нажмите кнопку **Заблокировать**.

  IP-адрес заблокирован на агенте.

- Чтобы разблокировать IP-адрес на агенте,

  напротив IP-адреса в списке нажмите кнопку **Разблокировать**.

  Примечание. Соединения с этим IP-адресом не восстановятся, если он заблокирован на уровне политики.

20.6. Перенаправление DNS-запросов

Если вы заметили на узле подозрительный или вредоносный трафик с какого-либо домена, вы можете перенаправить все DNS-запросы с этого домена на специальный адрес, заданный в параметрах модуля (см. раздел 19.4.5) в политике.

- Чтобы перенаправить DNS-запросы с домена:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.
  2. Нажмите на название агента, на котором вы хотите перенаправлять DNS-запросы.

     Откроется карточка агента.
  3. Выберите модуль «Перенаправление DNS-запросов (sinkholing)».
  4. Нажмите ⚙.

     Откроется карточка модуля.
  5. Введите один или несколько доменов, трафик с которых нужно перенаправлять.
  6. Нажмите кнопку **Добавить**.

  DNS-запросы с домена перенаправлены.

- Чтобы отменить перенаправление DNS-запросов,

  напротив домена в списке нажмите кнопку **Удалить**.

  Примечание. Отменить перенаправление DNS-запросов с доменов, которые заданы в политике, можно только в политике.

20.7. Работа с модулем «YARA-сканер»

Далее приведены инструкции по работе с модулем «YARA-сканер».

В этом разделе

Просмотр правил (см. раздел 20.7.3)

О кэшировании результатов проверок (см. раздел 20.7.4)

20.7.1. Запуск проверки

Модуль «YARA-сканер» выполняет сигнатурный анализ на основе правил YARA. Вы можете проверить:

— файл или папку с файлами;

— один или несколько процессов;

— важные системные файлы и процессы (быстрая проверка);

— все файлы и процессы (полная проверка).

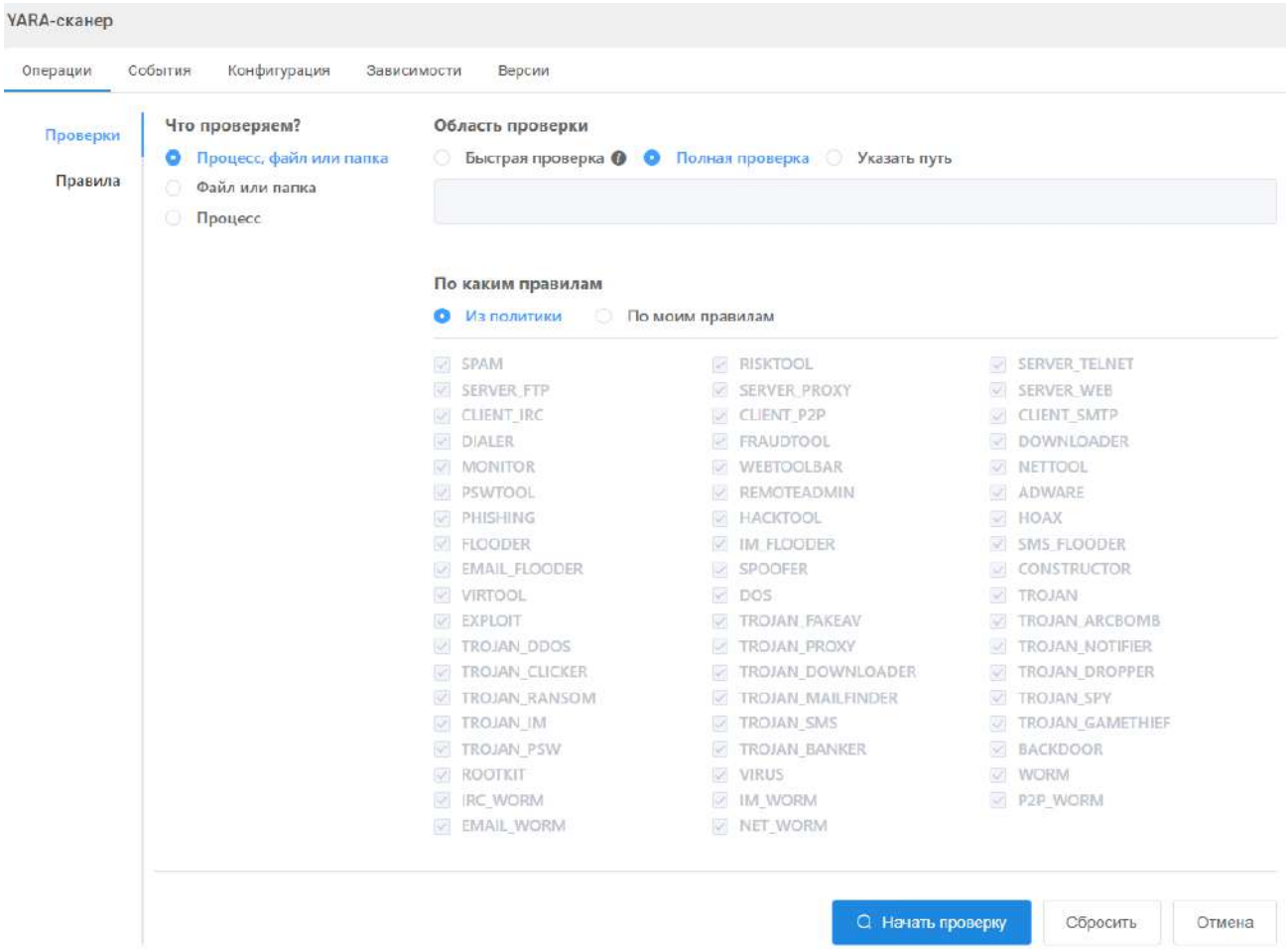

Рисунок 19. Запуск проверки

По умолчанию для проверки выбраны правила YARA, заданные в конфигурации политики (см. раздел 19.4). Вы можете вставить или импортировать свои правила для проверки.

Проверки выполняются в порядке очереди. При этом в конфигурации политики (см. раздел 19.4) вы можете назначить автоматические проверки, которые будут выполняться в приоритетном порядке, вне очереди.

- Чтобы запустить проверку:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Нажмите на название агента, на котором вы хотите запустить проверку.

     Откроется карточка агента.

  3. Выберите модуль «YARA-сканер».

  4. Нажмите ⚙.

     Откроется карточка модуля.

  5. Нажмите кнопку **Новая проверка**.

  6. Задайте параметры проверки.

  7. Нажмите кнопку **Начать проверку**.

  Проверка запущена.

20.7.2. Просмотр результатов проверки

Вы можете просмотреть список вредоносных файлов и процессов, которые были найдены с помощью правил YARA.

- Чтобы просмотреть результаты проверки:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Нажмите на название агента, на котором запускалась проверка модулем «YARA-сканер».

     Откроется карточка агента.

  3. Выберите модуль «YARA-сканер».

  4. Нажмите ⚙.

     Откроется карточка модуля и отобразится список проверок с указанием их статуса.

  5. Нажмите на дату и время начала проверки.

     Отобразятся результаты проверки.

20.7.3. Просмотр правил

Вы можете просмотреть список правил YARA и информацию о них. Эта информация может быть полезна при настройке модуля в политике (см. раздел 19.4). Например, вы можете отключить проверки на некоторые семейства вредоносного ПО.

- Чтобы просмотреть правила:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Нажмите на название агента, на котором установлен модуль «YARA-сканер».

     Откроется карточка агента.

  3. Выберите модуль «YARA-сканер».

  4. Нажмите  .

     Откроется карточка модуля.

  5. Выберите раздел **Правила**.

     Отобразится список правил.

20.7.4. О кэшировании результатов проверок

Частый запуск сигнатурного анализа файлов и процессов на основе правил YARA вызывает чрезмерное потребление ресурсов конечного устройства. Это может привести к увеличению продолжительности проверок, образованию очереди и, как следствие, медленному реагированию на угрозы.

Чтобы избежать таких ситуаций, в MaxPatrol EDR результаты проверок кэшируются. Срок хранения результатов сканирования файлов не ограничен, срок хранения результатов сканирования процессов вы можете задать в конфигурации политики (см. раздел 19.4). Перед запуском новой проверки MaxPatrol EDR проверяет сохраненные результаты и использует их, если такой файл или процесс уже проверялся. MaxPatrol EDR идентифицирует файлы по хеш-сумме, а процессы по идентификатору и пути к исполняемому файлу.

Если модуль взял результат сканирования из кэша, то к названию зарегистрированного события добавляется префикс `[Кэш]`. Для проверки наиболее важных файлов и процессов вы можете использовать специальные действия модуля (см. раздел 19.5), которые не будут брать результаты из кэша.

20.8. Работа с модулем «Проверка файлов в PT Sandbox»

Далее приведены инструкции по работе с модулем «Проверка файлов в PT Sandbox».

В этом разделе

20.8.1. Получение данных о проверенных файлах

Информация о файлах, отправленных на проверку с агента в PT Sandbox, содержится в таблице `files` в базе данных агента. Информация обо всех проверенных файлах со всех агентов с такой же политикой содержится в таблице `feeds` в базах данных и агента, и сервера MaxPatrol EDR. Вы можете получить данные о проверенных файлах с помощью SQL-запроса к базе данных агента или сервера.

- Чтобы получить информацию о проверенных в PT Sandbox файлах:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Нажмите на название агента, на котором установлен модуль «Проверка файлов в PT Sandbox».

     Откроется карточка агента.

  3. Выберите модуль «Проверка файлов в PT Sandbox».

  4. Нажмите ⚙.

     Откроется карточка модуля.

  5. Если требуется, измените SQL-запрос.

  6. Выберите базу данных, из которой вы хотите получить данные.

  7. Нажмите кнопку **Выполнить запрос**.

     Отобразится информация о проверенных файлах.

20.8.2. Проверка файлов в PT Sandbox

- Чтобы отправить файл с конечного устройства на проверку в PT Sandbox:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Нажмите на название агента, установленного на конечном устройстве.

     Откроется карточка агента.

  3. Выберите модуль «Проверка файлов в PT Sandbox».

  4. Нажмите ⚙.

Откроется карточка модуля.

5. Введите путь к файлу.
6. Нажмите кнопку **Проверить файл**.

Файл отправлен на проверку в PT Sandbox.

20.9. Отправка событий на syslog-сервер

► Чтобы отправить событие на syslog-сервер:

1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

   Откроется страница **Агенты EDR**.

2. Нажмите на название агента, событие с которого вы хотите отправить на syslog-сервер.

   Откроется карточка агента.

3. Выберите модуль «Отправка событий на syslog-сервер».
4. Нажмите ⚙.

   Откроется карточка модуля.

5. Введите данные о событии в формате `{'name': '<Название события>', 'data': {<Атрибуты события>}}`.
6. Нажмите кнопку **Отправить**.

Событие отправлено на syslog-сервер.

20.10. Работа с модулем «Сканирование в режиме аудита (MaxPatrol VM)»

Сканирование в режиме аудита используется:

— Для сканирования узлов методом черного ящика. Модуль обнаруживает открытые порты и сетевые сервисы на этих портах. Затем обнаруживает уязвимости на сетевых сервисах.

— Аудита узлов методом белого ящика. Модуль определяет детальную конфигурацию операционной системы, установленной на узле, перечень установленного программного обеспечения, список открытых портов, перечень зарегистрированных пользователей. Формирует перечень уязвимостей и карту сети.

— Сканирования веб-приложения. Модуль обнаруживает параметры веб-приложения, выявляет уязвимые параметры, формирует перечень уязвимых библиотек.

— Поиска уязвимостей в режиме пентеста. Модуль выполнит поиск уязвимостей с указанными CVE-идентификаторами.

После завершения сканирования модуль автоматически отправляет собранные данные в MaxPatrol VM.

Далее приведены инструкции по работе с модулем «Сканирование в режиме аудита (MaxPatrol VM)».

В этом разделе

20.10.1. Запуск сканирования на агенте

Вы можете вручную запустить сканирование в режиме аудита на агенте. Если на агенте уже выполняется сканирование, то оно не будет запущено повторно.

- Чтобы запустить сканирование:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.
  2. Нажмите на название агента, на котором вы хотите запустить сканирование.

     Откроется карточка агента.
  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  4. Нажмите  .

     Откроется карточка модуля.
  5. Нажмите кнопку **Запустить сканирование**.

  Сканирование запущено. Вы можете остановить сканирование по кнопке **Остановить сканирование**.

Скачать журнал работы модуля вы можете по кнопке **Скачать журнал модуля**.

20.10.2. Запуск сканирования на всех агентах группы

Вы можете вручную запустить сканирование в режиме аудита сразу на всех агентах группы. Сканирование на агенте из группы не будет запущено, если с ним нет связи или на нем уже выполняется сканирование.

- Чтобы запустить сканирование на всех агентах группы:

  1. В главном меню в разделе **EDR** выберите пункт **Группы агентов**.

     Откроется страница **Группы агентов EDR**.

  2. Нажмите на название группы, на агентах которой вы хотите запустить сканирование.

     Откроется карточка группы агентов.

  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».

  4. Нажмите ⚙.

     Откроется карточка модуля.

  5. Нажмите кнопку **Запустить сканирование**.

  Сканирование запущено.

20.10.3. Отключение запуска сканирования по расписанию на агенте

Вы можете отключить запуск сканирования по расписанию. В этом случае сканирование на агенте будет запускаться только вручную — или при регистрации того или иного события ИБ, если это было настроено в политике.

- Чтобы отключить запуск сканирования по расписанию:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Нажмите на название агента, на котором вы хотите отключить запуск сканирования по расписанию.

     Откроется карточка агента.

  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».

  4. Нажмите ⚙.

     Откроется карточка модуля.

  5. Нажмите кнопку **Отключить запуск по расписанию**.

  Запуск сканирования по расписанию отключен. Вы можете повторно включить запуск по расписанию по кнопке **Включить запуск по расписанию**.

20.10.4. Отключение запуска сканирования по расписанию на всех агентах группы

Вы можете отключить запуск сканирования по расписанию. В этом случае сканирование на всех агентах группы будет запускаться только вручную — или при регистрации того или иного события ИБ, если это было настроено в политике.

- Чтобы отключить запуск сканирования по расписанию для группы агентов:

  1. В главном меню в разделе **EDR** выберите пункт **Группы агентов**.

     Откроется страница **Группы агентов EDR**.

  2. Нажмите на название группы, для агентов которой вы хотите отключить запуск сканирования по расписанию.

     Откроется карточка группы агентов.

  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».

  4. Нажмите ⚙.

     Откроется карточка модуля.

  5. Нажмите кнопку **Отключить запуск по расписанию**.

  Запуск сканирования по расписанию отключен. Вы можете повторно включить запуск по расписанию по кнопке **Включить запуск по расписанию**.

20.10.5. Просмотр результатов сканирования на агенте

- Чтобы просмотреть результаты сканирования:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Нажмите на название агента, на котором установлен модуль «Сканирование в режиме аудита (MaxPatrol VM)».

     Откроется карточка агента.

  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».

  4. Нажмите ⚙.

     Откроется карточка модуля.

  5. Выберите раздел **Сканирования**.

     Отобразятся результаты сканирования узла.

20.10.6. Просмотр результатов сканирования на всех агентах группы

- Чтобы просмотреть результаты сканирования:

  1. В главном меню в разделе **EDR** выберите пункт **Группы агентов**.

     Откроется страница **Группы агентов EDR**.

  2. Нажмите на название группы, на которую назначена политика с модулем «Сканирование в режиме аудита (MaxPatrol VM)».

     Откроется карточка группы агентов.

  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».

  4. Нажмите ⚙.

     Откроется карточка модуля.

  5. Выберите раздел **Сканирования**.

     Отобразятся результаты последнего сканирования всех узлов группы.

20.11. Отправка файлов

Вы можете отправлять файлы с конечного устройства во внешнюю систему, адрес которой задан в конфигурации политики (см. раздел 19.4). Например, это может быть песочница.

- Чтобы отправить файл:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Нажмите на название агента, файл с которого вы хотите отправить во внешнюю систему.

     Откроется карточка агента.

  3. Выберите модуль «Отправка файлов».

  4. Нажмите ⚙.

     Откроется карточка модуля.

  5. Введите путь к файлу.

  6. Нажмите кнопку **Отправить файл**.

  Файл отправлен.

20.12. Выполнение кода на языке Lua

- Чтобы выполнить произвольный код на языке Lua:

  1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

     Откроется страница **Агенты EDR**.

  2. Нажмите на название агента, на котором вы хотите выполнить код.

     Откроется карточка агента.

  3. Выберите модуль «Интерпретатор языка Lua».

  4. Нажмите ⚙.

     Откроется карточка модуля.

  5. Введите код.

  6. Нажмите кнопку **Выполнить**.

     Запустится выполнение кода.

21. Администрирование MaxPatrol EDR

В этом разделе приводятся инструкции по администрированию MaxPatrol EDR.

В этом разделе

21.1. Резервное копирование и восстановление конфигурации

Вы можете создать резервную копию с конфигурацией MaxPatrol EDR. При возникновении сбоя на физическом сервере вы можете установить MaxPatrol EDR на другой сервер и восстановить конфигурацию из ранее созданной резервной копии. Вы также можете восстановить удачную конфигурацию в случае некорректной настройки системы или перенести экспертные данные на другой сервер.

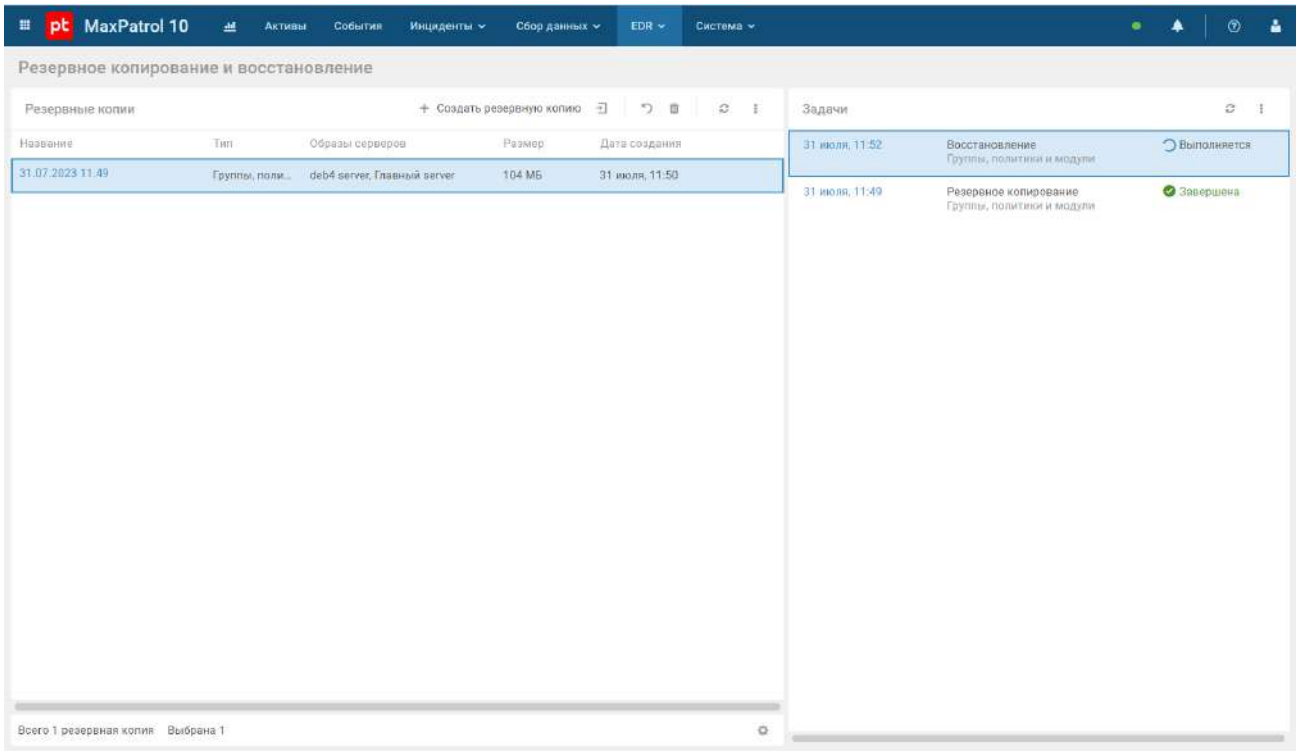

Рисунок 20. Резервные копии и задачи

В MaxPatrol EDR предусмотрено три типа резервных копий:

1. **Только политики.** Содержит только политики и их конфигурацию. После восстановления конфигурации системы из резервной копии этого типа вам нужно проверить связи групп агентов с политиками. Подходит для переноса экспертных данных на другой сервер.
2. **Группы, политики и модули.** Содержит группы агентов, модули и конфигурацию политик. После восстановления вам нужно добавить агенты в группы и проверить связи групп с политиками. Подходит для быстрой настройки системы на другом сервере.
3. **Полная копия, без событий.** Содержит полную конфигурацию системы, за исключением событий. После восстановления вам нужно проверить подключение агентов к серверу. Подходит для полного восстановления данных в случаях сбоя.

   Примечание. Тип резервной копии «Полная копия, без событий» будет доступен в следующей версии MaxPatrol EDR.

При создании или импорте резервной копии, а также при восстановлении конфигурации из нее в MaxPatrol EDR создается соответствующая задача. Задачи выполняются в порядке очереди, одновременно в системе может выполняться только одна задача.

В этом разделе

Создание резервной копии (см. раздел 21.1.1)

Импорт резервной копии (см. раздел 21.1.2)

Восстановление (см. раздел 21.1.3)

Отмена задачи (см. раздел 21.1.4)

Удаление резервной копии (см. раздел 21.1.5)

21.1.1. Создание резервной копии

- Чтобы создать резервную копию:

  1. В главном меню в разделе **EDR** выберите пункт **Управление** → **Резервное копирование и восстановление**.

     Откроется страница **Резервное копирование и восстановление**.

  2. Нажмите кнопку **Создать резервную копию**.

     Откроется окно **Новая резервная копия**.

  3. Если требуется, в поле **Название** измените название резервной копии.

  4. Если требуется, снимите флажки с тех серверов агентов, конфигурацию которых не требуется добавлять в резервную копию.

  5. В блоке параметров **Тип** выберите тип резервной копии.

  6. Нажмите кнопку **Создать**.

     В систему будет добавлена задача на создание резервной копии.

21.1.2. Импорт резервной копии

Вы можете импортировать резервную копию, созданную в другой системе. Перед импортом вам нужно скопировать архив с резервной копией на управляющий сервер в каталог `/opt/edr/backups`.

- Чтобы импортировать резервную копию:

  1. В главном меню в разделе **EDR** выберите пункт **Управление** → **Резервное копирование и восстановление**.

     Откроется страница **Резервное копирование и восстановление**.

  2. Нажмите .

     Откроется окно **Импорт резервной копии**.

  3. Введите имя архива с резервной копией, которую вы хотите импортировать в систему.

  4. Нажмите кнопку **Импортировать**.

     В систему будет добавлена задача на импорт резервной копии.

21.1.3. Восстановление

Во время восстановления конфигурации из резервной копии работа с системой в веб-интерфейсе будет приостановлена для всех пользователей. Также будет приостановлена работа всех модулей на агентах.

После восстановления конфигурации вам нужно выполнить одно из следующих действий:

— проверить связи групп агентов с политиками (после восстановления из резервной копии типа «Только политики»);

— добавить агенты в группы и проверить связи групп с политиками («Группы, политики и модули»);

— проверить подключение агентов к серверу («Полная копия, без событий»).

► Чтобы восстановить конфигурацию системы:

1. В главном меню в разделе **EDR** выберите пункт **Управление** → **Резервное копирование и восстановление**.

   Откроется страница **Резервное копирование и восстановление**.

2. В панели **Резервные копии** выберите резервную копию.

3. Нажмите ⮌.

   Откроется окно **Восстановление системы**.

4. Для каждого сервера агентов в соответствующем раскрывающемся списке выберите образ для восстановления из резервной копии.

   Внимание! Если для сервера агентов был выбран образ другого сервера, то ваша конфигурация и модули на агентах могут быть удалены.

5. Нажмите кнопку **Восстановить**.

   В систему будет добавлена задача на восстановление из резервной копии.

21.1.4. Отмена задачи

Вы можете отменить задачу на создание или импорт резервной копии, а также на восстановление конфигурации из нее.

► Чтобы отменить задачу:

1. В главном меню в разделе **EDR** выберите пункт **Управление** → **Резервное копирование и восстановление**.

   Откроется страница **Резервное копирование и восстановление**.

2. В панели **Задачи** выберите задачу, нажав на дату ее создания.

Откроется карточка задачи.

3. Нажмите кнопку **Отмена**.

Задача отменена.

21.1.5. Удаление резервной копии

Вы можете удалить резервную копию. При этом все задачи на восстановление из этой резервной копии будут отменены.

- Чтобы удалить резервную копию:

1. В главном меню в разделе **EDR** выберите пункт **Управление** → **Резервное копирование и восстановление**.

   Откроется страница **Резервное копирование и восстановление**.

2. В панели **Резервные копии** выберите резервную копию.
3. Нажмите  и подтвердите удаление.

Резервная копия удалена.

21.2. Автоматизация операций в системе

В этом разделе приводятся информация о планировщике задач в MaxPatrol EDR и инструкции по автоматизации операций в системе с его помощью.

В этом разделе

21.2.1. О планировщике задач

Вы можете автоматизировать операции с агентами с помощью планировщика задач. Это может быть полезно, если количество агентов в системе велико и работа с ними занимает много времени. В планировщике вы можете создать регулярную задачу:

— на обновление агентов до последней версии;

— установку выбранной версии агента;

— перемещение агентов в группу (можно использовать для авторизации агентов);

— удаление агентов.

Все задачи выполняются автоматически при соблюдении заданных условий. Каждая задача может выполняться неограниченное число раз. Работать с задачами вы можете на странице **Планировщик задач**. При выборе задачи в списке карточка с информацией о ней отображается в панели справа.

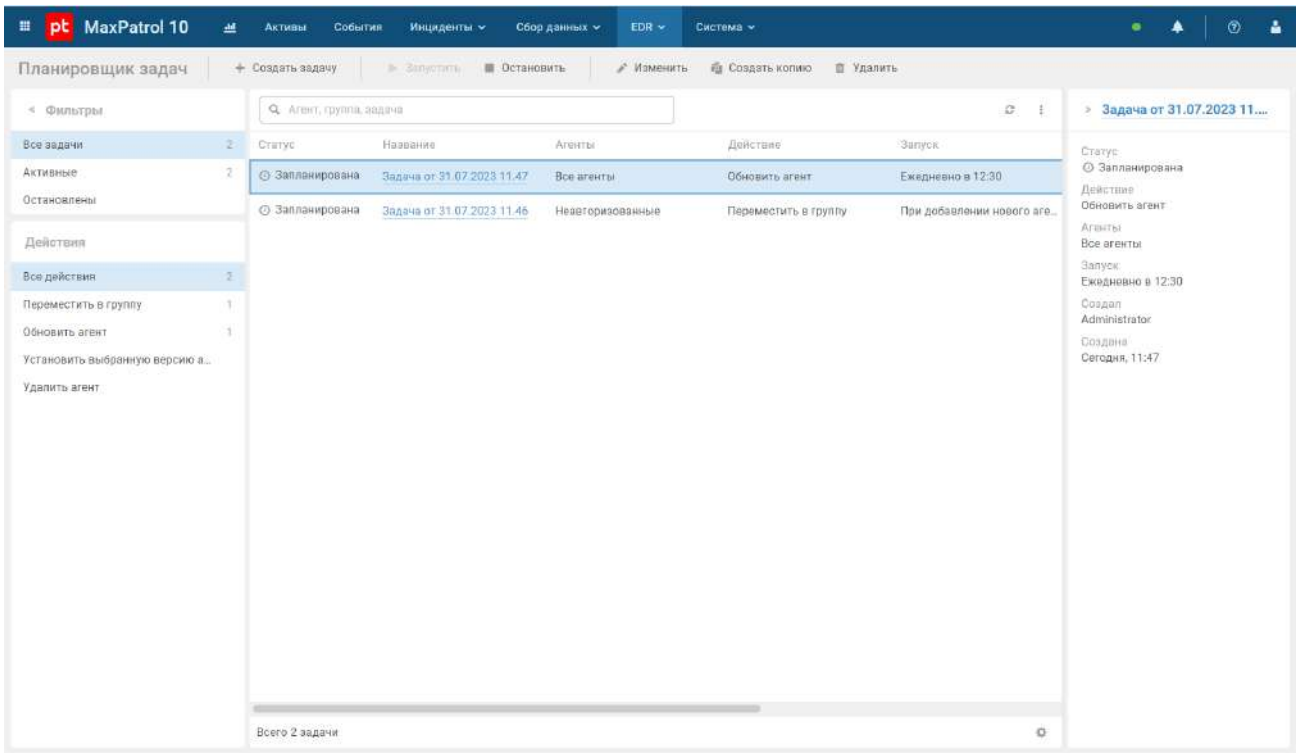

Рисунок 21. Страница **Планировщик задач**

Если задача не была выполнена при последнем запуске, то в столбце **Результатов** будет отображаться значок ⚠. Если задача выполнилась, но были ошибки — ⚠.

21.2.2. Создание задачи

- Чтобы создать задачу:

  1. В главном меню в разделе **EDR** выберите пункт **Управление** → **Планировщик задач с агентами**.

     Откроется страница **Планировщик задач**.

  2. Нажмите кнопку **Создать задачу**.

     Откроется окно **Новая задача**.

  3. В поле **Название** введите название задачи.
  4. В блоке параметров **Запуск** выберите, когда нужно запускать задачу.
  5. В раскрывающемся списке **Агенты** выберите, для каких агентов будет выполняться задача.
  6. Если на предыдущем шаге вы выбрали пункт **Из выбранных групп**, в раскрывающемся списке **Группы** выберите группы, для агентов которых будет выполняться задача.
  7. В поле **Дополнительное условие на языке PDQL** введите дополнительное условие выполнения задачи на языке PDQL (см. раздел 21.2.3).
  8. В раскрывающемся списке **Действие** выберите действие, которое необходимо выполнять с агентами.
  9. Если вы выбрали действие **Установить выбранную версию агента**, в раскрывающемся списке **Версия агента** выберите версию агента, которую нужно установить.
  10. Если вы выбрали действие **Переместить в группу**, в раскрывающемся списке **Куда** выберите группу, в которую нужно переместить агенты.
  11. Нажмите кнопку **Создать**.

  Задача создана.

21.2.3. Синтаксис языка PDQL для фильтрации агентов

Вы можете задавать дополнительную фильтрацию агентов при создании задач на языке запросов Positive Data Query Language (PDQL). Язык PDQL разработан в Positive Technologies для написания запросов в процессе обработки событий, инцидентов, динамических групп активов и табличных списков в MaxPatrol SIEM. Подробная информация приведена в Справочнике по языку запросов PDQL из комплекта поставки MaxPatrol SIEM.

Для фильтрации агентов при создании задачи вы можете использовать базовые операторы: `=`, `!=`, `<`, `<=`, `>`, `>=`, `IN`, `NOT IN`, `MATCH`, `NOT MATCH`, `LIKE`, `NOT LIKE`, `CONTAINS`, `INTERSECT`, `NOT`. Параметры агентов, по которым вы можете их фильтровать, приведены в таблице.

Примечание. Не все операторы совместимы со всеми параметрами. Например, операторы <, <=, >, >= вы можете использовать только с параметром `Agent.ConnectedDate`.

Таблица 12. Параметры агентов

Параметр	Описание	Примеры

`Agent.Ips`	Сетевые протоколы	`Agent.Ips intersect [::1/128, 127.0.0.1/8]`
		`Agent.Ips contains ::1/128`
		`Agent.Ips like '%fe80::1/64%'`

`Agent.Tags`	Метки	`Agent.Tags = 'localhost'`
		`Agent.Tags like '%local%'`
		`Agent.Tags contains 'host'`

`Agent.UserNames`	Имя пользователя, зарегистрированного в операционной системе конечного устройства	`Agent.UserNames = 'Administrator'` `Agent.UserNames like '%Admin%'`
`Agent.UserGroups`	Группа пользователя	`Agent.UserGroups contains 'root'` `Agent.UserGroups intersect ['root', 'admins']`
`Agent.ConnectedDate`	Дата и время последнего подключения к серверу	`Agent.ConnectedDate > 2022-08-29T08:00` `Agent.ConnectedDate = 2022-08-29T03:27:17`
`Agent.AuthStatus`	Статус авторизации	`Agent.AuthStatus in ['authorized', 'blocked']` `Agent.AuthStatus = ' unauthorized '`
`Agent.Description`	Название	`Agent.Description = 'test'`
`Agent.Hostname`	Имя конечного устройства	`Agent.Hostname like '%edr%'` `Agent.Hostname = 'server'`
`Agent.Ip`	IP-адрес	`Agent.Ip not like '%127%'` `Agent.Ip != 127.0.0.1`
`Agent.OsArch`	Архитектура операционной системы	`Agent.OsArch in ['amd64', '386']`

Параметр	Описание	Примеры
		`not (Agent.OsArch = 'amd64')`
`Agent.OsName`	Имя операционной системы	`Agent.OsName in ['Debian GNU/Linux 11', 'Microsoft Windows 10.0']` `Agent.OsName match '^Deb+'`
`Agent.OsType`	Тип операционной системы	`Agent.OsType in ['linux', 'windows']` `not (Agent.OsType = 'linux')`
`Agent.Status`	Подключен или отключен	`Agent.Status = 'connected'` `Agent.Status = 'disconnected'`
`Agent.Version`	Версия	`Agent.Version like '%1.0.%'`

21.2.4. Запуск и остановка задачи

После создания задача запускается автоматически. Если выполнение задачи сейчас не требуется, вы можете ее остановить.

- Чтобы остановить задачу:

  1. В главном меню в разделе **EDR** выберите пункт **Управление** → **Планировщик задач с агентами**.

     Откроется страница **Планировщик задач**.

  2. Выберите задачу со статусом **Запланирована** или **Выполняется**.
  3. Нажмите кнопку **Остановить**.

  Задача остановлена.

- Чтобы запустить остановленную задачу:

  1. В главном меню в разделе **EDR** выберите пункт **Управление** → **Планировщик задач с агентами**.

     Откроется страница **Планировщик задач**.

  2. Выберите задачу со статусом **Остановлена**.
  3. Нажмите кнопку **Запустить**.

  Задача запущена.

21.2.5. Просмотр результатов задачи

- Чтобы просмотреть результаты выполнения задачи:

  1. В главном меню в разделе **EDR** выберите пункт **Управление** → **Планировщик задач с агентами**.

     Откроется страница **Планировщик задач**.

  2. Нажмите на название задачи.

     Отобразится список результатов задачи.

21.2.6. Копирование задачи

Вы можете создавать новые задачи на основе имеющихся. Это полезно в тех случаях, когда нужно незначительно изменить параметры задачи.

- Чтобы скопировать задачу:

  1. В главном меню в разделе **EDR** выберите пункт **Управление** → **Планировщик задач с агентами**.

     Откроется страница **Планировщик задач**.

  2. Выберите задачу.
  3. Нажмите кнопку **Создать копию**.

     Откроется окно **Копия задачи**.

  4. Измените параметры задачи.
  5. Нажмите кнопку **Создать**.

  Задача скопирована.

21.2.7. Изменение параметров задачи

Перед изменением задачи вам нужно ее остановить (см. раздел 21.2.4).

- Чтобы изменить параметры задачи:

  1. В главном меню в разделе **EDR** выберите пункт **Управление** → **Планировщик задач с агентами**.

     Откроется страница **Планировщик задач**.

  2. Выберите задачу.
  3. Нажмите кнопку **Изменить**.

4. Измените параметры задачи.
5. Нажмите кнопку **Сохранить**.

Параметры задачи изменены.

21.2.8. Удаление задачи

Вы можете удалить задачу. После этого данные о ее результатах будут недоступны.

- Чтобы удалить задачу:

  1. В главном меню в разделе **EDR** выберите пункт **Управление** → **Планировщик задач с агентами**.

     Откроется страница **Планировщик задач**.
  2. Выберите задачу.
  3. Нажмите кнопку **Удалить** и подтвердите удаление.

  Задача удалена.

21.3. Мониторинг состояния MaxPatrol EDR

Вы можете отслеживать работу сервера MaxPatrol EDR, агентов, модулей и внутренних компонентов, анализируя специальные метрики и данные трассировки. Для мониторинга состояния MaxPatrol EDR вместе с продуктом устанавливаются следующие сервисы:

— OpenTelemetry — для передачи данных трассировки с агента на сервер MaxPatrol EDR;

— Jaeger — для работы с данными трассировки;

— Elasticsearch — для хранения данных трассировки;

— VictoriaMetrics — для хранения метрик;

— Grafana — для визуализации, мониторинга и анализа метрик и данных трассировки;

— Grafana Loki — для хранения и просмотра журналов.

Рисунок 22. Мониторинг MaxPatrol EDR в Grafana

В этом разделе

21.3.1. Просмотр записей в системном журнале

Вы можете просмотреть записи о работе системы с помощью сервиса Grafana Loki.

► Чтобы просмотреть записи в системном журнале:

1. Войдите в веб-интерфейс Grafana.

   Примечание. Подробные инструкции по работе с Grafana приведены на сайте вендора.

2. В панели слева нажмите  .

   Откроется страница **Explore**.

3. В раскрывающемся списке сверху выберите источник данных **Loki**.

4. Выберите режим редактирования запроса **Code**.
5. Нажмите кнопку **Log browser**.
6. В блоке параметров **Select labels to search in** выберите метки, по которым нужно искать записи в журнале.
7. В блоке параметров **Find values for the selected labels** укажите значения выбранных меток.

   Например, для поиска записей об ошибках в работе какого-либо модуля на агенте вы можете выбрать идентификатор агента, модуль и уровень записи **ERROR** с помощью меток **agent_id**, **component** и **level**.
8. Нажмите кнопку **Show logs**.

   Отобразятся записи из системного журнала, подходящие под условия запроса.

21.3.2. Поиск и просмотр данных об ошибках агента

- Чтобы просмотреть данные об ошибках агента:

1. Войдите в веб-интерфейс Grafana.

   Примечание. Подробные инструкции по работе с Grafana приведены на сайте вендора.
2. В панели слева нажмите  .

   Откроется страница **Explore**.
3. В раскрывающемся списке сверху выберите источник данных **Jaeger**.
4. Выберите тип запроса **Search**.
5. В раскрывающемся списке **Service** выберите компонент **vxagent**.
6. Выполните одно из следующих действий:

   Если вы хотите отобразить ошибки всех агентов, в поле **Tags** введите `error=true`.

   Если вы хотите отобразить ошибки конкретного агента, в поле **Tags** введите `error=true agent_id="<Идентификатор агента>"`.
7. Нажмите кнопку **Run query**.

   Отобразится таблица данных трассировки.
8. Выберите запись о трассировке.

   Справа откроется панель с данными об ошибке.

21.3.3. Поиск и просмотр данных об ошибках сервера агентов

- Чтобы просмотреть данные об ошибках сервера агентов:

  1. Войдите в веб-интерфейс Grafana.

     Примечание. Подробные инструкции по работе с Grafana приведены на сайте вендора.

  2. В панели слева нажмите  .

     Откроется страница **Explore**.

  3. В раскрывающемся списке сверху выберите источник данных **Jaeger**.
  4. Выберите тип запроса **Search**.
  5. В раскрывающемся списке **Service** выберите компонент **vxserver**.
  6. В поле **Tags** введите `error=true`.
  7. Нажмите кнопку **Run query**.

     Отобразится таблица данных трассировки.

  8. Выберите запись о трассировке.

     Справа откроется панель с данными об ошибке.

21.3.4. Поиск и просмотр данных об ошибках модуля

- Чтобы просмотреть данные об ошибках модуля:

  1. Войдите в веб-интерфейс Grafana.

     Примечание. Подробные инструкции по работе с Grafana приведены на сайте вендора.

  2. В панели слева нажмите  .

     Откроется страница **Explore**.

  3. В раскрывающемся списке сверху выберите источник данных **Jaeger**.
  4. Выберите тип запроса **Search**.
  5. В раскрывающемся списке **Service** выберите компонент **vxagent**.
  6. Выполните одно из следующих действий:

     Если вы хотите отобразить ошибки модуля со всех агентов, в поле **Tags** введите `error=true log.module="<Идентификатор модуля>"`.

     Если вы хотите отобразить ошибки модуля с конкретного агента, в поле **Tags** введите `error=true log.module="<Идентификатор модуля>" agent_id="<Идентификатор агента>"`.

7. Нажмите кнопку **Run query**.

   Отобразится таблица данных трассировки.

8. Выберите запись о трассировке.

   Справа откроется панель с данными об ошибке.

21.3.5. Работа с дашбордами

Дашборд в Grafana — это страница, на которой отображаются панели с графиками, диаграммами и прочей статистической информацией о работе продукта и операционной системы.

При установке MaxPatrol EDR в Grafana добавляются несколько стандартных дашбордов для мониторинга состояния продукта.

- Чтобы открыть дашборд:

  1. Войдите в веб-интерфейс Grafana.

     Примечание. Подробные инструкции по работе с Grafana приведены на сайте вендора.

  2. В левом верхнем углу нажмите кнопку **General / Home**.

     Откроется страница со списком папок и дашбордов по компонентам продукта.

  3. Выберите дашборд.

     Откроется страница с дашбордом.

21.3.6. Построение графика метрики

Вы можете анализировать метрики в Grafana на графиках.

- Чтобы построить график метрики:

  1. Войдите в веб-интерфейс Grafana.

     Примечание. Подробные инструкции по работе с Grafana приведены на сайте вендора.

  2. В панели слева нажмите  .

     Откроется страница **Explore**.

  3. В раскрывающемся списке сверху выберите источник данных **VictoriaMetrics**.

  4. В поле **Metrics browser** введите метрику или выберите ее в списке.

  5. Нажмите кнопку **Run query**.

     Отобразится график метрики.

21.4. Настройка отображения данных в MaxPatrol EDR

Для удобства поиска и просмотра информации об агентах, политиках, группах и зависимостях в MaxPatrol EDR вы можете фильтровать данные, а также настраивать их отображение в таблицах.

В этом разделе

Фильтрация данных в таблицах (см. раздел 21.4.1)

Настройка таблиц с данными (см. раздел 21.4.2)

Обновление данных в таблицах (см. раздел 21.4.3)

21.4.1. Фильтрация данных в таблицах

В этом разделе приведена инструкция по фильтрации данных в таблице агентов на странице **Агенты EDR**. Фильтрация в таблицах на других страницах выполняется таким же способом.

► Чтобы отфильтровать агенты:

1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

   Откроется страница **Агенты EDR**.

2. В правом верхнем углу списка агентов нажмите .

   Появится строка с названиями фильтров.

3. Выберите значения фильтров.

   Примечание. Вы можете очистить значения всех фильтров, нажав в строке фильтрации.

Агенты отфильтрованы.

21.4.2. Настройка таблиц с данными

Вы можете настраивать отображение данных в таблицах:

— сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки);

— изменять ширину столбцов;

— изменять порядок следования столбцов, перемещая заголовок столбца;

— изменять набор столбцов.

Далее в разделе приведена инструкция по настройке набора столбцов для таблицы агентов на странице **Агенты EDR**. Настройка столбцов в других таблицах выполняется таким же способом.

► Чтобы настроить набор столбцов в таблице:

1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

   Откроется страница **Агенты EDR**.

2. Нажмите ⚙ в нижней части страницы.
3. Во всплывающем окне выберите столбцы.
4. Нажмите кнопку **Применить**.

Набор столбцов настроен.

21.4.3. Обновление данных в таблицах

В этом разделе приведена инструкция по обновлению данных в таблице агентов на странице **Агенты EDR**. Обновление данных в таблицах на других страницах выполняется таким же способом.

► Чтобы обновить данные:

1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

   Откроется страница **Агенты EDR**.

2. Выберите вариант обновления данных:

   - Если вы хотите обновить данные вручную, нажмите ↻.
   - Если вы хотите, чтобы данные обновлялись автоматически, нажмите ⋮, установите флажок **Автоматически обновлять** и выберите период обновления.

21.5. Экспорт данных в файл формата CSV

Вы можете экспортировать данные об агентах, группах агентов, политиках и модулях в файл формата CSV. Далее в разделе приведена инструкция по экспорту данных об агентах. Экспорт данных из других таблиц выполняется таким же способом.

► Чтобы экспортировать данные в файл формата CSV:

1. В главном меню в разделе **EDR** выберите пункт **Агенты**.

   Откроется страница **Агенты EDR**.

2. Если требуется, отфильтруйте агенты в таблице (см. раздел 21.4.1) и выберите столбцы для отображения (см. раздел 21.4.2).

   Примечание. В CSV-файл будут экспортированы только те данные, которые отображаются в таблице.

3. Если вы хотите экспортировать данные только о некоторых агентах, выберите их в таблице, удерживая клавишу Ctrl или Shift.
4. Нажмите .
5. В открывшемся окне выберите, какие данные вы хотите экспортировать — только выбранные или все.

Файл сохранен на вашем компьютере.

21.6. Замена SSL-сертификата

SSL-сертификат нужен для того, чтобы пользователи MaxPatrol EDR имели доступ к веб-интерфейсу продукта через HTTPS-соединение. При установке продукта генерируется уникальный сертификат Positive Technologies. При необходимости вы можете заменить этот сертификат на собственный, например корпоративный. Он должен отвечать следующим требованиям:

— иметь формат PEM;

— использовать алгоритм подписи SHA-256;

— использовать алгоритм шифрования ключей RSA;

— иметь длину закрытого ключа не менее 2048 бит;

— включать область применения сертификата Digital Signature или Key Encipherment;

Перед выполнением инструкции вам нужно загрузить на узел с установленным управляющим сервером файл SSL-сертификата открытого ключа и файл закрытого ключа, идущего с ним в паре. Если у вас есть промежуточные сертификаты, которые нужно использовать, они должны быть сохранены в одном файле вместе с сертификатом открытого ключа (записаны после него).

► Чтобы заменить SSL-сертификат:

1. Перейдите в каталог, в котором хранятся файлы вашего сертификата.

   Например:

   ```
   cd /home/username/cert
   ```

2. Переименуйте файлы вашего сертификата:

   ```
   cp <Название файла сертификата открытого ключа> server.crt
   cp <Названия файла закрытого ключа> server.key
   ```

   Например:

   ```
   cp example_com.pem server.crt
   cp example_com.key server.key
   ```

   Примечание. Файл `server.key` не должен быть защищен паролем.

3. Создайте резервную копию сертификата Positive Technologies:

   ```
   tar cvzf <Название архива с создаваемой резервной копией> /var/lib/docker/volumes/
   edr_vxui-server-ssl/_data
   ```

   Например:

   ```
   tar cvzf backup.tar.gz /var/lib/docker/volumes/edr_vxui-server-ssl/_data
   ```

4. Скопируйте файлы вашего сертификата в хранилище сертификатов:

   ```
   cp server.* /var/lib/docker/volumes/edr_vxui-server-ssl/_data
   ```

5. Настройте права доступа к файлам сертификата:

   ```
   chmod g+r server.crt
   chmod g+r server.key
   ```

6. Перезапустите управляющий сервер:

   ```
   docker restart vx_edr_ui
   ```

   SSL-сертификат заменен.

Вы можете проверить работоспособность нового сертификата, открыв веб-интерфейс MaxPatrol EDR. В адресной строке браузера, слева от адреса, должен появиться значок .

22. Решение проблем

Этот раздел содержит информацию для решения проблем при работе с MaxPatrol EDR.

В этом разделе

22.1. Автоматическая деавторизация агента

Проблема

Авторизованный ранее агент отображается в веб-интерфейсе со статусом **Не авторизован**.

Возможные причины

Агент при подключении к серверу агентов MaxPatrol EDR не прошел проверку безопасности.

Решение

- Чтобы решить проблему:

  1. Найдите причину сбоя в журнале агента или в журнале сервера агентов MaxPatrol EDR. Файлы журналов расположены в каталогах с исполняемыми файлами.
  2. Исходя из описания ошибки, самостоятельно устраните причину или обратитесь в службу технической поддержки Positive Technologies.
  3. Повторно авторизуйте агент (см. раздел 16.3).

22.2. Автоматическая блокировка агента

Проблема

Авторизованный ранее агент отображается в веб-интерфейсе со статусом **Заблокирован**.

Возможные причины

Агент при подключении к серверу агентов MaxPatrol EDR не прошел проверку безопасности.

Решение

- Чтобы решить проблему:

  1. Найдите причину сбоя в журнале агента или в журнале сервера агентов MaxPatrol EDR. Файлы журналов расположены в каталогах с исполняемыми файлами.
  2. Исходя из описания ошибки, самостоятельно устраните причину или обратитесь в службу технической поддержки Positive Technologies.
  3. Разблокируйте агент, добавив его в группу (см. раздел 17.7).

22.3. Не открывается карточка модуля

Проблема

В браузере Google Chrome не открывается карточка модуля.

Возможные причины

Расширение Kaspersky Protection блокирует необходимые компоненты.

Решение

- Чтобы решить проблему,

  добавьте адрес сервера MaxPatrol EDR в список сайтов с разрешенными баннерами в параметрах «Анти-Баннера».

22.4. Обновление завершилось с ошибкой

Проблема

Обновление MaxPatrol EDR прошло неуспешно.

Возможные причины

Ошибка программы установки.

Решение

- Чтобы решить проблему:

  1. Удалите MaxPatrol EDR с сохранением конфигурации с помощью команды `edr-clean`.
  2. Установите новую версию MaxPatrol EDR.

22.5. Удаление MaxPatrol EDR завершилось с ошибкой

Проблема

Удаление MaxPatrol EDR в двухсерверной конфигурации завершилось с ошибкой **Not found the inventory file**.

Возможные причины

На сервере, с которого выполнялась установка MaxPatrol EDR, был удален инвентарный файл Ansible.

Решение

- Чтобы решить проблему:

  1. На сервере, с которого выполнялась установка, выполните команду `sudo /opt/edr/edr_installer --only-create-inventory`.
  2. Для удаления MaxPatrol EDR выполните команду `edr-purge`.

22.6. Не удается добавить модуль в политику или создать новый объект в системе

Проблема

При добавлении модуля в политику появляется ошибка **Не удалось включить модуль**, при создании новой политики или группы — **Не удалось создать <Тип объекта>**.

Возможные причины

Закончилось свободное место на сервере MaxPatrol EDR.

Решение

- Чтобы решить проблему:

  1. Проверьте свободное место на сервере MaxPatrol EDR:
     ```
     sudo df -h
     ```
  2. Если свободное место закончилось, проверьте размер журналов контейнеров:
     ```
     sudo du -sh /var/lib/docker/containers/
     ```
  3. Если размер журналов превышает 1 ГБ, в каталоге `/etc/docker/` создайте файл `daemon.json` со следующим содержимым:
     ```
     {
     "log-driver": "json-file",
     "log-opts": {
     "max-size": "250m",
     "max-file": "3"
      }
     }
     ```
  4. Перезапустите контейнеры и сервер MaxPatrol EDR:
     ```
     sudo systemctl daemon-reload
     sudo systemctl restart docker
     edr-stop
     edr-start
     ```
  5. Дополнительно освободите место на диске или увеличьте его размер.
  6. Повторно добавьте модуль в политику или создайте новую политику или группу.
  7. Если ошибка сохраняется, обратитесь в службу технической поддержки Positive Technologies и предоставьте записи из журнала Docker Compose:
     ```
     sudo docker-compose -f /opt/edr/docker-compose.yml logs -f vxapi
     ```

22.7. Установленный агент не отображается в веб-интерфейсе MaxPatrol EDR

Проблема

После установки агент не отображается в веб-интерфейсе MaxPatrol EDR, в журнале установки сообщение:

```
level=error msg="an unexpected error occurred while reading messages"
component=reader_messages error="failed to get connection reader: websocket: close
1000 (normal)" step="connection initialization"
```

Возможные причины

Версия агента несовместима с версией сервера MaxPatrol EDR.

Решение

- Чтобы решить проблему:

  1. Перейдите в веб-интерфейс MaxPatrol EDR.
  2. В главном меню в разделе **EDR** выберите пункт **Управление** → **Дистрибутивы агентов**.

     Откроется страница **Дистрибутивы агентов**.
  3. Скачайте подходящий дистрибутив агента и установите его (см. раздел 16.2).

22.8. Ошибка подключения агентов после переустановки сервера агентов

Проблема

После полной переустановки сервера агентов MaxPatrol EDR (включая операционную систему) ранее подключенные агенты не могут подключиться к серверу, в журнале агентов сообщение:

```
level=info msg="connection to the server has not been initialized yet, trying to init
connection" error="failed to get the connection config: failed to get the TLS config
for the client connection: failed to get the LTAC certificate: failed to get the LTAC
certificate for connection (failed to call the Lua function GetLTAC: script exited
with an error: SSA blob has not been initialized (secure store has not been
initialized)): failed to connect to the server: a connection initialization required"
time="2023-04-20T11:30:32+03:00" level=error msg="an unexpected error occurred while
reading messages" component=reader_messages error="failed to get connection reader:
websocket: close 1000 (normal)" step="connection initialization"
time="2023-04-20T11:30:32+03:00" level=warning msg="vxagent: try reconnect"
error="init connection failed: failed to initialize connection: connection
initialization failed: failed to perform the initial connection: failed to connect to
the server: a connection initialization required (failed to read an init connect
response: read channel is closed)"
```

Возможные причины

Агенты при подключении к серверу агентов MaxPatrol EDR не прошли проверку безопасности.

Решение

- Чтобы решить проблему:

  1. Повторно авторизуйте агенты (см. раздел 16.3).
  2. Если ранее установленные агенты не отображаются в веб-интерфейсе MaxPatrol EDR, переустановите их (см. раздел 16.2).

Примечание. Агенты могут не отображаться в веб-интерфейсе, если их версия несовместима с версией сервера MaxPatrol EDR.

22.9. Внутренняя ошибка модуля «Сбор данных из файлов журналов» после добавления в политику

Проблема

После добавления модуля «Сбор данных из файлов журналов» в политику появляется ошибка **Внутренняя ошибка в модуле**, в поле `reason` указано `unexpected exit from worker`.

Возможные причины

На сервере MaxPatrol EDR установлена старая версия OpenSSL.

Решение

- Чтобы решить проблему,

  на сервере MaxPatrol EDR установите OpenSSL версии 1.1.1f или выше.

23. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

23.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

23.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

23.3. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

23.3.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста Positive Technologies нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

23.3.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист Positive Technologies оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

Positive Technologies поставляет пакеты обновления в течение срока обновления, указанного в лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, Positive Technologies обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

23.3.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 13).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 13. Время реакции на запрос и время его обработки

Уровень значимости запроса	**Критерии значимости запроса**	**Время реакции на запрос**	**Время обработки запроса**
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

23.3.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

- о диагностике проблемы и ее результатах;
- о поиске решения или возможности обойти причины возникновения проблемы;
- о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

- предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;
- проблема классифицирована как неподдерживаемая.

Приложение A. Псевдонимы команд для работы с MaxPatrol EDR

В таблице ниже приведен список псевдонимов команд для работы с MaxPatrol EDR, определенных в операционной системе сервера.

Таблица 14. Псевдонимы команд

Псевдоним команды	Описание
`edr-compose`	Определение и запуск контейнеров MaxPatrol EDR. Аналог команды `sudo /opt/edr/bin/docker-compose -f /opt/edr/docker-compose.yml_edr_lastUp`
`edr-clean`	Удаление службы MaxPatrol EDR. Аналог команды `sudo /opt/edr/edr_installer --clean`
`edr-purge`	Полное удаление MaxPatrol EDR. Аналог команды `sudo /opt/edr/edr_installer --purge`
`edr-ps`	Просмотр статуса компонентов MaxPatrol EDR. Аналог команды `edr-compose ps`
`edr-logs`	Просмотр журнала MaxPatrol EDR. Аналог команды `edr-compose logs`
`edr-start`	Запуск службы MaxPatrol EDR. Аналог команды `sudo systemctl start edr`
`edr-stop`	Остановка службы MaxPatrol EDR. Аналог команды `sudo systemctl stop edr`
`edr-status`	Проверка статуса службы MaxPatrol EDR. Аналог команды `sudo systemctl status edr`
`edr-version`	Просмотр компонентов MaxPatrol EDR и их версий. Аналог команды `sudo bash /opt/edr/get_versions.sh`
`edr-update`	Обновление пакета экспертизы и скачивание архива с установочным комплектом новой версии MaxPatrol EDR. Аналог команды `sudo /opt/edr/check_updates.sh`

Приложение Б. Параметры модулей агентов

Таблица 15. Параметры модулей агентов

Параметр или блок параметров	Описание
«Завершение процессов»	
Список исключений	Список исполняемых файлов процессов, которые не будут завершаться модулем
«Изоляция узлов»	
Исключения	Параметры сетевого трафика, который не будет блокироваться модулем. Добавлять в исключения сервер MaxPatrol EDR не требуется: обмен данных с ним не будет блокироваться
«Отправка событий на syslog-сервер»	
Адрес syslog-сервера	Адрес syslog-сервера, на который вы хотите отправлять события
«Проверка файлов в PT Sandbox»	
Ключ API	Ключ для доступа к публичному API PT Sandbox. Для генерации ключа API вам нужно выполнить команду `sudo ptmsctl api auth create <Название ключа API>` в консольной утилите PT Sandbox
Глубина распаковки архивов	Максимальное количество вложенных друг в друга архивов, которые будут распаковываться при проверке. Увеличение глубины распаковки архивов снижает скорость проверки. Если распаковывать архивы не требуется, вы можете ввести `0`, тогда архивы будут проверяться как обычные файлы
Продолжительность наблюдения за файлом	Максимальное время наблюдения за файлом в ОС в секундах
Максимальный размер файла	Максимальный размер файла, который вы можете отправить на проверку в PT Sandbox
Классы вредоносного ПО	Список классов вредоносного ПО, при обнаружении которых PT Sandbox вынесет вердикт «вредоносный файл». При обнаружении вредоносного ПО, относящегося к другому классу, будет вынесен вердикт «безопасный файл». Не рекомендуется изменять стандартный список классов
Адрес сервера	Адрес сервера PT Sandbox
«Отправка файлов»	
Максимальный размер файла, МБ	Максимальный размер файла, который вы можете отправить во внешнюю систему

Параметр или блок параметров	Описание
Адрес внешней системы и метод HTTP-запроса	Адрес внешней системы и метод HTTP-запроса, с помощью которого будут отправляться файлы
Список заголовков запроса	Заголовки запроса, которые будут добавляться к HTTP-запросам
«Установщик Sysmon»	
Заменить исполняемый файл Sysmon на агенте	Определяет, заменять ли исполняемый файл, если Sysmon уже установлен на конечном устройстве
Заменить файл конфигурации на агенте	Определяет, заменять ли файл конфигурации, если Sysmon уже установлен на конечном устройстве
Файл конфигурации	Файл конфигурации Sysmon, который будет использоваться на конечном устройстве
«Драйвер сбора данных и реагирования»	
Имя для файлов журнала действий	Имя для файлов, в которых будут содержаться записи о действиях, выполненных драйвером
Имя для файлов журнала событий	Имя для файлов, в которых будут содержаться записи о полученных драйвером событиях
Хранить файлы журналов	Определяет, хранить ли файлы журналов на конечном устройстве
Время хранения файлов журналов (в днях)	Время хранения файлов журналов на конечном устройстве (в днях)
Конфигурация драйвера	Конфигурация драйвера в формате JSON
Модули, получающие необработанные события	Список идентификаторов модулей, которые будут получать данные
«YARA-сканер»	
Список исключений для проверок в Linux	Список файлов и каталогов, которые не будут проверяться модулем в Linux
Список исключений для проверок в Windows	Список файлов и папок, которые не будут проверяться модулем в Windows
Список исключений для YARA-правил	Список идентификаторов YARA-правил, которые не будут использоваться для проверок

Параметр или блок параметров	Описание
Параметры быстрой проверки файлов в Linux	Список файлов и каталогов для быстрой проверки в Linux
Параметры быстрой проверки файлов в Windows	Список файлов и папок для быстрой проверки в Windows
Параметры быстрой проверки процессов в Linux	Список процессов для быстрой проверки в Linux
Параметры быстрой проверки процессов в Windows	Список процессов для быстрой проверки в Windows
Классы вредоносного ПО	Список классов вредоносного ПО, при обнаружении которых модуль вынесет вердикт «вредоносный файл». Не рекомендуется изменять стандартный список классов
Время хранения результатов сканирования процесса (в минутах)	Время хранения результатов сканирования процесса (в минутах). При перезагрузке модуля результаты сканирования очищаются
«WinEventLog: сбор данных из журнала событий Windows»	
Каналы журналов	Список каналов журнала событий Windows, которые будут обрабатываться модулем
«Сбор данных из файлов журналов»	
Файлы журналов	Список файлов журналов, которые будут обрабатываться модулем. Поддерживаются файлы журналов из Linux и Windows
«Сканирование в режиме аудита (MaxPatrol VM)»	
Запуск	Периодичность запуска сканирования по расписанию
День недели	Дни недели, в которые будет запускаться сканирование по расписанию
Месяцы	Месяцы, в которые будет запускаться сканирование по расписанию
День месяца	Дни месяца, в которые будет запускаться сканирование по расписанию
Время в часовом поясе агента	Время в часовом поясе агента, в которое будет запускаться сканирование по расписанию

Параметр или блок параметров	Описание
Макс. загрузка ЦП	Доля загрузки процессора конечного устройства, при которой сканирование будет отложено. Модуль учитывает среднюю загрузку за последние 100 секунд. Параметр учитывается только при автоматическом запуске сканирования
Ждать не более	Максимальное время в часах, на которое модуль будет откладывать сканирование из-за превышения заданной загрузки процессора. Параметр учитывается только при автоматическом запуске сканирования
Пауза между повторными сканированиями	Время после успешного окончания сканирования, в течение которого не будет запускаться новое сканирование. Параметр учитывается только при автоматическом запуске сканирования
«Блокировка по IP-адресу»	
Заблокированные IP-адреса	Список заблокированных IP-адресов через пробел, запятую, точку с запятой или с новой строки
«Перенаправление DNS-запросов (sinkholing)»	
IP-адрес, на который перенаправлять трафик	IP-адрес, на который следует перенаправлять трафик. Это может быть специальный сервер, на котором входящие данные будут анализироваться, или неиспользуемый внутренний IP-адрес для блокировки трафика, например `0.0.0.0`
Префиксы доменных имен	Один или несколько префиксов, которые будут добавляться к доменным именам
Домены, с которых перенаправлять трафик	Один или несколько доменов, трафик с которых будет перенаправляться

Глоссарий

агент EDR

Приложение, которое устанавливается на конечном устройстве для обеспечения работы модулей и связи с сервером агентов.

группа агентов EDR

Один или несколько агентов EDR, объединенных по определенному принципу для назначения им одних и тех же политик.

действие модуля

Операция, которую модуль выполняет на конечном устройстве. Запуск операции может выполняться по команде пользователя или автоматически при регистрации того или иного события ИБ.

зависимость

Условие, которое должно выполняться для корректной работы модуля агента.

конечное устройство

Оборудование, имеющее ценность для организации и подлежащее защите от киберугроз.

модуль агента

Приложение, которое запускается на агенте для выполнения основных функций продукта. Есть пять типов модулей: модули доставки и установки, сбора, интеграции, обнаружения, реагирования.

модуль доставки и установки

Модуль агента, который устанавливает и настраивает приложения, а также управляет конфигурацией ОС на конечном устройстве.

модуль обнаружения

Модуль агента, который анализирует собранные события, обнаруживает подозрительную и вредоносную активность на конечном устройстве — и регистрирует события ИБ.

модуль реагирования

Модуль агента, который пресекает подозрительную и вредоносную активность на конечном устройстве, выполняя действия в соответствии с политикой модуля обнаружения.

модуль сбора

Модуль агента, который собирает данные о событиях на конечном устройстве и передает их в модули обнаружения и в SIEM-системы.

поведенческий анализ

Технология выявления атак и киберугроз, основанная на анализе поведения файлов, приложений и пользователя в информационной системе.

политика конфигурации модулей агентов

Механизм управления поставкой модулей агентов в заданной конфигурации на конечные устройства. Политика состоит из перечня модулей и описания их конфигурации, который назначается группе агентов.

приоритет действия

Условная величина, которая определяет порядок выполнения действий при регистрации того или иного события ИБ.

сервер агентов

Серверное приложение, предназначенное для управления агентами и модулями.

управляющий сервер

Серверное приложение, предназначенное для управления конфигурацией системы.

positive
technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 170 тысяч акционеров.