MaxPatrol EDR версия 8.0

Руководство администратора

Дата редакции документа: 18.06.2025

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.

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

- удалить файл;
- завершить один или несколько процессов;
- заблокировать сетевой трафик;
- заблокировать учетную запись;
- запустить проверку файлов и процессов на основе YARA-правил;
- отправить файл на проверку в PT Sandbox;
- запустить сканирование в режиме аудита и отправить результаты в MaxPatrol VM;
- заблокировать все сетевые соединения по IP-адресу;
- перенаправить DNS-запросы на IP-адрес;
- изолировать файл в зашифрованном хранилище;
- 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 17.1).
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.
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 22.3) на сервер агентов.
9. Управляющий сервер получает обновления продукта и пакетов экспертизы с сервера обновлений.

Взаимодействие компонентов

При обычной установке управляющий сервер в системе один, а серверов агентов может быть несколько. При установке в отказоустойчивом кластере компонент `api` управляющего сервера может быть установлен на нескольких серверах (см. раздел 6.7). Компоненты Observability (см. раздел 22.3) для снижения сетевого трафика могут быть установлены на одних серверах с серверами агентов.

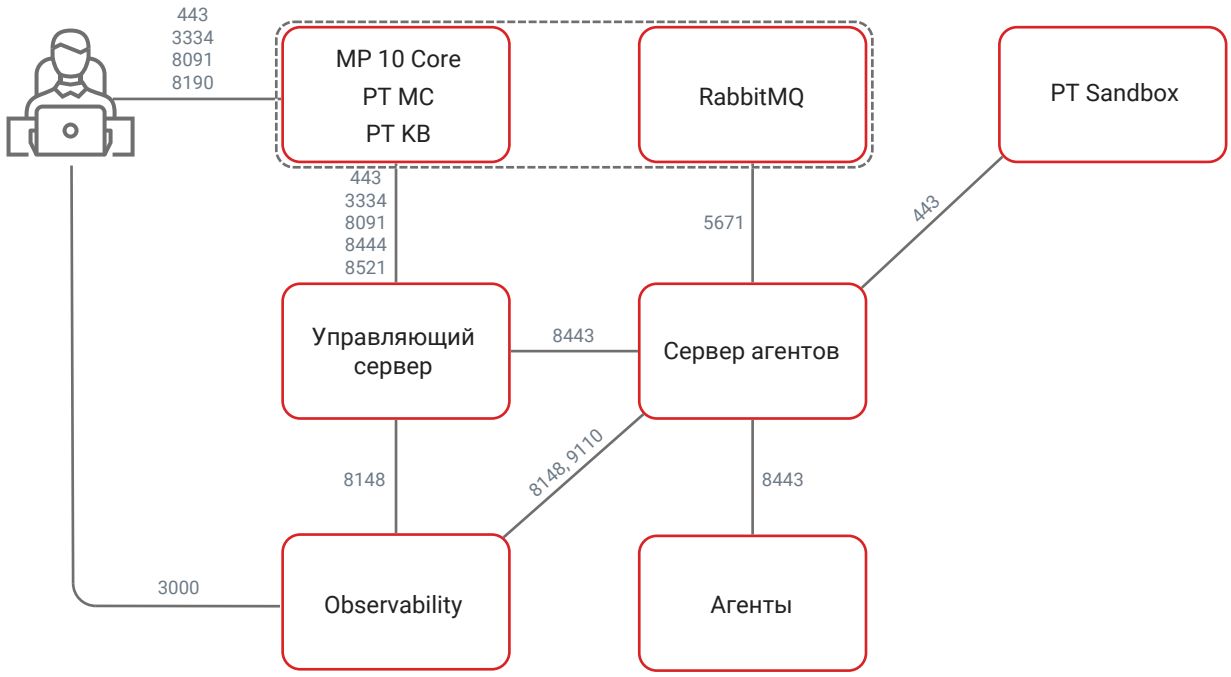

Рисунок 1. Взаимодействие компонентов MaxPatrol EDR

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

Примечание. Если какие-либо компоненты MaxPatrol EDR расположены на одном сервере, то обеспечивать внешнюю доступность портов при их взаимодействии необязательно. Например, при установке всех компонентов на один сервер открывать порты 5431, 8148, 8443, 9000, 9047, 9110 не требуется.

Примечание. В таблице приведены порты, используемые по умолчанию.

Таблица 1. Компоненты и порты взаимодействия

Источник	Получатель	Протокол	TCP-порт
Управляющий сервер	Сервер агентов	HTTPS	8443

Источник	Получатель	Протокол	TCP-порт
Управляющий сервер	MP 10 Core	HTTPS	443, 3334, 8444, 8521
Управляющий сервер	Компонент Observability	gRPC	8148
Управляющий сервер	Сервис пользовательской экспертизы (компонент `custom_expertise`)	HTTPS	9047 (при установке в отказоустойчивом кластере (см. раздел 6.7))
Сервер агентов	PT Sandbox	HTTPS	443
Сервер агентов	Сервер RabbitMQ	AMQP	5671
Сервер агентов	Компонент Observability	gRPC	8148
Сервер агентов	Компонент Observability	HTTPS	9110
Агент	Сервер агентов	WSS	8443
Рабочая станция пользователя	Управляющий сервер	SSH	22 (при необходимости для удаленного доступа по протоколу SSH)
Рабочая станция пользователя	Сервер агентов	SSH	22 (при необходимости для удаленного доступа по протоколу SSH)
Рабочая станция пользователя	MP 10 Core	HTTPS	443, 3334, 8091, 8190
Рабочая станция пользователя	Компонент `observability`	HTTPS	3000 (веб-интерфейс Grafana)
Внешние системы (взаимодействие через публичный API)	Управляющий сервер	HTTPS	8444
Сервер с ролью Deployer (если эта роль установлена отдельно от компонента MP 10 Core)	Управляющий сервер Сервер агентов Компонент Observability	TCP	22

См. также

Мониторинг состояния MaxPatrol EDR (см. раздел 22.3)

4. Лицензирование

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

В MaxPatrol EDR доступно два способа лицензирования: в первом управление лицензией осуществляется в PT MC (при версии 101.1 или выше), во втором — в MaxPatrol EDR. При новой установке способ лицензирования выбирается автоматически в зависимости от версии PT MC. При обновлении с версии MaxPatrol EDR 7.1 вы можете выбрать способ лицензирования самостоятельно, если у вас используется PT MC версии 101.1 или выше.

При любом способе лицензирования для каждой лицензии указываются срок ее действия, максимальное количество авторизованных агентов и возможность разработки модулей. После истечения срока действия лицензии будут ограничены обновление системы, авторизация и перемещение агентов между группами, создание и настройка политик, восстановление системы из резервной копии, а также обновление модулей на конечных устройствах.

Для активации MaxPatrol EDR в PT MC вам нужно добавить лицензию и привязать ее к приложению. Файл с лицензией вам нужно запросить у вашего менеджера Positive Technologies.

> **Примечание.** Для управления лицензией в PT MC вам нужны соответствующие привилегии.

Добавление лицензии в PT MC

- Чтобы добавить лицензию при наличии доступа к интернету:

  1. В главном меню выберите **Лицензии**.
  2. Нажмите **Обновить список лицензий**.

Для добавления лицензии вручную вам потребуется ZIP-файл с лицензией из комплекта поставки.

> **Примечание.** Если ваш комплект не содержит ZIP-файла с лицензией, вы можете запросить его в службе технической поддержки.

- Чтобы добавить лицензию вручную, без доступа к интернету:

  1. В главном меню выберите **Лицензии**.
  2. Нажмите **Добавить**.
  3. Выберите ZIP-файл с лицензией.

     > **Примечание.** Файл может содержать как одну, так и несколько лицензий. В систему будут добавлены все корректные лицензии, которые содержатся в файле.

  4. Нажмите **Добавить**.

Привязка лицензии в PT MC

- Чтобы привязать лицензию к приложению MaxPatrol EDR:

  1. В главном меню выберите **Лицензии**.
  2. Выберите лицензию и нажмите **Привязать**.
  3. Выберите установленное приложение MaxPatrol EDR, к которому нужно привязать лицензию.
  4. Нажмите **Привязать**.

Лицензирование в MaxPatrol EDR

Если вы используете старый способ лицензирования, то управление лицензией осуществляется в MaxPatrol EDR. В этом случае процесс лицензирования состоит из следующих шагов:

1. В веб-интерфейсе MaxPatrol EDR вы генерируете фингерпринт на странице **Лицензии EDR**.
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

MaxPatrol EDR используется совместно с системой MaxPatrol 10 версии 26.1, 27.2 или 27.3.

Управляющий сервер и сервер агентов MaxPatrol EDR рекомендуется устанавливать на чистую 64-разрядную операционную систему. Поддерживаются следующие операционные системы:

— Debian 10, 11, 12;

— Astra Linux Special Edition 1.7.6, 1.8;

  Внимание! Перед установкой управляющего сервера или сервера агентов в Astra Linux (кроме систем с уровнем защищенности «Орел») необходимо в файл `/etc/docker/daemon.json` добавить параметр `"astra-sec-level" : 6` и перезапустить службу Docker с помощью команды `sudo systemctl restart docker`. Также необходимо в конфигурационный файл `/etc/parsec/fs-ilev.conf` добавить каталоги `/opt/edr`, `/opt/edr_data`, `/opt/edr_tmp` с уровнем целостности `min`.

— «Альт Сервер» 10.1.

Если управляющий сервер или сервер агентов планируется использовать на одном сервере с компонентами системы MaxPatrol 10, то установку необходимо выполнять на операционную систему, поддерживаемую этой системой.

Для работы управляющего сервера и сервера агентов MaxPatrol EDR в операционной системе должнен быть установлен компонент Docker CE версии 20.10.24 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.

> **Примечание.** Дистрибутив компонента Docker CE версии 20.10.24 для операционных систем Debian и Astra Linux вы можете скачать по ссылке. Для установки Docker CE в другой ОС обратитесь в службу технической поддержки Positive Technologies.

Для работы в интерфейсе MaxPatrol EDR рекомендуется использовать последние версии браузеров Google Chrome или Яндекс Браузер.

5.2. Требования к аппаратному обеспечению конфигурации для низконагруженных систем

Компоненты системы необходимо устанавливать на сервер или в виртуальную среду, которые удовлетворяют приведенным ниже аппаратным требованиям.

Таблица 2. Аппаратные требования к управляющему серверу и серверу агентов (при установке отдельно от компонентов системы MaxPatrol 10)

	Минимальные требования	
	До 2000 событий в секунду (до 1000 агентов)	**До 5000 событий в секунду (до 2000 агентов)**
Количество логических ядер в системе виртуализации	8	10
Память (ОЗУ)	40 ГБ	40 ГБ
Твердотельный накопитель (SSD) для системных данных	500 ГБ	500 ГБ

Таблица 3. Аппаратные требования к управляющему серверу и серверу агентов (с учетом компонентов системы MaxPatrol 10)

	Минимальные требования	
	До 2000 событий в секунду (до 1000 агентов)	**До 5000 событий в секунду (до 2000 агентов)**
Количество логических ядер в системе виртуализации [1]	32	42
Память (ОЗУ)	104 ГБ	136 ГБ
Твердотельный накопитель (SSD) для системных данных [2]	1 000 ГБ	1 000 ГБ
Жесткий диск (HDD) для хранения событий (LogSpace) [3]	1 000 ГБ	2 500 ГБ
Жесткий диск (HDD) для хранения событий (Elasticsearch) [4]	6 000 ГБ	14 000 ГБ

Рекомендуется использовать сетевой адаптер со скоростью не менее 1 Гбит/с.

5.3. Требования к аппаратному обеспечению конфигурации для средненагруженных систем

Компоненты системы необходимо устанавливать на серверы или в виртуальную среду, которые удовлетворяют приведенным ниже аппаратным требованиям.

1 Соответствует количеству потоков в физических ядрах процессора с включенной технологией Hyper-Threading. Рекомендуется использовать процессоры Intel Xeon Scalable второго поколения и выше или их аналоги. Установка хранилища LogSpace возможна только на серверы с процессорами, поддерживающими расширение AVX для системы команд.

2 Рекомендуется объединить твердотельные накопители (SSD) в массив RAID 1, создать раздел с файловой системой ext4 (размер блока 4096 байт) объемом не менее указанного в таблице и смонтировать его как корневой каталог `/`.

3 При хранении событий за 30 дней и среднем размере события 1—2 КБ, а также сохранении сырых и нормализованных данных о событиях. Рекомендуется использовать жесткие диски (HDD) со скоростью вращения 7200 об./мин каждый, объединенные в массив RAID 10, и выделить один каталог для хранения событий (по умолчанию `/opt/logspaced`).

4 При хранении событий за 30 дней и среднем размере события 1—2 КБ, а также сохранении сырых и нормализованных данных о событиях. Рекомендуется использовать жесткие диски (HDD) со скоростью вращения 7200 об./мин каждый, объединенные в массив RAID 10, и выделить один каталог для хранения событий (по умолчанию `/data`).

Таблица 4. Аппаратные требования к управляющему серверу (при установке на отдельный сервер)

	Минимальные требования
Центральный процессор	4
Память (ОЗУ)	10 ГБ
Твердотельный накопитель (SSD)	100 ГБ

Рекомендуется использовать сетевой адаптер со скоростью не менее 1 Гбит/с.

Таблица 5. Аппаратные требования к управляющему серверу (с учетом компонента MP 10 Core системы MaxPatrol 10)

	Минимальные требования	
	До 10 000 событий в секунду	**До 15 000 событий в секунду**
Количество логических ядер в системе виртуализации [5]	24	28
Память (ОЗУ)	44 ГБ	56 ГБ
Твердотельный накопитель (SSD) [6]	1 000 ГБ	1 000 ГБ

Рекомендуется использовать сетевой адаптер со скоростью не менее 1 Гбит/с.

5 Соответствует количеству потоков в физических ядрах процессора с включенной технологией Hyper-Threading. Рекомендуется использовать процессоры Intel Xeon Scalable второго поколения и выше или их аналоги. Установка хранилища LogSpace возможна только на серверы с процессорами, поддерживающими расширение AVX для системы команд.

6 Рекомендуется объединить твердотельные накопители (SSD) в массив RAID 1, создать раздел с файловой системой ext4 (размер блока 4096 байт) объемом не менее указанного в таблице и смонтировать его как корневой каталог `/`.

Таблица 6. Аппаратные требования к серверу агентов (при установке на сервер с компонентами MP SIEM Server и MP SIEM Events Storage системы MaxPatrol 10)

	Минимальные требования	
	До 10 000 событий в секунду (до 3 000 агентов)	**До 15 000 событий в секунду (до 5 000 агентов)**
Количество логических ядер в системе виртуализации [5]	48	66
Память (ОЗУ)	160 ГБ	176 ГБ
Твердотельный накопитель (SSD) [6] для системных данных	500 ГБ	500 ГБ
Жесткий диск (HDD) для хранения событий (LogSpace) [7]	5 000 ГБ	7 500 ГБ
Жесткий диск (HDD) для хранения событий (Elasticsearch) [8]	28 000 ГБ	42 000 ГБ

Рекомендуется использовать сетевой адаптер со скоростью не менее 1 Гбит/с.

Таблица 7. Аппаратные требования к серверу агентов

	Минимальные требования	
	До 10 000 событий в секунду (до 3 000 агентов)	**До 15 000 событий в секунду (до 5 000 агентов)**
Количество логических ядер в системе виртуализации [5]	8	10
Память (ОЗУ)	48 ГБ	48 ГБ
Твердотельный накопитель (SSD) [6] для системных данных	300 ГБ	300 ГБ

Рекомендуется использовать сетевой адаптер со скоростью не менее 1 Гбит/с.

7 При хранении событий за 30 дней и среднем размере события 1—2 КБ, а также сохранении сырых и нормализованных данных о событиях. Рекомендуется использовать жесткие диски (HDD) со скоростью вращения 7200 об./мин каждый, объединенные в массив RAID 10, и выделить один каталог для хранения событий (по умолчанию `/opt/logspaced`).

8 При хранении событий за 30 дней и среднем размере события 1—2 КБ, а также сохранении сырых и нормализованных данных о событиях. Рекомендуется использовать жесткие диски (HDD) со скоростью вращения 7200 об./мин каждый, объединенные в массив RAID 10, и выделить один каталог для хранения событий (по умолчанию `/data`).

Таблица 8. Аппаратные требования к серверу агентов (при установке с компонентом observability)

	Минимальные требования	
	До 10 000 событий в секунду (до 3 000 агентов)	**До 15 000 событий в секунду (до 5 000 агентов)**
Количество логических ядер в системе виртуализации [5]	12	14
Память (ОЗУ)	56 ГБ	56 ГБ
Твердотельный накопитель (SSD) [6] для системных данных	500 ГБ	500 ГБ

Рекомендуется использовать сетевой адаптер со скоростью не менее 1 Гбит/с.

Примечание. Аппаратные требования к серверам с компонентами системы MaxPatrol 10 приведены в Руководстве по внедрению из комплекта поставки MaxPatrol 10.

5.4. Требования к аппаратному обеспечению конфигурации для высоконагруженных систем

Компоненты системы необходимо устанавливать на серверы или в виртуальную среду, которые удовлетворяют приведенным ниже аппаратным требованиям.

Таблица 9. Аппаратные требования к управляющему серверу (при установке на отдельный сервер)

	Минимальные требования
Центральный процессор	4
Память (ОЗУ)	10 ГБ
Твердотельный накопитель (SSD)	100 ГБ

Рекомендуется использовать сетевой адаптер со скоростью не менее 1 Гбит/с.

Таблица 10. Аппаратные требования к управляющему серверу (с учетом компонента MP 10 Core системы MaxPatrol 10)

	Минимальные требования			
	До 30 000 событий в секунду	**До 50 000 событий в секунду**	**До 100 000 событий в секунду**	**До 300 000 событий в секунду**
Количество логических ядер в системе виртуализации [9]	36	36	52	66
Память (ОЗУ)	72 ГБ	72 ГБ	104 ГБ	136 ГБ
Твердотельный накопитель (SSD) [10]	1 000 ГБ	1 500 ГБ	2 500 ГБ	5 000 ГБ

Рекомендуется использовать сетевой адаптер со скоростью не менее 10 Гбит/с.

Таблица 11. Аппаратные требования к серверу агентов (при установке на сервер с компонентом MP SIEM Server системы MaxPatrol 10)

	Минимальные требования			
	До 20 000 событий в секунду (до 5 000 агентов)	**До 30 000 событий в секунду (до 5 000 агентов)**	**До 40 000 событий в секунду (до 5 000 агентов)**	**До 50 000 событий в секунду (до 5 000 агентов)**
Количество логических ядер в системе виртуализации [9]	60	84	118	144
Память (ОЗУ)	96 ГБ	96 ГБ	96 ГБ	112 ГБ
Твердотельный накопитель (SSD) [10]	1 000 ГБ	1 000 ГБ	1 000 ГБ	1 000 ГБ

Рекомендуется использовать сетевой адаптер со скоростью не менее 10 Гбит/с.

9 Соответствует количеству потоков в физических ядрах процессора с включенной технологией Hyper-Threading. Рекомендуется использовать процессоры Intel Xeon Scalable второго поколения и выше или их аналоги.

10 Рекомендуется объединить твердотельные накопители (SSD) в массив RAID 10, создать раздел с файловой системой ext4 (размер блока 4096 байт) объемом не менее указанного в таблице и смонтировать его как корневой каталог `/`.

Таблица 12. Аппаратные требования к серверу агентов

	Минимальные требования			
	До 20 000 событий в секунду (до 5 000 агентов)	**До 30 000 событий в секунду (до 5 000 агентов)**	**До 40 000 событий в секунду (до 5 000 агентов)**	**До 50 000 событий в секунду (до 5 000 агентов)**
Количество логических ядер в системе виртуализации [9]	12	20	22	32
Память (ОЗУ)	48 ГБ	48 ГБ	48 ГБ	48 ГБ
Твердотельный накопитель (SSD) [10]	300 ГБ	300 ГБ	300 ГБ	300 ГБ

Рекомендуется использовать сетевой адаптер со скоростью не менее 10 Гбит/с.

Таблица 13. Аппаратные требования к серверу агентов (при установке с компонентом observability)

	Минимальные требования			
	До 20 000 событий в секунду (до 5 000 агентов)	**До 30 000 событий в секунду (до 5 000 агентов)**	**До 40 000 событий в секунду (до 5 000 агентов)**	**До 50 000 событий в секунду (до 5 000 агентов)**
Количество логических ядер в системе виртуализации [9]	16	24	26	36
Память (ОЗУ)	56 ГБ	56 ГБ	56 ГБ	56 ГБ
Твердотельный накопитель (SSD) [10]	500 ГБ	500 ГБ	500 ГБ	500 ГБ

Рекомендуется использовать сетевой адаптер со скоростью не менее 10 Гбит/с.

Примечание. Аппаратные требования к серверам с компонентами системы MaxPatrol 10 приведены в Руководстве по внедрению из комплекта поставки MaxPatrol 10.

5.5. Требования к программному и аппаратному обеспечению конечного устройства

Агент поддерживает установку на конечные устройства под управлением следующих 64-разрядных операционных систем:

- Windows 7, 8, 8.1, 10, 11 (только редакции Pro);
- Windows Server 2016, 2019, 2022;
- macOS: 11, 12 (поддерживаются только компьютеры Mac с процессорами Intel);
- Debian 10, 11, 12;
- Ubuntu 20.04 LTS; 22.04 LTS; 24.04 LTS;
- CentOS Stream 9, Stream 10;
- Red Hat Enterprise Linux 7, 8, 9;
- Astra Linux Special Edition 1.3, 1.7, 1.8 («Орел»);
- Astra Linux Common Edition 2.12 («Орел»);
- «РЕД ОС Рабочая станция» 7.3, 8.0;
- AlterOS Desktop 7.5;
- Oracle Linux 9;
- «ОСнова» 2.0 «Оникс»;
- «Альт Сервер» 9, 10.1, 10.2;
- «Альт Рабочая станция» 10.2;
- «МОС» 12.

Внимание! В текущей версии MaxPatrol EDR невозможно сканирование в режиме аудита на узлах под управлением следующих ОС: Windows 11, Astra Linux Common Edition 2.12 («Орел»), «РЕД ОС Рабочая станция» 7.3, AlterOS Desktop 7.5, «ОСнова» 2.0 «Оникс», «Альт Сервер» 9, 10.1, 10.2, «Альт Рабочая станция» 10.2 и «МОС» 12. Кроме того, в CentOS Stream 10 невозможна установка компонента auditd с помощью модуля «Установщик auditd».

Примечание. Если на конечном устройстве под управлением Linux нет доступа к пакетным менеджерам, то для корректной установки и работы агента в ОС должны быть установлены пакеты libpthread, libnsl и libcrypto.

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

Таблица 14. 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 4 логических ядра
Память (ОЗУ)	Зависит от установленных модулей, количества обрабатываемых событий и ряда других факторов (см. раздел 5.6)	
Сетевой адаптер	От 200 Кбит/с	От 5 Мбит/с
Жесткий диск, свободное дисковое пространство	HDD или SSD, от 500 МБ	HDD или SSD, от 1000 МБ

5.6. Расчет потребления ресурсов агентом на конечном устройстве

Потребление агентом ресурсов на конечном устройстве зависит от установленных модулей, количества обрабатываемых событий и ряда других факторов. В целях оптимизации потребления ресурсов нужно при настройке политик придерживаться следующих рекомендаций:

— В модулях сбора необходимо использовать фильтры и исключать события, не представляющие значимости для информационной безопасности.

— Для каждой группы конечных устройств, на которых установлено нестандартное ПО, необходимо использовать отдельные политики, в которых учтены особенности такого ПО.

— Модуль «YARA-сканер» при сканировании резервирует память, соизмеримую с размером проверяемого файла или процесса. При настройке автоматического реагирования нужно учитывать, что проверка больших файлов или процессов может вызвать резкий рост потребления ресурсов.

— Не рекомендуется использовать модуль «Проверка файлов по хеш-сумме» на большом потоке уникальных файлов. Чем больше размер файла или их количество, тем больше ресурсов будет тратиться на их проверку.

Ниже приведен расчет потребления ресурсов агентом. В Windows расчет производился на виртуальной машине на компьютере с процессором Intel Xeon E5-2698 v4, в Linux — с процессором Intel Xeon E-2288G. Исследование проводилось на следующих наборах модулей:

— В Windows:

- Сбор данных — «WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор».
- Сбор данных и обнаружение — «WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор», «Коррелятор».

- Сбор данных, расширенное обнаружение и реагирование — «WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор», «YARA-сканер», «Коррелятор» и модули реагирования (см. раздел 19.5).
- Сбор данных и интеграции с PT Sandbox и MaxPatrol VM — «WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор», «Проверка файлов в PT Sandbox», «Сканирование в режиме аудита (MaxPatrol VM).

— В Linux:

- Сбор данных — «Установщик auditd», «Сбор данных из файлов журналов», «Нормализатор».
- Сбор данных и обнаружение — «Установщик auditd», «Сбор данных из файлов журналов», «Нормализатор», «Коррелятор (Linux)».
- Сбор данных, обнаружение и интеграции с PT Sandbox и MaxPatrol VM — «Установщик auditd», «Сбор данных из файлов журналов», «Нормализатор», «Коррелятор (Linux)», «Проверка файлов в PT Sandbox», «Сканирование в режиме аудита (MaxPatrol VM).

Внимание! Расчет является ориентировочным, в других условиях потребление ресурсов может отличаться. На загрузку центрального процессора может влиять множество факторов.

Таблица 15. Потребление ресурсов агентом (от 2 до 10 событий в секунду)

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор
Windows	Сбор данных	124—132 МБ	1 ядро, до 3,3%
	Сбор данных и обнаружение	605—656 МБ	1 ядро, до 18,2%
	Сбор данных, расширенное обнаружение и реагирование	1—1,5 ГБ	2 ядра
	Сбор данных и интеграции с PT Sandbox и MaxPatrol VM	149—176 МБ	1 ядро, до 2,7%
Linux	Сбор данных	До 319 МБ	1 ядро, до 1,5%
	Сбор данных и обнаружение	До 745 МБ	1 ядро, до 1,8%
	Сбор данных, обнаружение и интеграции с PT Sandbox и MaxPatrol VM	756—790 МБ	1 ядро, до 17%

Таблица 16. Потребление ресурсов агентом (до 20 событий в секунду)

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор
Windows	Сбор данных	До 143 МБ	1 ядро, до 2%

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор
	Сбор данных и обнаружение	До 693 МБ	1 ядро, до 40,5%
	Сбор данных, расширенное обнаружение и реагирование	До 1,51 ГБ	2 ядра
	Сбор данных и интеграции с PT Sandbox и MaxPatrol VM	До 212 МБ	1 ядро, до 3,7%
Linux	Сбор данных	До 319 МБ	1 ядро, до 1,8%
	Сбор данных и обнаружение	До 745 МБ	1 ядро, до 1,6%
	Сбор данных, обнаружение и интеграции с PT Sandbox и MaxPatrol VM	До 814 МБ	1 ядро, до 17%

Таблица 17. Потребление ресурсов агентом (до 50 событий в секунду)

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор
Windows	Сбор данных	До 172 МБ	1 ядро, до 7%
	Сбор данных и обнаружение	До 744 МБ	1 ядро, до 65,3%
	Сбор данных, расширенное обнаружение и реагирование	До 1,53 ГБ	3 ядра
	Сбор данных и интеграции с PT Sandbox и MaxPatrol VM	До 272 МБ	1 ядро, до 7,2%
Linux	Сбор данных	До 319 МБ	1 ядро, до 1,2%
	Сбор данных и обнаружение	До 746 МБ	1 ядро, до 2%
	Сбор данных, обнаружение и интеграции с PT Sandbox и MaxPatrol VM	До 830 МБ	1 ядро, до 26,8%

Таблица 18. Потребление ресурсов агентом (до 100 событий в секунду)

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор
Windows	Сбор данных	До 189 МБ	1 ядро, до 7%
	Сбор данных и обнаружение	До 777 МБ	1 ядро, до 65,3%
	Сбор данных, расширенное обнаружение и реагирование	До 1,55 ГБ	3 ядра
	Сбор данных и интеграции с PT Sandbox и MaxPatrol VM	До 291 МБ	1 ядро, до 7,2%

ОС	Набор модулей	Память (ОЗУ)	Центральный процессор
Linux	Сбор данных	До 320 МБ	1 ядро, до 1,2%
	Сбор данных и обнаружение	До 746 МБ	1 ядро, до 1,8%
	Сбор данных, обнаружение и интеграции с PT Sandbox и MaxPatrol VM	До 835 МБ	1 ядро, до 19,5%

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 ролью Deployer.

- 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
     ```
     Внимание! Для корректной установки MaxPatrol EDR путь к распакованному дистрибутиву должен быть без пробелов.
  4. Распакуйте архив в созданный каталог:
     ```
     tar xvf edr-installer.<Версия продукта>.tar.gz -C edr-installer/
     ```
     Например:
     ```
     tar xvf edr-installer.v6.1.0.1111.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 19. Параметры в манифесте установки MaxPatrol EDR

Параметр	Описание
`hosts` → `<IP-адрес или полное доменное имя сервера>` → `components`	Список устанавливаемых компонентов MaxPatrol EDR. При обычной установке список компонентов управляющего сервера должен содержать `dbms`, `observability`, `edr_update`, `api` и `custom_expertise`, других серверов — `agent_server` и при необходимости `observability`. Вы также можете установить компонент `agent_server` на управляющем сервере. При установке в отказоустойчивом кластере компонент `api` может быть установлен на нескольких серверах, а остальные компоненты управляющего сервера могут располагаться на отдельных серверах
`hosts` → `<IP-адрес или полное доменное имя 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>:<Путь к файлу с SSH-ключом>`; — `<Логин>::<Путь к файлу с SSH-ключом>`
`hosts` → `<IP-адрес или полное доменное имя сервера>` → `service_name`	Название сервера агентов в системе

Параметр	Описание
hosts → <IP-адрес или полное доменное имя сервера> → wan_ip	Определяет IP-адрес, по которому будет доступен сервер. Этот параметр полезен для повышения безопасности, если сервер имеет несколько назначенных IP-адресов. 0.0.0.0 — сервер доступен по любому назначенному IP-адресу
hosts → <IP-адрес или полное доменное имя 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 или полное доменное имя сервера> → mp_rmq → siem_server_name	Название экземпляра роли MaxPatrol SIEM Server. Для получения названий экземпляров роли в системе MaxPatrol 10 вам нужно на сервере с ролью Deployer выполнить команду sudo /opt/deployer/bin/Get-Params.ps1 -json -RoleTypeId SiemServer. Пример ответа:
	{
	"< Название экземпляра роли 1>": {
	...
	},
	"< Название экземпляра роли 2>": {
	...
	},
	}

hosts → <IP-адрес или полное доменное имя сервера> → mp_rmq → ssl_ca	Путь до файла корневого SSL-сертификата на сервере, с которого выполняется установка

Параметр	Описание
`hosts → <IP-адрес или полное доменное имя сервера> → mp_rmq → ssl_cert`	Путь до файла публичного SSL-сертификата на сервере, с которого выполняется установка
`hosts → <IP-адрес или полное доменное имя сервера> → mp_rmq → ssl_key`	Путь до файла закрытого ключа SSL-сертификата на сервере, с которого выполняется установка
`hosts → <IP-адрес или полное доменное имя сервера> → mp_rmq → rmq_host`	IP-адрес или FQDN сервера RabbitMQ
`hosts → <IP-адрес или полное доменное имя сервера> → mp_rmq → rmq_port`	Порт сервера RabbitMQ
`hosts → <IP-адрес или полное доменное имя сервера> → mp_rmq → rmq_vhost`	Имя виртуального узла RabbitMQ
`hosts → <IP-адрес или полное доменное имя сервера> → cmc_certs → manage`	Определяет, с помощью каких сертификатов будет подписываться код пользовательских модулей. Возможные значения: — `skip` — подпись кода пользовательских модулей выполняться не будет; — `auto` — сертификаты будут выпущены автоматически (каталог `/opt/edr/cmc_certs/`); — `manual` — будут использоваться пользовательские сертификаты (задаются с помощью параметров `cmc_cert_path`, `cmc_key_path`, `cmc_certs_dir`). Группу параметров `cmc_certs` необходимо задавать только для управляющего сервера
`hosts → <IP-адрес или полное доменное имя сервера> → cmc_certs → cmc_cert_path`	Путь до файла сертификата, которым будут подписываться пользовательские модули
`hosts → <IP-адрес или полное доменное имя сервера> → cmc_certs → cmc_key_path`	Путь до файла ключа сертификата
`hosts → <IP-адрес или полное доменное имя сервера> → cmc_certs → cmc_certs_dir`	Путь до каталога с дополнительными сертификатами (может быть задан при любом значении параметра `manage`). Перед установкой продукта в этот каталог необходимо скопировать сертификаты с других серверов MaxPatrol EDR, если вы планируете импортировать оттуда разработанные модули

Параметр	Описание
`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 → api → MINIO_ACCESS_KEY`
`param → edr_update → MINIO_ACCESS_KEY`
	Ключ доступа к объектному хранилищу MinIO на управляющем сервере. Значения всех параметров должны совпадать

`param → custom_expertise → MINIO_ACCESS_KEY`	Ключ доступа к объектному хранилищу сервиса пользовательской экспертизы в MinIO
`param → agent_server → MINIO_SECRET_KEY`	Секретный ключ доступа к объектному хранилищу MinIO на сервере агентов

`param → dbms → MINIO_SECRET_KEY`
`param → api → MINIO_SECRET_KEY`
`param → edr_update → MINIO_SECRET_KEY`
	Секретный ключ доступа к объектному хранилищу MinIO на управляющем сервере. Значения всех параметров должны совпадать

`param → custom_expertise → MINIO_SECRET_KEY`	Секретный ключ доступа к объектному хранилищу сервиса пользовательской экспертизы в MinIO
`param → <Компонент> → Resources → limits → cpus`	Максимальное количество логических ядер, выделенных для контейнера с компонентом. Допускаются дробные значения с шагом 0,1, например `2.5`. `0` — отсутствие ограничений
`param → <Компонент> → Resources → limits → memory`	Максимальное количество памяти (ОЗУ), выделенной для контейнера с компонентом. Поддерживаемые единицы: `b` (байт), `k` или `kb` (килобайт), `m` или `mb` (мегабайт), `g` или `gb` (гигабайт)

Параметр	Описание
`param → <Компонент> → Resources → limits → pids`	Максимальное количество процессов, которые могут выполняться внутри контейнера с компонентом. `-1` — отсутствие ограничений
`param → <Компонент> → Resources → ulimits`	Задает `ulimit` для контейнера с компонентом. Допускается задание мягких и жестких ограничений

Примечание. Группы параметров `limits` и `ulimits` необязательные.

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", "api", "edr_update",
"custom_expertise"],
"credentials": "login:password",
"service_name": "First server",
"mp_rmq": { "auto": true, "siem_server_name": "siemserver-1" }
"cmc_certs": {"manage": "auto", "cmc_certs_dir": "/opt/certs/extra/"}
}
```

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", "api", "edr_update",
"custom_expertise"],
"credentials": "login:password",
"service_name": "Management server",
"mp_rmq": { "auto": true, "siem_server_name": "siemserver-1" }
"cmc_certs": {"manage": "manual", "cmc_cert_path": "/opt/certs/cert.crt",
"cmc_key_path": "/opt/certs/cert.key", "cmc_certs_dir": "/opt/certs/extra/"}
},
"192.0.2.5": {
"components": ["agent_server],
"credentials": "login:password",
"service_name": "Agent server north",
"mp_rmq": { "auto": true, "siem_server_name": " siemserver-2" }
},
"203.0.113.34": {
```

```
"components": ["agent_server"],
"credentials": "login:password",
"service_name": "Agent server east",
"mp_rmq": { "auto": true, "siem_server_name": "siemserver-3" }
}
},
```

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:
     `sudo 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 установлена роль Deployer системы MaxPatrol 10. Перед этим нужно распаковать архив с дистрибутивом (см. раздел 6.1), задать параметры установки в манифесте (см. раздел 6.2) и убедиться, что все серверы соответствуют аппаратным и программным требованиям (см. раздел 5). Если роль Deployer установлена отдельно от компонента MP 10 Core, то на сервере с этой ролью необходимо:

1. создать каталог `/var/lib/deployed-roles/mp10-application/core-<Идентификатор>/certs/`, скопировать в него все сертификаты и их ключи из такого же каталога на сервере с MP 10 Core;
2. если установлена версия MaxPatrol 10 27.2, создать каталог `/var/lib/deployed-roles/mc-application/managementandconfiguration-<Идентификатор>/tools/`, скопировать в него скрипт `auto-approve-registration.sh` из такого же каталога на сервере с MP 10 Core;
3. назначить права доступа к сертификатам (с помощью команды `chmod 644`) и к скрипту (`chmod 755`).

► 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`.

Если до установки MaxPatrol EDR вы вошли в MaxPatrol 10, то для появления в главном меню раздела **EDR** необходимо выйти из системы и заново войти.

См. также

Распаковка архива с дистрибутивом MaxPatrol EDR (см. раздел 6.1)

Манифест установки MaxPatrol EDR (см. раздел 6.2)

Программные и аппаратные требования (см. раздел 5)

6.5. Параметры установочного скрипта

В таблице ниже приведены допустимые параметры установочного скрипта.

Таблица 20. Параметры установочного скрипта

Параметр	Описание	Значение по умолчанию
`--wan-hostname`	Задает внешний адрес, по которому будет доступен управляющий сервер. Обязателен для установки в отказоустойчивом кластере. В обычной установке может быть использован, если установочный скрипт не смог	Не используется

Параметр	Описание	Значение по умолчанию
	автоматически определить адрес (например, если в манифесте был задан IP-адрес сервера 127.0.0.1)	
`--wan-port`	Задает внешний порт, по котором будет доступен управляющий сервер (используется в сертификатах и при регистрации в PT MC)	`8444` (при установке всех компонентов на один сервер), `443` (в любой другой конфигурации)
`--wan-cert`	Задает путь до файла SSL-сертификата, который будет использоваться для доступа к управляющему серверу	Не используется
`--wan-cert-key`	Задает путь до файла ключа SSL-сертификата, который будет использоваться для доступа к управляющему серверу	Не используется
`--cluster`	Используется для установки в отказоустойчивом кластере	Не используется
`--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
`--enable-module-verify`	Активирует проверку подписи кода модулей	`True` (при новой установке), `False` (при обновлении с предыдущих версий до версии 6.0)
`--allow-old-docker-version`	Разрешает установку MaxPatrol EDR при версии компонента Docker CE ниже 20.10.24	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), и распаковать архив с дистрибутивом (см. раздел 6.1).

- Чтобы установить дополнительный сервер агентов:

  1. Перейдите в каталог `opt/edr/`.
     ```
     cd /opt/edr/
     ```
  2. Откройте файл `manifest.json` для редактирования:
     ```
     sudo 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`.

6.7. Установка MaxPatrol EDR в отказоустойчивом кластере

Вы можете установить MaxPatrol EDR в отказоустойчивом кластере. При таком способе установки будет обеспечиваться отказоустойчивость СУБД PostgreSQL, объектного хранилище MinIO и управляющего сервера. Установку MaxPatrol EDR в отказоустойчивом кластере рекомендуется выполнять, если система MaxPatrol 10 также установлена в кластере.

> **Примечание.** Если MaxPatrol 10 установлен в обычном режиме, вам нужно самостоятельно установить кластер PostgreSQL.

Для развертывания отказоустойчивого кластера MaxPatrol EDR вам необходимо:

1. Установить и настроить службу Keepalived для кластера с управляющим сервером MaxPatrol EDR.
2. Установить службу Keepalived для кластера MinIO.
3. Установить кластер MinIO.

   > **Примечание.** Для установки кластера MinIO нужны четыре сервера с установленным компонентом Docker CE.
4. Настроить манифест установки MaxPatrol EDR.
5. Установить MaxPatrol EDR.

Установка и настройка службы Keepalived для кластера с управляющим сервером MaxPatrol EDR

Служба Keepalived обеспечивает работоспособность управляющего сервера в случае сбоев его отдельных узлов. Перед выполнением инструкции вам нужно выделить в сетевой инфраструктуре организации виртуальный IP-адрес, по которому будет доступен управляющий сервер, и добавить для него DNS-запись. Этот IP-адрес не должен принадлежать ни одному из узлов кластера. Также необходимо выбрать порт, по которому будут идти обращения к управляющему серверу.

Внимание! Инструкцию необходимо выполнить на всех узлах, на которых будет установлен управляющий сервер. Инструкция дана для узлов под управлением Debian.

- Чтобы установить и настроить службу Keepalived:

  1. Установите службу:
     ```
     sudo apt install keepalived -y
     ```
  2. Включите поддержку виртуальных IP-адресов в ядре Linux:
     ```
     echo 'net.ipv4.ip_nonlocal_bind=1' >> /etc/sysctl.conf
     sysctl -p /etc/sysctl.conf
     ```

3. Заполните конфигурационный файл `/etc/keepalived/keepalived.conf` в следующем формате:

```
global_defs {
   router_id keepalived
}
   vrrp_instance VI_1 {
      state <MASTER или BACKUP>
      interface <Название сетевого адаптера, на котором находится виртуальный IP-адрес>
      virtual_router_id <Идентификатор сети>
      priority <Приоритет узла>
      advert_int 1
      virtual_ipaddress {
          <Выделенный виртуальный IP-адрес кластера>
}
```

   В кластере один узел должен быть `MASTER`, остальные `BACKUP`. Приоритет узла — это число от 0 до 255, причем у узла `MASTER` приоритет должен быть выше, чем у узлов `BACKUP`. Идентификатором сети может быть любое число, которое будет одинаковым на всех узлах кластера.

   Пример конфигурации:

```
global_defs {
   router_id keepalived
}
   vrrp_instance VI_1 {
      state MASTER
      interface eth0
      virtual_router_id 50
      priority 101
      advert_int 1
      virtual_ipaddress {
          10.0.11.33
}
```

4. Запустите службу Keepalived:

```
sudo systemctl enable --now keepalived
```

Установка службы Keepalived для кластера MinIO

Перед выполнением инструкции вам нужно выделить в сетевой инфраструктуре организации виртуальный IP-адрес, по которому будет доступен MinIO, и добавить для него DNS-запись. Этот IP-адрес не должен принадлежать ни одному из узлов кластера.

Установку службы Keepalived необходимо проводить с сервера, на котором установлена роль Deployer системы MaxPatrol 10.

- Чтобы установить службу Keepalived:

  1. Установите Ansible и его зависимости:

     ```
     sudo pip3 install ansible==2.9.15
     sudo ansible-galaxy collection install community.crypto
     sudo apt install sshpass
     ```

  2. Перейдите в каталог с установочным комплектом MaxPatrol EDR:

     ```
     cd <Имя каталога>
     ```

  3. Создайте инвентарный файл `keepalived_nodes` со следующим содержимым:

     ```
     [vrrp]
     minio-node-01 ansible_host=<Адрес узла MinIO 1> ansible_user=<Логин учетной записи для авторизации на сервере> ansible_password=<Пароль учетной записи> ansible_sudo=true node_state=MASTER
     minio-node-02 ansible_host=<Адрес узла MinIO 2> ansible_user=<Логин учетной записи для авторизации на сервере> ansible_password=<Пароль учетной записи> ansible_sudo=true
     minio-node-03 ansible_host=<Адрес узла MinIO 3> ansible_user=<Логин учетной записи для авторизации на сервере> ansible_password=<Пароль учетной записи> ansible_sudo=true
     minio-node-04 ansible_host=<Адрес узла MinIO 4> ansible_user=<Логин учетной записи для авторизации на сервере> ansible_password=<Пароль учетной записи> ansible_sudo=true
     ```

     Примечание. Адреса узлов MinIO необходимо задавать без протокола и порта, например `192.0.2.24` или `minio.example`.

  4. Запустите установку службы:

     ```
     sudo ansible-playbook -i keepalived_nodes ansible/sample_install_keepalived.yml -e vip="<Виртуальный IP-адрес узла MinIO>"
     ```

Установка кластера MinIO

- Чтобы установить кластер MinIO:

  1. Перейдите в каталог с установочным комплектом MaxPatrol EDR:

     ```
     cd <Имя каталога>
     ```

  2. Создайте инвентарный файл `inventory_minio.yml` со следующим содержимым:

     ```
     [minio]
     minio-node-01 ansible_host=<Адрес узла MinIO 1> ansible_user=<Логин учетной записи для авторизации на сервере> ansible_password=<Пароль учетной записи> ansible_sudo=true
     minio-node-02 ansible_host=<Адрес узла MinIO 2> ansible_user=<Логин учетной записи для авторизации на сервере> ansible_password=<Пароль учетной записи> ansible_sudo=true
     minio-node-03 ansible_host=<Адрес узла MinIO 3> ansible_user=<Логин учетной записи для авторизации на сервере> ansible_password=<Пароль учетной записи> ansible_sudo=true
     minio-node-04 ansible_host=<Адрес узла MinIO 4> ansible_user=<Логин учетной записи для авторизации на сервере> ansible_password=<Пароль учетной записи> ansible_sudo=true
     ```

Примечание. Адреса узлов MinIO необходимо задавать без протокола и порта, например `192.0.2.24` или `minio.example`.

3. Запустите установку кластера MinIO:

   ```
   sudo ANSIBLE_HOST_KEY_CHECKING=False ansible-playbook -i inventory_minio.yml /ansible/sample_install_minio_cluster.yml -e minio_s3_domain=<Название DNS-записи, указывающей на IP-адрес узла MinIO>
   ```

Настройка манифеста

- Чтобы настроить манифест:

1. Перейдите в каталог с установочным комплектом MaxPatrol EDR:

   ```
   cd <Имя каталога>
   ```

2. Скопируйте файл `manifest_template.json` в файл `manifest.json`:

   ```
   cp manifest_template.json manifest.json
   ```

3. Откройте файл `manifest.json` для редактирования:

   ```
   sudo nano manifest.json
   ```

4. В блоке `hosts` настройте конфигурацию компонентов (см. раздел 6.2).

   Компонент `api` может находиться на нескольких серверах.

5. В блоках `dbms`, `api`, `edr_update` и `custom_expertise` задайте актуальные значения для параметров `MINIO_ACCESS_KEY`, `MINIO_SECRET_KEY`, `S3Storage_Endpoint`, `Database_ConnectionString`, `POSTGRES_USER` и `POSTGRES_PASSWORD`.

   Для параметра `S3Storage_Endpoint` необходимо задать такое же значение, которое было задано для параметра `minio_s3_domain` при установке кластера MinIO. В строке подключения к PostgreSQL (параметр `Database_ConnectionString`) необходимо исправить значение параметра `Host`. Для получения логина и пароля для подключения к PostgreSQL необходимо на сервере с СУБД выполнить команду `sudo docker inspect <PSQL_STORAGE_CONTAINER_NAME> | grep POSTGRES` (параметр `PSQL_STORAGE_CONTAINER_NAME` зависит от параметров установки кластера MaxPatrol 10).

6. Нажмите клавишу F2 и сохраните изменения в файле.

Установка MaxPatrol EDR

Установка MaxPatrol EDR в отказоустойчивом кластере выполняется так же, как обычная установка (см. раздел 6.4). В команде на запуск необходимо использовать параметры `--use-manifest`, `--cluster`, `--wan-hostname` и `--wan-port`:

```
sudo ./edr_installer --use-manifest manifest.json --cluster --wan-hostname <Виртуальный IP-адрес кластера с управляющим сервером> --wan-port <Порт управляющего сервера>
```

См. также

Установка MaxPatrol EDR (см. раздел 6.4)

7. 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`.

> **Внимание!** Обновление рекомендуется выполнять только с предыдущей версии. Например, вы можете обновить MaxPatrol EDR до версии 8.0 с версии 7.2. Если вам нужно обновить более раннюю версию, обновление необходимо выполнять в несколько этапов (7.1 → 7.2 → 8.0). После обновления с пропуском версии может потребоваться переустановка всех агентов.

> **Внимание!** Перед обновлением MaxPatrol EDR до версии 8.0 рекомендуется создать резервную копию баз данных, выполнив на управляющем сервере команду `docker exec storage-postgres.EDR-Application.EDR bash -c 'pg_dumpall -p 5431' > /opt/db_backup.sql`. Также рекомендуется создать резервную копию конфигурации (см. раздел 22.1).

Перед обновлением нужно обновить все агенты до последней версии (см. раздел 15.4.2), которая поддерживается текущей версией сервера, а также убедиться, что серверы соответствуют 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.

> **Примечание.** Если роль Deployer системы MaxPatrol 10 установлена отдельно от компонента MP 10 Core, то на сервере с этой ролью вам нужно проверить наличие скрипта `auto-approve-registration.sh` в каталоге `/var/lib/deployed-roles/mc-application/managementandconfiguration-<Идентификатор>/tools/` (если версия MaxPatrol 10 27.2), каталога с сертификатами `/var/lib/deployed-roles/mp10-application/core-<Идентификатор>/certs/` и права доступа к ним (см. раздел 6.4).

- Чтобы обновить MaxPatrol EDR:

  1. Перейдите в каталог с установочным комплектом:
     ```
     cd edr-installer/
     ```
  2. Запустите установочный скрипт и дождитесь завершения обновления:
     ```
     sudo ./edr_installer
     ```

     > **Примечание.** Если вы запускаете обновление с сервера, на котором не установлен MaxPatrol EDR, то вам нужно скопировать в каталог с установочным комплектом файл `manifest.json` с управляющего сервера и запустить установочный скрипт с параметром `--use-manifest manifest.json`.

3. Если вы используете PT MC версии 101.1 или выше, выберите способ лицензирования (см. раздел 4).
4. Удалите установочный комплект и архив с ним:

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

   MaxPatrol EDR обновлен.

После обновления MaxPatrol EDR необходимо выйти из системы и заново войти.

Особенности обновления MaxPatrol EDR в отказоустойчивом кластере до версии 8.0

Перед обновлением MaxPatrol EDR в отказоустойчивом кластере до версии 8.0 на всех узлах с управляющим сервером нужно установить и настроить службу Keepalived (см. раздел 6.7). В команде запуска установочного скрипта необходимо использовать параметры `--use-manifest`, `--cluster`, `--wan-hostname` и `--wan-port`:

```
sudo ./edr_installer --use-manifest manifest.json --cluster --wan-hostname
<Виртуальный IP-адрес кластера с управляющим сервером> --wan-port <Порт управляющего
сервера>
```

См. также

Настройка обновления MaxPatrol EDR с локального зеркала (см. раздел 9)

Лицензирование (см. раздел 4)

8. 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, правила корреляции и хеш-суммы подозрительных файлов.

> **Примечание.** Обновление модулей и экспертизы доступно при наличии действующей лицензии.

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 последнее сообщение будет `done`. Вы можете проверить его с помощью команды `sudo docker logs modules.EDR-Application.EDR`.

9. Настройка обновления MaxPatrol EDR с локального зеркала

MaxPatrol EDR может работать на сервере в изолированном от интернета сегменте сети. В зависимости от политики информационной безопасности организации вы можете реализовать две схемы обновления MaxPatrol EDR.

Один локальный сервер обновлений

Если из изолированного сегмента организации есть доступ в интернет через прокси-сервер, то вы можете настроить в нем локальное зеркало обновлений. Это зеркало будет загружать обновления с сервера обновлений Positive Technologies.

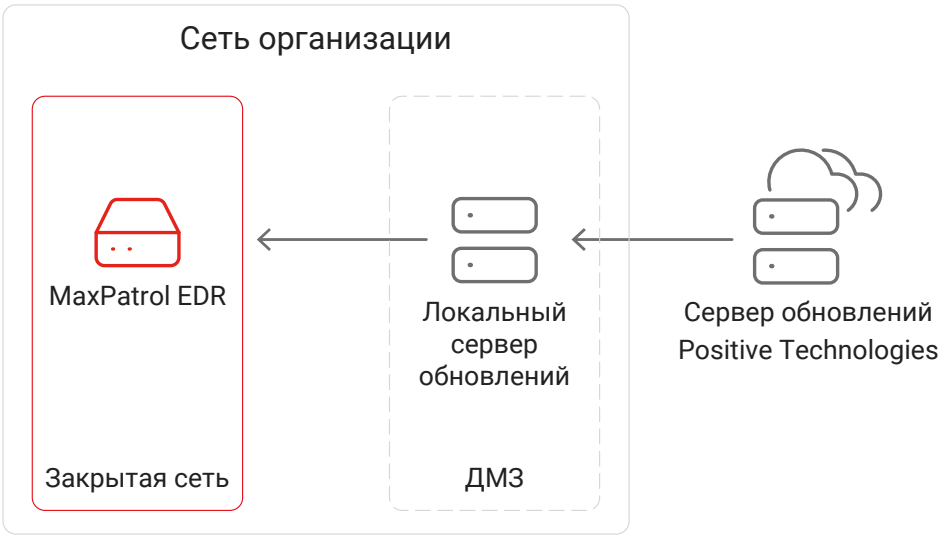

Рисунок 2. Обновление MaxPatrol EDR с использованием одного локального сервера обновлений

Для настройки обновлений MaxPatrol EDR с локального зеркала вам нужно:

1. Установить локальный сервер обновлений (см. раздел 9.3).
2. Настроить локальный сервер обновлений (см. раздел 9.4).
3. Активировать лицензию на локальном сервере обновлений (см. раздел 9.5).
4. Настроить подключение продукта к локальному серверу обновлений (см. раздел 9.6).

Связка локальных серверов обновлений

Если MaxPatrol EDR установлен в изолированном от интернета сегменте сети, то вы можете реализовать схему обновления с двумя локальными серверами обновлений: один в изолированном сегменте сети рядом с MaxPatrol EDR, другой — в демилитаризованной зоне (ДМЗ). Зеркало в ДМЗ будет загружать обновления с сайта Positive Technologies. Для передачи

обновлений в закрытый сегмент сети вы можете либо вручную копировать их при помощи внешнего носителя, либо настроить автоматическую передачу обновлений, если между зеркалами есть сетевое взаимодействие.

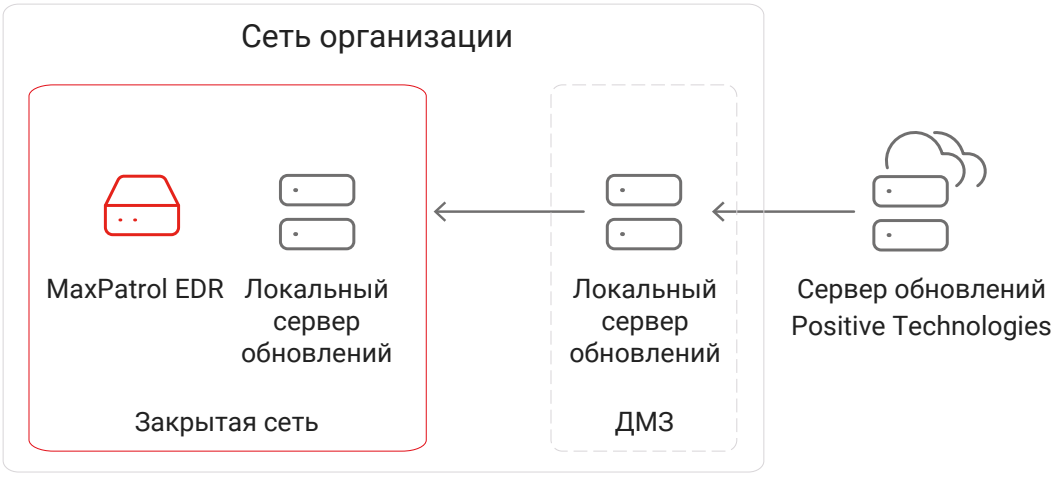

Рисунок 3. Обновление MaxPatrol EDR с использованием двух локальных серверов обновлений

Для настройки обновлений MaxPatrol EDR с локального зеркала вам нужно:

1. Установить два локальных сервера обновлений (см. раздел 9.3): один в изолированном сегменте сети рядом с MaxPatrol EDR, другой — в ДМЗ.
2. Настройте оба локальных сервера обновлений (см. раздел 9.4).
3. Активировать приобретенную вашей организацией лицензию (см. раздел 9.5) на сервере обновлений, установленном в ДМЗ.
4. Если между локальными серверами обновлений есть сетевое взаимодействие и необходимо автоматизировать процедуру обновления, настроить подключение зеркала в изолированном сегменте к зеркалу в ДМЗ (см. раздел 9.8).
5. Настроить подключение продукта к локальному серверу обновлений в изолированном сегменте (см. раздел 9.6).

В этом разделе

9.1. Аппаратные и программные требования

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.

9.2. 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
   ```

9.3. 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 9.1).

— Распаковать архив с установщиком локального сервера обновлений (см. раздел 9.2).

► 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`.

9.4. 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. Сертификат должен отвечать следующим требованиям:

— соответствовать формату 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;

— содержать в расширении Subject Alternative Name (SAN) запись о доменном имени или IP-адресе сервера с установленным веб-интерфейсом продукта;

— если в цепочке между корневым сертификатом и сертификатами компонентов и систем есть промежуточные сертификаты — включать в себя всю цепочку сертификатов.

► 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. В содержимое блока параметров `products` добавьте репозитории MaxPatrol EDR.

   Список репозиториев приведен в приложении (см. приложение Б).
4. Если необходимо настроить скачивание обновлений для компонентов MaxPatrol EDR, в секции `products` → `MP.EDR` укажите значения параметров скачивания:
   - В параметре `count_number_on_version_parse` укажите количество старших разрядов в номере версии, которые определяют номер релиза. Например, при значении 2 для версии 6.0.0.2166 номером релиза будет 6.0.
   - В параметре `minimal_release` укажите номер самого раннего релиза, для которого необходимо скачивать обновления. Например, при значении 6.0 будут скачиваться обновления для релизов 6.0 и выше.
   - В параметре `store_release_versions` укажите количество версий, которое нужно скачивать и хранить на сервере для каждого релиза. Например, если выпущены версии 5.1.0.1682, 5.1.0.1830, 6.0.0.2166, 6.1.0.2344, при значении 2 на сервере будут храниться для релиза 5.1 — версии 5.1.0.1682 и 5.1.0.1830, для релиза 6.0 — версия 6.0.0.2166, для релиза 6.1 версия 6.1.0.2344.
5. Если локальный сервер обновлений должен подключаться к интернету через прокси-сервер, в качестве значения параметра `proxy` введите адрес (и при необходимости) порт прокси-сервера.
6. Если прокси-сервер требует аутентификации, укажите логин и пароль для подключения в параметрах `proxy-user` и `proxy-password` соответственно.
7. Сохраните изменения в файле `/etc/pt-update-mirror/config.json`.
8. Перезапустите локальный сервер обновлений:
   ```
   sudo systemctl restart pt-update-mirror.service
   ```

9.5. 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. Если управление лицензированием осуществляется в MaxPatrol EDR, то активация выполняется с помощью файла лицензии `license-access-token.key`. Вы можете найти этот файл в архиве, который вам прислали при заказе лицензии. При использовании нового способа лицензирования через PT MC вам потребуется ZIP-файл с лицензиями.

Лицензирование в PT MC

- Чтобы активировать лицензию на локальном сервере обновлений,

  выполните одно из действий:

  - Если требуется, чтобы локальный сервер обновлений получал данные от сервера обновлений через интернет, выполните команду:

    ```
    sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --offline-pack <Путь к ZIP-файлу с лицензиями> --update-server https://update.ptsecurity.ru
    ```

  - Если требуется, чтобы локальный сервер обновлений, установленный в закрытом сегменте сети, автоматически получал данные от локального сервера, установленного в демилитаризованной зоне, выполните команду:

    ```
    sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --offline-pack <Путь к ZIP-файлу с лицензиями>
    ```

Лицензирование в MaxPatrol EDR

- 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
  ```

9.6. 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 9.7).

9.7. 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. Сертификаты должны иметь формат PEM и расширение `.crt`.

- Чтобы добавить самоподписанные сертификаты в список доверенных:

1. Скопируйте файлы сертификатов в каталог `/usr/local/share/ca-certificates` на управляющем сервере MaxPatrol EDR.
2. Обновите список доверенных сертификатов в операционной системе:
   ```
   sudo update-ca-certificates
   ```
3. Создайте каталог `/etc/docker/certs.d/<IP-адрес или доменное имя локального сервера обновлений>:8743`.
4. Скопируйте файлы сертификатов в созданный каталог.
5. Если MaxPatrol EDR уже установлен, добавьте файл `cert.crt` к остальным сертификатам:
   ```
   cat /usr/local/share/ca-certificates/cert.crt >> /opt/edr/certs/ca-certificates.crt
   ```
6. Перезапустите компонент Docker:
   ```
   systemctl restart docker
   ```

9.8. Настройка автоматического переноса обновлений в закрытый сегмент сети

Если между локальными серверами обновлений есть сетевое взаимодействие, вы можете настроить подключение зеркала в изолированном сегменте к зеркалу в демилитаризованной зоне. Это позволит автоматически переносить обновления с сайта Positive Technologies в MaxPatrol EDR через цепочку локальных серверов обновлений.

- Чтобы настроить автоматический перенос обновлений в закрытый сегмент сети:

  1. На локальном сервере обновлений в изолированном сегменте откройте файл `/etc/pt-update-mirror/config.json`:
     ```
     sudo nano /etc/pt-update-mirror/config.json
     ```
  2. В качестве значения параметра `update-server` введите адрес локального сервера обновлений в демилитаризованной зоне, например:
     ```
     "update-server": "https://mirror-dmz.example.com",
     ```
     Внимание! Подключение одного зеркала к другому возможно только по протоколу HTTPS.
  3. Если подключение выполняется через прокси-сервер, настройте параметры подключения к нему (см. раздел 9.4).
  4. Сохраните изменения в файле `/etc/pt-update-mirror/config.json`.
  5. Перезапустите локальный сервер обновлений:
     ```
     sudo systemctl restart pt-update-mirror.service
     ```

9.9. Ручной перенос обновлений MaxPatrol EDR в закрытый сегмент сети

Если между локальными серверами обновлений отсутствует сетевое взаимодействие, вам нужно вручную перенести обновления в закрытый сегмент сети для последующего обновления MaxPatrol EDR.

- Чтобы вручную перенести обновления в закрытый сегмент сети:

  1. На локальном сервере обновлений в демилитаризованной зоне запустите получение обновлений с глобального сервера обновлений Positive Technologies:
     ```
     sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository update
     ```
  2. Запустите экспорт репозитория с обновлениями в файл:
     ```
     sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository export <Название файла>.tgz
     ```
  3. Скопируйте с помощью внешнего носителя полученный файл архива в каталог, принадлежащий пользователю pt-update-mirror, на локальном сервере обновлений в закрытом сегменте сети.
  4. На локальном сервере обновлений в закрытом сегменте сети импортируйте обновления из скопированного файла архива:
     ```
     sudo opt/pt/pt-update-mirror/bin/pt-update-mirror repository import <Путь к архиву>/
     <Название архива>.tgz
     ```

10. Удаление MaxPatrol EDR

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

- Чтобы удалить MaxPatrol EDR,

  на сервере с установленным MaxPatrol EDR выполните команду `edr-purge` и подтвердите удаление.

См. также

Удаление MaxPatrol EDR завершилось с ошибкой (см. раздел 23.7)

11. 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 **Войти**.

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

12. 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 дополнительные роли в PT MC. Например, вы можете скопировать одну из стандартных ролей и отключить для нее возможность реагировать на угрозы (см. приложение Г).

Внимание! Для работы с MaxPatrol EDR пользователю также должна быть назначена одна из стандартных ролей MaxPatrol 10.

Таблица 21. Стандартные роли пользователей и доступные функции

Страница продукта	**Администратор**	**Оператор**	**Разработчик**
	Доступные функции		
Серверы агентов	Просмотр списка серверов агентов и их карточек		
	Изменение параметров серверов	—	
Агенты	Просмотр списка агентов и их карточек		
	Ручное реагирование на угрозы		
	Операции с агентами		—
Политики	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		—
Шаблоны политик	Просмотр списка шаблонов		
	Импорт, экспорт и удаление шаблонов	—	
Группы агентов	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

Страница продукта	Администратор	Оператор	Разработчик
	Доступные функции		
Лицензии	Просмотр загруженных лицензий		
	Генерация фингерпринта	—	
	Загрузка и активация лицензии	—	
Резервное копирование и восстановление	Создание резервной копии, импорт и восстановление конфигурации	—	
Планировщик задач	Управление задачами	—	
Дистрибутивы агентов	Скачивание дистрибутивов	—	
Наборы экспертизы	Управление наборами экспертизы		

13. Интерфейс MaxPatrol EDR

После входа в веб-интерфейс открывается страница **Агенты**.

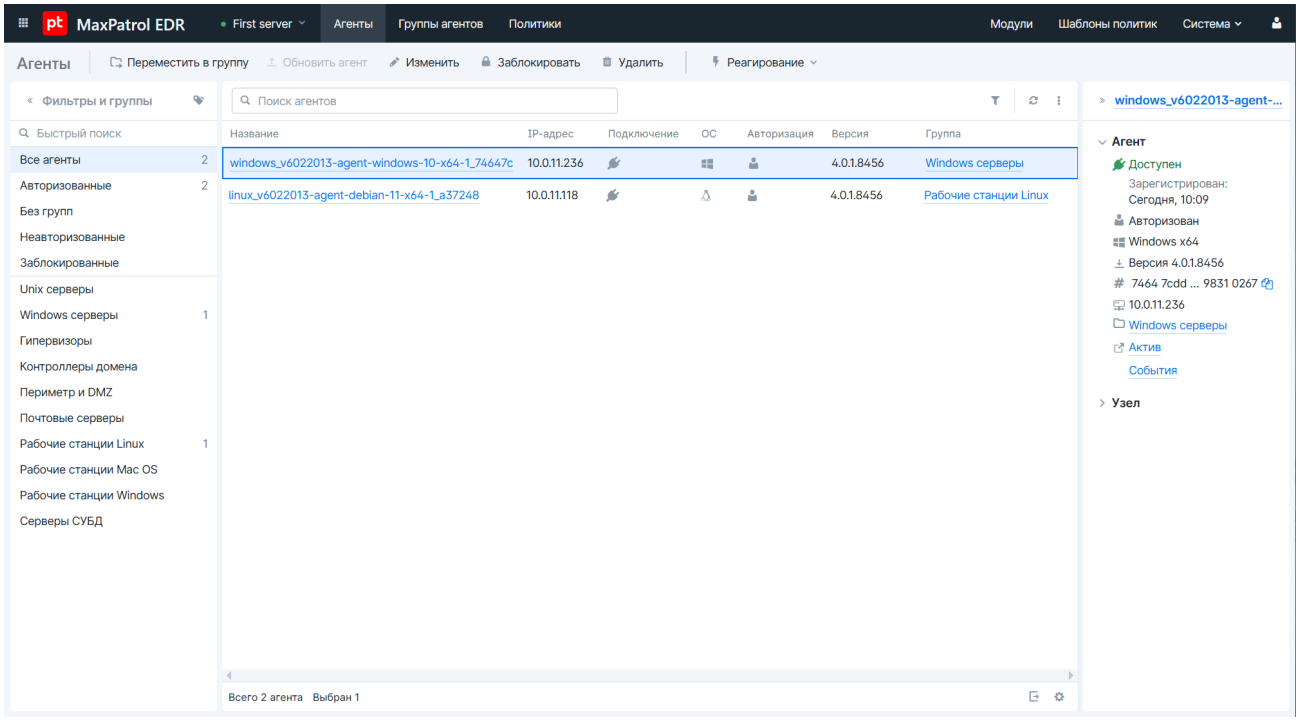

Рисунок 4. Страница **Агенты EDR**

Веб-интерфейс MaxPatrol EDR состоит из главного меню, панели инструментов и рабочей области. Главное меню содержит раскрывающийся список для выбора сервера агентов (если их в системе несколько), разделы для перехода к страницам продукта, а также кнопки:

— для перехода из MaxPatrol EDR к другим приложениям;

— для выбора языка интерфейса и выхода из MaxPatrol EDR.

Панель инструментов содержит кнопки. С их помощью вы можете выполнять действия (в том числе групповые) с данными, представленными в рабочей области.

14. Управление серверами агентов

В системе может быть несколько серверов агентов. Для каждого сервера агентов уникален набор агентов, групп и политик. Список всех серверов агентов отображается в веб-интерфейсе продукта на странице **Серверы агентов**. При выборе сервера в списке откроется его карточка. В карточке отображается количество подключенных и недоступных агентов и информация о компоненте MaxPatrol SIEM Server, на котором обрабатываются события. Также в карточке вы можете настроить шаблон для названий агентов и максимальное количество агентов, на которых одновременно будут обновляться набор модулей и пакет экспертизы.

Настройка обновления набора модулей и пакета экспертизы

При сильной загрузке канала связи между сервером агентов и агентами система может работать нестабильно. Вы можете ограничить максимальное количество агентов, на которых будут одновременно обновляться набор модулей и пакет экспертизы (см. раздел 8). Это позволит контролировать загрузку канала.

- Чтобы настроить обновление:

  1. В главном меню в раскрывающемся списке серверов агентов нажмите **Управление серверами агентов**.
  2. Выберите сервер агентов.
  3. Напротив параметра **Сколько агентов обновлять одновременно** нажмите .
  4. Введите количество агентов и нажмите **Применить**.

Настройка шаблона для названий агентов

Вы можете настроить шаблон для названий агентов, которые будут подключаться к выбранному серверу агентов. Изменение шаблона не затронет названия уже подключенных агентов.

- Чтобы настроить шаблон названия агентов:

  1. В главном меню в раскрывающемся списке серверов агентов нажмите **Управление серверами агентов**.
  2. Выберите сервер агентов.
  3. Напротив параметра **Шаблон названия агентов** нажмите .
  4. Задайте необходимый шаблон и нажмите **Применить**.

Выбор сервера агентов

Если в системе используется несколько серверов агентов, вы можете переключаться между ними в веб-интерфейсе. 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 раскрывающемся списке серверов агентов выберите нужный вам сервер.

Удаление сервера агентов

Вы можете удалить сервер агентов из системы. Если к этому серверу агентов подключены агенты, которые вы хотите сохранить, вам нужно переподключить их к другому серверу (см. раздел 15.3).

- Чтобы удалить сервер агентов:

  1. На управляющем сервере MaxPatrol EDR выполните команду `sudo edr-compose exec edr-cli bin/edr service remove "<Название сервера агентов>"`.

     Примечание. Название сервера агентов задается в манифесте (см. раздел 6.2) при установке MaxPatrol EDR.

  2. Удалите из манифеста информацию о сервере агентов (см. раздел 6.3).

15. Работа с агентами

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

В этом разделе

15.1. Об агентах

Агент EDR (далее также — агент) — это приложение, которое необходимо установить на конечном устройстве (см. раздел 15.2) для обнаружения угроз и реагирования на них. После установки вам необходимо авторизовать агент и добавить его в группу, на которую назначена хотя бы одна политика (см. раздел 17).

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 18.1) 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**. 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 (см. раздел 17)

Установка агента на конечное устройство (см. раздел 15.2)

15.2. 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 пакет установки.

> **Внимание!** После установки агента необходимо добавить папку, в которую он был установлен, в исключения антивируса.

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

- Чтобы скачать дистрибутив агента:

  1. Перейдите в веб-интерфейс MaxPatrol EDR.
  2. В главном меню выберите **Система** → **Дистрибутивы агентов**.
  3. Нажмите кнопку, соответствующую версии ОС и архитектуре, и в раскрывшемся списке выберите необходимый дистрибутив.

  Дистрибутив агента сохранен на вашем компьютере.

Далее приведены инструкции по установке агента на конечное устройство.

В этом разделе

Установка агента в Windows (см. раздел 15.2.1)

Установка агента в Linux (см. раздел 15.2.2)

Установка агента в macOS (см. раздел 15.2.3)

15.2.1. 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 windows_<Архитектура>_agent.msi VXSERVER_CONNECT=wss://<Адрес сервера агентов>:<Порт>
     ```

     Примечание. Порт сервера агентов по умолчанию — 8443.

     Примечание. Если вы хотите установить агент в виртуальной среде на сервере, на котором уже установлен агент, вам нужно добавить в команду запуска параметр `AGENT_ID_SALT=<Любое значение>`.

15.2.2. 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 операционных системах с версией библиотеки glibs ниже 2.28 (Astra Linux, Red Hat Enterprise Linux 7, AlterOS Desktop 7.5) рекомендуется использовать дистрибутив с именем `linux_<Архитектура>_agent-bundle`, в остальных ОС — стандартный.

> **Примечание.** Для установки агента в операционной системе «Альт Сервер» 10.2 необходимо использовать отдельный RPM-пакет (доступен на странице **Дистрибутивы агентов**).

- 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 ./
     linux_<Архитектура>_agent.deb
     ```

     Примечание. Порт сервера агентов по умолчанию — 8443.

     Примечание. Если вы хотите установить агент в виртуальной среде на сервере, на котором уже установлен агент, вам нужно добавить в команду запуска параметр `AGENT_ID_SALT=<Любое значение>`.

- Чтобы установить агент из RPM-пакета:

  1. Перейдите в каталог с RPM-пакетом:

     ```
     cd <Имя каталога>
     ```

  2. Если установка выполняется на конечном устройстве, с которого недоступны пакетные менеджеры Linux, установите пакеты libpthread, libnsl и libcrypto.

  3. Если пакет `initscripts` не установлен, установите его:

     ```
     yum install -y initscripts
     ```

  4. Запустите установку агента:

     Если установка выполняется на конечном устройстве, с которого доступны пакетные менеджеры Linux (рекомендуемый вариант):

     ```
     sudo VXSERVER_CONNECT=wss://<Адрес сервера агентов>:<Порт> yum --nogpgcheck
     localinstall ./linux_<Архитектура>_agent.rpm
     ```

     Если установка выполняется на конечном устройстве, с которого недоступны пакетные менеджеры Linux:

     ```
     sudo VXSERVER_CONNECT=wss://<Адрес сервера агентов>:<Порт> rpm -i ./
     linux_<Архитектура>_agent.rpm
     ```

     Если установка выполняется в ОС «Альт Сервер»:

     ```
     sudo VXSERVER_CONNECT=wss://<Адрес сервера агентов>:<Порт> apt-get install ./
     linux_amd64_agent.rpm
     ```

Примечание. Порт сервера агентов по умолчанию — 8443.

Примечание. Если вы хотите установить агент в виртуальной среде на сервере, на котором уже установлен агент, вам нужно добавить в команду запуска параметр `AGENT_ID_SALT=<Любое значение>`.

15.2.3. 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 ./darwin_<Архитектура>_agent.pkg -target /Library/"
   ```

   Примечание. Порт сервера агентов по умолчанию — 8443.

   Примечание. Если вы хотите установить агент в виртуальной среде на сервере, на котором уже установлен агент, вам нужно добавить в команду запуска параметр `AGENT_ID_SALT=<Любое значение>`.

15.3. Массовая установка и удаление агентов

Вы можете массово устанавливать и удалять агенты в Windows и Linux с помощью плейбука Ansible, который поставляется вместе с дистрибутивом MaxPatrol EDR.

Программные требования для массовых операций с агентами

На узле, с которого запускается плейбук, должны быть установлены следующие компоненты:

— Ansible Core версии 2.15.13 или выше;

— Python 3.9 или выше;

— pywinrm (только для операций в Windows);

— коллекция Ansible.Windows (только для операций в Windows).

На узлах под управлением Linux, на которых будет выполняться установка агентов, должен быть установлен Python версии 3.5 или выше. На узлах под управлением Windows должна быть настроена служба WinRM.

Запуск плейбука возможен с любого узла, который удовлетворяет требованиям и который имеет сетевой доступ по портам SSH (в Linux, по умолчанию 22) или WinRM (в Windows, по умолчанию 5985) к узлам, заданным в инвентарном файле.

Подготовка инвентарного файла

Перед установкой агентов вам нужно в каталоге с установочным комплектом MaxPatrol EDR создать инвентарный файл в формате YAML с параметрами узлов, на которых будут установлены агенты, и серверов агентов, к которым они будут подключены. Структура инвентарного файла:

```
all:
 children:
   <Любое название группы узлов 1>:
     hosts:
       <IP-адрес или полное доменное имя узла 1>:
       <IP-адрес или полное доменное имя узла 2>:
       <IP-адрес или полное доменное имя узла 3>:
     vars:
       vxserver: "<IP-адрес сервера агентов 1>:<Порт>"
   <Любое название группы узлов 2>:
     hosts:
       <IP-адрес или полное доменное имя узла 4>:
       <IP-адрес или полное доменное имя узла 5>:
       <IP-адрес или полное доменное имя узла 6>:
         ansible_connection: winrm
         ansible_port: 5985
         ansible_winrm_transport: basic
         ansible_winrm_server_cert_validation: ignore
     vars:
       vxserver: "<IP-адрес сервера агентов 2>:<Порт>"
```

Внимание! Для всех узлов под управлением Windows необходимо указывать дополнительные параметры подключения: `ansible_connection`, `ansible_port`, `ansible_winrm_transport`, `ansible_winrm_server_cert_validation`.

Получение токена доступа

Для массовой установки агентов нужен токен доступа к MaxPatrol EDR.

- Чтобы создать токен доступа:

  1. На управляющем сервере перейдите в каталог `/opt/edr/`.
  2. Запустите скрипт для генерации токена:

     ```
     sudo ./register_client --privileges pt.edr.ui.agents.downloads --client-id deployagents
     ```

Установка агентов

- Чтобы запустить установку агентов:

  1. Перейдите в каталог с установочным комплектом.
  2. Запустите плейбук:

     ```
     sudo ansible-playbook -i <Путь до инвентарного файла> ansible/sample_agent_install.yml -e api_addr="<IP-адрес или доменное имя узла с управляющим сервером>:8444" -e edr_access_token="<Токен доступа>" -u root -k
     ```

     Примечание. При необходимости в команду запуска вы можете добавить параметры `-e agent_id_salt=True` (при установке агента в виртуальной среде на узле, на котором уже установлен агент) и `-e force_agent_update=True` (для принудительной установки агента на узлах, на которых уже установлен агент).

Удаление агентов

С помощью плейбука вы можете массово удалить на узлах все агенты, параметры которых заданы в инвентарном файле.

- Чтобы запустить удаление агентов:

  1. Перейдите в каталог с установочным комплектом.
  2. Запустите плейбук:

     ```
     sudo ansible-playbook -i <Путь до инвентарного файла> ansible/sample_agent_install.yml -e package_action="absent" -u root -k
     ```

Переподключение агентов к другому серверу агентов

С помощью плейбука вы можете массово переподключить все агенты на Linux, параметры которых заданы в инвентарном файле, к другому серверу агентов.

- Чтобы переподключить агенты к другому серверу агентов:

  1. Перейдите в каталог с установочным комплектом.
  2. Запустите плейбук:

     ```
     sudo ansible-playbook -i <Путь до инвентарного файла> ansible/sample_agent_install.yml -e package_action="change_vxserver" -e vxserver="<Адрес нового сервера агентов>:<Порт>" -u root -k
     ```

15.4. Управление агентами

Далее даны инструкции по управлению агентами в MaxPatrol EDR.

В этом разделе

15.4.1. 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 16).

- Чтобы авторизовать агент:

  1. В главном меню выберите **Агенты**.
  2. Выберите фильтр **Неавторизованные**.
  3. Выберите агент.

     Примечание. Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.
  4. Нажмите **Переместить в группу**.
  5. Выберите группу, в которую вы хотите добавить агент, или введите название новой группы.
  6. Нажмите **Переместить**.

15.4.2. Обновление агента

Если для агента доступно обновление, то его версия в таблице будет выделена желтым цветом. Вы можете обновлять только авторизованные агенты. Обновление выполняется только до следующей версии. Рекомендуется обновлять агенты до последней доступной версии.

- Чтобы обновить агент:

  1. В главном меню выберите **Агенты**.
  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.

15.4.3. 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 выберите **Агенты**.
  2. Выберите агент.

     Примечание. Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.
  3. Нажмите **Переместить в группу**.
  4. Выберите группу, в которую вы хотите добавить агент, или введите название новой группы.
  5. Нажмите **Переместить**.

15.4.4. 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 выберите **Агенты**.
  2. Выберите агент.

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

15.4.5. 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 15.4.6).

- Чтобы заблокировать агент:

  1. В главном меню выберите **Агенты**.
  2. Выберите агент.

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

См. также

Добавление агента в группу (см. раздел 15.4.6)

15.4.6. 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 выберите **Агенты**.
  2. Выберите фильтр **Агенты без группы** или **Заблокированные**.
  3. Выберите агент.

     Примечание. Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.
  4. Нажмите **Переместить в группу**.
  5. Выберите группу, в которую вы хотите добавить агент, или введите название новой группы.
  6. Нажмите **Переместить**.

15.4.7. 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 выберите **Агенты**.
  2. Выберите агент.

     Примечание. Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.
  3. Нажмите **Удалить** и подтвердите удаление.

15.5. Настройка хранения и передачи системных событий

Системные события, которые собирают модули «WinEventLog: сбор данных из журнала событий Windows», «ETW: трассировка событий Windows» 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.

> **Внимание!** Для отправки системных событий в MaxPatrol SIEM на агентах группы должен быть установлен и включен модуль «Нормализатор». Системные события, для которых нет правил нормализации, будут отправлены в необработанном виде.
>
> **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 выберите **Группы агентов**.
2. Выберите группу.
3. Нажмите **Изменить**.
4. В блоке параметров **Отправлять системные события** выберите, куда нужно отправлять системные события со всех агентов группы.

   Если вы не обрабатываете события в MaxPatrol SIEM и хотите отправлять их только во внешнюю систему по протоколу syslog, выберите **Только на сервер агентов**. В этом случае в политике, назначенной на группу, должен быть настроен модуль «Отправка событий на syslog-сервер» (см. раздел 19.6.3).
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 **Сохранить**.

См. также

Отправка событий на syslog-сервер (см. раздел 19.6.3)

15.6. Ограничение скорости передачи данных на агент

При сильной загрузке канала связи между агентом и сервером агентов модули могут работать нестабильно. Вы можете ограничить скорость передачи данных на агент, чтобы контролировать загрузку канала. Скорость ограничивается для всех агентов группы.

- Чтобы ограничить скорость передачи данных на агент:

  1. В главном меню выберите **Группы агентов**.
  2. Выберите группу.
  3. Нажмите **Изменить**.
  4. В поле **Макс. скорость передачи данных на агент** укажите максимальную скорость передачи данных с сервера агентов на агент.
  5. Нажмите **Сохранить**.

15.7. Удаление агента с конечного устройства

Этот раздел содержит инструкции по удалению агента с конечного устройства.

В этом разделе

Удаление агента в Windows (см. раздел 15.7.1)

Удаление агента в Linux (см. раздел 15.7.2)

Удаление агента в macOS (см. раздел 15.7.3)

15.7.1. 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.

15.7.2. Удаление агента в Linux

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

  выполните команду `dpkg --purge vxagent`.

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

  выполните команду `rpm -e vxagent`.

- Чтобы удалить агент, который был установлен из RPM-пакета в ОС «Альт Сервер»,

  выполните команду `apt-get remove --purge vxagent`.

15.7.3. Удаление агента в macOS

- Чтобы удалить агент в macOS,

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

Агент удален.

16. Управление группами агентов

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

В этом разделе

16.1. О группах агентов

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 17), назначенные на группу.

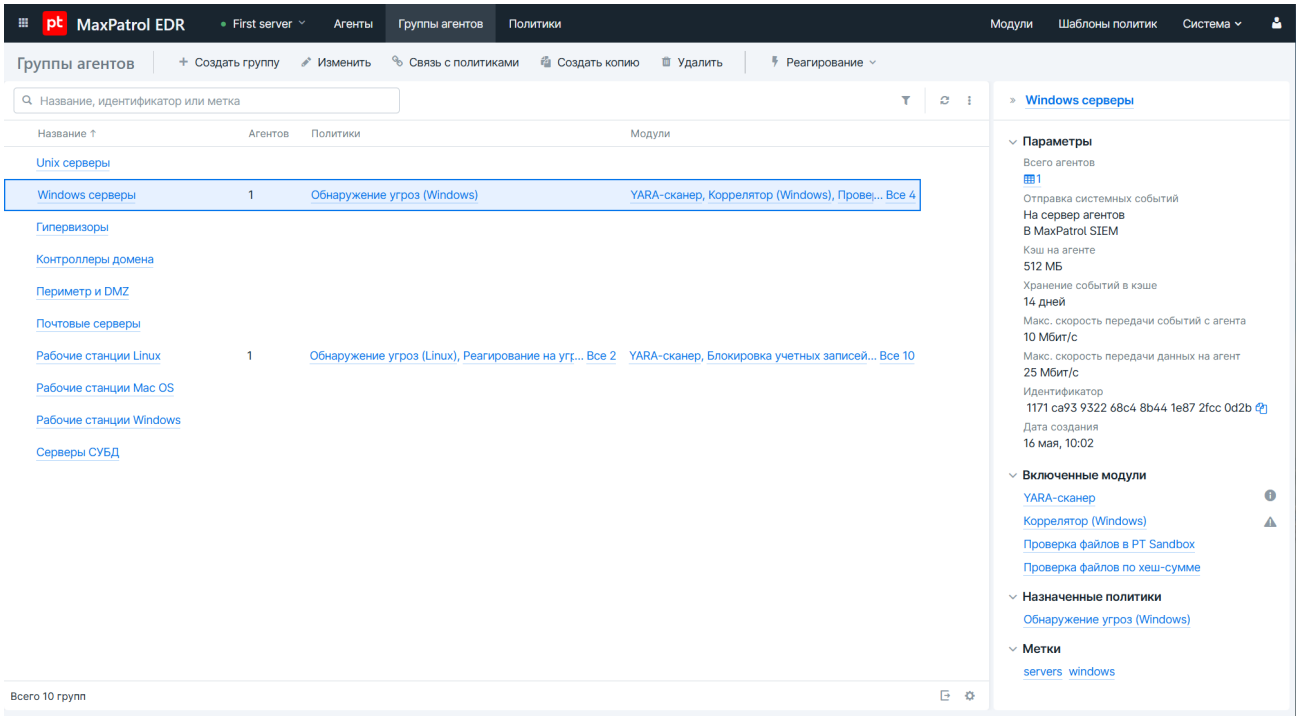

Рисунок 5. Страница **Группы агентов EDR**

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.

16.2. Создание группы

- Чтобы создать группу:

  1. В главном меню выберите **Группы агентов**.
  2. Нажмите кнопку **Создать группу**.
  3. Введите название группы.
  4. 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. В поле **Макс. скорость передачи данных на агент** укажите максимальную скорость передачи данных с сервера агентов на агент.
  10. Нажмите кнопку **Добавить**.

Вы также можете копировать группы (см. раздел 16.3) или создавать их при перемещении агентов (см. раздел 15.4.3).

16.3. 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 выберите **Группы агентов**.
  2. Выберите группу.
  3. Нажмите **Создать копию**.
  4. Введите название группы.
  5. Выберите существующие метки для быстрого поиска группы или задайте свои.
  6. Если требуется, измените параметры хранения и передачи системных событий (см. раздел 15.5).
  7. Нажмите **Создать**.

16.4. 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 выберите **Группы агентов**.
  2. Выберите группу.
  3. Нажмите **Удалить** и подтвердите удаление.

17. Управление политиками

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

В этом разделе

17.1. О политиках

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. Список всех политик отображается на странице **Политики**.

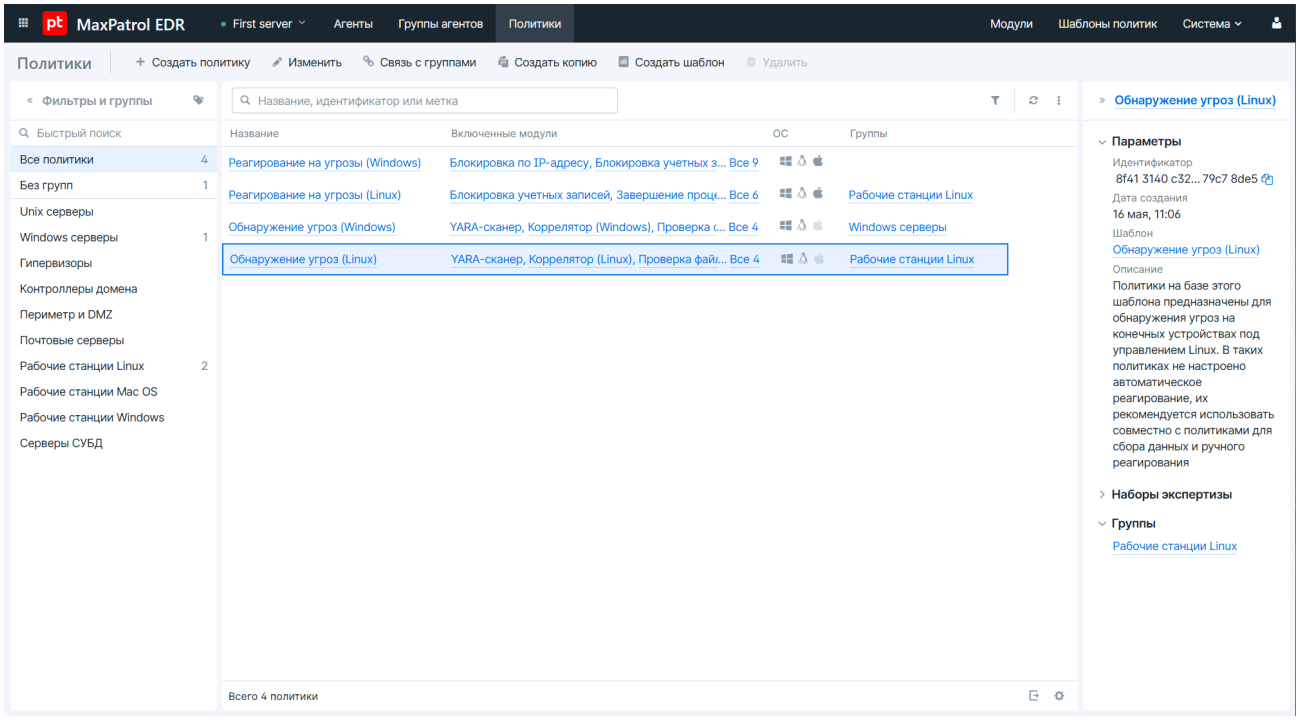

Рисунок 6. Страница **Политики EDR**

При нажатии на название политики откроется карточка политики, в которой вы можете управлять модулями агентов (см. раздел 18), а также просматривать списки:

— зависимостей модулей политики;

— агентов с этой политикой;

— групп, на которые назначена эта политика.

17.2. Шаблоны политик

Вы можете создавать политики из шаблонов. Шаблон политики содержит набор модулей и их конфигурацию для решения определенных задач. В системе есть несколько стандартных шаблонов политик, которые сконфигурированы экспертами Positive Technologies. Вы также можете создавать собственные шаблоны на базе сконфигурированных политик. Такие шаблоны вы можете экспортировать для использования на других серверах агентов или на других установках MaxPatrol EDR. Это позволит вам один раз настроить политику для агентов с похожими характеристиками и распространить ее на все серверы.

Список всех шаблонов политик отображается на странице **Шаблоны политик**.

В этом разделе

17.2.1. Стандартные шаблоны

Таблица 22. Стандартные шаблоны политик

Название	Описание	Модули
Сбор данных (Linux)	Политики на базе этого шаблона предназначены для сбора данных на конечных устройствах под управлением Linux. В шаблоне настроено отслеживание журналов `audit.log` и `vsftpd.log`	«Нормализатор», «Сбор данных из файлов журналов», «Установщик auditd»
Обнаружение угроз (Linux)	Политики на базе этого шаблона предназначены для обнаружения угроз на конечных устройствах под управлением Linux. В таких политиках не настроено автоматическое реагирование, их рекомендуется использовать совместно с политиками для сбора данных и ручного реагирования	«Коррелятор (Linux)», «Проверка файлов по хеш-сумме», «YARA-сканер», «Проверка файлов в PT Sandbox»
Реагирование на угрозы (Linux)	Политики на базе этого шаблона предназначены для ручного реагирования на подозрительные или вредоносные действия на конечных устройствах под управлением Linux. Такие политики необходимо использовать совместно с политиками для сбора данных и обнаружения угроз	«Блокировка учетных записей», «Завершение процессов», «Удаление файлов», «Карантин», «Перенаправление DNS-запросов (sinkholing)»
Обнаружение угроз и реагирование (Linux)	Политики на базе этого шаблона предназначены для обнаружения угроз и автоматического реагирования на конечных устройствах под управлением Linux. Такие политики рекомендуется использовать совместно с политикой для сбора данных	«Коррелятор (Linux)», «Проверка файлов по хеш-сумме», «YARA-сканер», «Проверка файлов в PT Sandbox», «Блокировка учетных записей», «Завершение процессов», «Удаление файлов», «Карантин», «Пере-

Название	Описание	Модули
		направление DNS-запросов (sinkholing)»
Сбор данных с рабочих станций (Windows)	Политики на базе этого шаблона предназначены для сбора данных на рабочих станциях под управлением Windows. В шаблоне настроено отслеживание журналов Security, Kaspersky Endpoint Security, Kaspersky Event Log, Microsoft-Windows-Windows Defender/Operational, Microsoft-Windows-Sysmon/Operational, Microsoft-Windows-PowerShell/Operational, Microsoft-Windows-TaskScheduler/Operational, System, Application	«WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор»
Сбор данных с контроллеров доменов (Windows)	Политики на базе этого шаблона предназначены для сбора данных на контроллерах доменов под управлением Windows. В шаблоне настроено отслеживание журналов Security, Kaspersky Endpoint Security, Kaspersky Event Log, Microsoft-Windows-Windows Defender/Operational, Microsoft-Windows-Sysmon/Operational, Microsoft-Windows-PowerShell/Operational, Microsoft-Windows-TaskScheduler/Operational, System, Application, DhcpAdminEvents, Microsoft-Windows-Dhcp-Server/Operational, Microsoft-Windows-Dhcp-Server/FilterNotifications, Directory Service, DNS Server, Active Directory Web Services, DFS Replication	«WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор»
Сбор данных с серверов (Windows)	Политики на базе этого шаблона предназначены для сбора данных на серверах под управлением Windows. В шаблоне настроено отслеживание журналов Security, Kaspersky Endpoint Security, Kaspersky Event Log, Microsoft-Windows-Windows Defender/Operational, Microsoft-Windows-Sysmon/Operational, Microsoft-Windows-PowerShell/Operational, Microsoft-Windows-TaskScheduler/Operational, System, Application, DhcpAdminEvents, Microsoft-Windows-Dhcp-Server/Operational, Microsoft-Windows-Dhcp-Server/FilterNotifications, Directory Service, DNS Server, Active Directory Web Services, DFS Replication	«WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор»
Обнаружение угроз (Windows)	Политики на базе этого шаблона предназначены для обнаружения угроз на агентах под управлением Windows. В таких политиках не настроено автомати-	«Коррелятор (Windows)», «Проверка

Название	Описание	Модули
	ческое реагирование, их рекомендуется использовать совместно с политиками для сбора данных и ручного реагирования	файлов по хеш-сумме», «YARA-сканер», «Проверка файлов в PT Sandbox»
Реагирование на угрозы (Windows)	Политики на базе этого шаблона предназначены для ручного реагирования на подозрительные или вредоносные действия на конечных устройствах под управлением Windows. Такие политики необходимо использовать совместно с политиками для сбора данных и обнаружения угроз	«Блокировка по IP-адресу», «Блокировка учетных записей», «Завершение процессов», «Удаление файлов», «Карантин», «Перенаправление DNS-запросов (sinkholing)», «Изоляция узлов»
Обнаружение угроз и реагирование (Windows)	Политики на базе этого шаблона предназначены для обнаружения угроз и автоматического реагирования на конечных устройствах под управлением Windows. Такие политики рекомендуется использовать совместно с политикой для сбора данных	«Коррелятор (Windows)», «Проверка файлов по хеш-сумме», «YARA-сканер», «Проверка файлов в PT Sandbox», «Блокировка по IP-адресу», «Блокировка учетных записей», «Завершение процессов», «Удаление файлов», «Карантин», «Перенаправление DNS-запросов (sinkholing)», «Изоляция узлов»

Название	Описание	Модули
Конфигуратор аудита Windows	Политики на базе этого шаблона предназначены для конфигурирования расширенной политики аудита Windows на контроллерах доменов, серверах и рабочих станциях	«Конфигуратор аудита Windows»
Интеграция с MaxPatrol VM	Политики на базе этого шаблона предназначены для сканирования в режиме аудита и отправки результатов в MaxPatrol VM	«Сканирование в режиме аудита (MaxPatrol VM)»

17.2.2. Пользовательские шаблоны

Вы можете создавать шаблоны из сконфигурированных политик. В шаблон войдут все модули из выбранной политики и их конфигурация. Для распространения шаблона вы можете на странице **Шаблоны политик** экспортировать его в файл формата JSON, а затем импортировать на другой сервер агентов или на другую установку MaxPatrol EDR. После создания изменить конфигурацию шаблона невозможно. В этом случае вы можете создать политику на базе этого шаблона, изменить ее конфигурацию и создать на ее основе новый шаблон.

> **Примечание.** Экспортировать шаблон с пользовательскими наборами экспертизы (см. раздел 17.4) невозможно.

Создание шаблона

- Чтобы создать шаблон политики:

  1. В главном меню выберите **Политики**.
  2. Выберите политику, на базе которой вы хотите создать шаблон.
  3. Нажмите **Создать шаблон**.
  4. Введите название шаблона.
  5. Нажмите **Создать**.

Изменение конфигурации политики с помощью шаблона

Вы можете обновить конфигурацию политики, выбрав в ее параметрах новый шаблон. Это может быть полезно, когда вам нужно внести изменения в политики с одинаковой конфигурацией на разных серверах или установках MaxPatrol EDR.

> **Внимание!** После выбора шаблона конфигурация политики полностью изменится, восстановить предыдущую конфигурацию будет невозможно. На агентах, связанных с этой политикой, сначала будут удалены все модули из старой конфигурации, а затем будут установлены модули из выбранного шаблона.

- Чтобы изменить конфигурацию политики:

  1. В главном меню выберите **Политики**.
  2. Выберите политику, в которой вы хотите изменить конфигурацию.
  3. Нажмите **Изменить**.
  4. Выберите новый шаблон.
  5. Нажмите **Сохранить**.

См. также

Пользовательская экспертиза (см. раздел 17.4)

17.3. Создание политики

Вы можете создавать политики на базе шаблонов или пустые. В политиках, которые созданы на базе шаблонов, добавлены модули (см. раздел 18.1) 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 18.4.1), сконфигурировать их (см. раздел 19) и настроить автоматические действия (см. раздел 18.6).

- Чтобы создать политику:

  1. В главном меню выберите **Политики**.
  2. Нажмите **Создать политику**.
  3. Выберите шаблон, на базе которого вы хотите создать политику.

     Примечание. Для создания пустой политики вы можете выбрать значение **Не выбран**.
  4. Введите название политики.
  5. Выберите существующие метки для быстрого поиска политики или задайте свои.
  6. Нажмите **Создать**.

Вы также можете создавать копии существующих политик (см. раздел 17.5).

17.4. Пользовательская экспертиза

В базе знаний PT KB системы MaxPatrol 10 вы можете создавать наборы экспертизы с собственными правилами корреляции, нормализации и табличными списками. Эти наборы вы можете загрузить в MaxPatrol EDR для использования в модулях «Коррелятор» и «Нормализатор». Это позволит адаптировать работу модулей под вашу инфраструктуру.

Например, вы можете исключить ненужные правила для оптимизации нагрузки на конечные устройства или добавить свои правила для обнаружения угроз, характерных для вашего нестандартного ПО.

Если в PT KB внесли изменения в набор, вам нужно обновить его в MaxPatrol EDR. При обновлении набора создается его новая версия. Наборы с несколькими версиями отмечены в списке значком  . В модулях вы можете использовать любую версию набора.

Если правила корреляции в наборе предусматривают заполнение табличных списков, то это будет происходить только в MaxPatrol EDR: в PT KB табличные списки изменены не будут. Кроме того, содержимое табличных списков в MaxPatrol EDR автоматически не обновляется при их изменении в PT KB. В этом случае вам нужно обновить набор экспертизы.

Если вы удалите набор в MaxPatrol EDR, модули продолжат использовать экспертизу из него. Если удаленный набор использовался в шаблонах политик (см. раздел 17.2), их нужно пересоздать.

Загрузка наборов экспертизы

- Чтобы загрузить наборы экспертизы в MaxPatrol EDR:

  1. В главном меню выберите **Система** → **Наборы экспертизы**.
  2. Нажмите **Загрузить**.
  3. Выберите один или несколько наборов.
  4. Нажмите **Загрузить**.

Выбор наборов экспертизы в политике

Для использования экспертизы из ваших наборов их нужно выбрать в параметрах политики с модулями «Коррелятор» и «Нормализатор».

Внимание! Использование пользовательских правил нормализации может повлиять на работу других модулей на агенте в случае, если нормализованное событие не будет содержать необходимые для этих модулей данные.

- Чтобы выбрать наборы экспертизы в политике:

  1. В главном меню выберите **Политики**.
  2. Выберите политику.
  3. Нажмите **Изменить**.
  4. Нажмите **Наборы экспертизы**.
  5. Выберите наборы для модулей.
  6. Нажмите **Сохранить**.

17.5. 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 выберите **Политики**.
  2. Выберите политику.
  3. Нажмите **Создать копию**.
  4. Введите название политики.
  5. Выберите существующие метки для быстрого поиска политики или задайте свои.
  6. Нажмите **Создать**.

17.6. Назначение политики на группу агентов

Для установки модулей на агенты необходимо назначить политику на группу агентов. Одну политику можно назначить на множество групп, а на одну группу — несколько разных политик. 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 18.4.2) в политике или снять политику (см. раздел 17.7) с группы.

- Чтобы назначить политику на группу:

  1. В главном меню выберите **Политики**.
  2. Выберите политику.
  3. Нажмите **Связь с группами**.
  4. Напротив группы, на которую вы хотите назначить политику, нажмите  .

17.7. 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 выберите **Политики**.
  2. Выберите политику.
  3. Нажмите **Связь с группами**.
  4. Напротив группы, с которой вы хотите снять политику, нажмите  .

17.8. 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 выберите **Политики**.
  2. Выберите политику.
  3. Нажмите **Удалить** и подтвердите удаление.

18. Управление модулями агента

Далее приведена основная информация о модулях агента, а также даны инструкции по управлению модулями в политике и системе.

В этом разделе

18.1. 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 18.3).

В MaxPatrol EDR есть шесть типов модулей:

- **Системные модули.** Обеспечивают работу других модулей и агента.
- **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.

См. также

18.2. О безопасности модулей

Для защиты конечных устройств от внедрения вредоносного кода в стандартные модули реализован механизм проверки подписи кода. Этот механизм может быть активирован при установке продукта (см. раздел 6.5). Версия модуля, которая не прошла проверку подписи, не может быть добавлена в политику и установлена на конечных устройствах. Кроме того, система регулярно выполняет проверку уже установленных модулей. При обнаружении несоответствия модуль будет отключен в политике и удален с конечных устройств. Код пользовательских модулей, разрабатываемых в интерфейсе MaxPatrol EDR, также может быть подписан.

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

18.3. 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 .

Вы можете обеспечить зависимость от другого модуля двумя способами:

— добавив необходимый модуль (см. раздел 18.4.1) в политику, которая назначена на группу;

— назначив на группу (см. раздел 17.6) политику, в которой есть необходимый модуль.

Для обеспечения зависимости от версии агента вам нужно обновить агент (см. раздел 15.4.2).

18.4. Управление модулями в политике

Далее приведены инструкции по управлению модулями в политике.

В этом разделе

18.4.1. Добавление модуля в политику

- Чтобы добавить модуль в политику:

  1. В главном меню выберите **Политики**.
  2. Выберите политику.
  3. В списке **Доступны для добавления** выберите модуль.
  4. Нажмите **Добавить**.

  Модуль добавлен в политику. Если политика назначена на группу (см. раздел 17.6), то сразу после добавления модуля он будет автоматически установлен на всех агентах группы.

18.4.2. 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 18.4.3).

- Чтобы отключить модуль в политике:

  1. В главном меню выберите **Политики**.
  2. Выберите политику.
  3. В списке **Включенные** выберите модуль.
  4. Нажмите **Отключить**.

     Внимание! Если политика назначена на группу (см. раздел 17.6), то сразу после отключения модуль будет автоматически удален со всех агентов группы.

См. также

Включение модуля (см. раздел 18.4.3)

18.4.3. Включение модуля

Ранее отключенный модуль (см. раздел 18.4.2) может быть включен в прежней конфигурации.

- Чтобы включить модуль:

  1. В главном меню выберите **Политики**.
  2. Выберите политику.
  3. В списке **Отключенные** выберите модуль.
  4. Нажмите **Включить**.

  Модуль включен. Если политика назначена на группу (см. раздел 17.6), 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».

18.4.4. 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 выберите **Политики**.
  2. Выберите политику.
  3. Выберите модуль.
  4. Нажмите **Сменить версию**.
  5. Нажмите **Установить** напротив версии модуля.

18.4.5. Удаление модуля из политики

Вы можете удалить модуль из политики.

Внимание! Если политика назначена на группу (см. раздел 17.6), то модуль будет автоматически удален со всех агентов группы.

- Чтобы удалить модуль из политики:

  1. В главном меню выберите **Политики**.
  2. Выберите политику.

3. Выберите модуль.
4. Нажмите  и подтвердите удаление.

См. также

Назначение политики на группу агентов (см. раздел 17.6)

18.5. Управление модулями в системе

Далее приведены инструкции по управлению модулями в системе.

В этом разделе

Импорт модуля (см. раздел 18.5.1)

Удаление версии модуля (см. раздел 18.5.2)

Удаление модуля (см. раздел 18.5.3)

18.5.1. Импорт модуля

Вы можете импортировать модуль на сервер MaxPatrol EDR из ZIP-архива. Архив может содержать несколько разных модулей и несколько версий каждого модуля. За одну операцию вы можете загрузить только один модуль, при этом возможен импорт сразу всех версий этого модуля. Если загружаемая версия модуля уже есть на сервере, то импорт будет возможен только при условии перезаписи ее файлов и конфигурации. Размер архива не должен превышать 100 МБ.

► Чтобы импортировать модуль:

1. В главном меню выберите раздел **Модули**.
2. Нажмите **Импортировать**.
3. Выберите архив с файлами модуля.
4. Выберите модуль, который вы хотите импортировать на сервер MaxPatrol EDR.
5. Выберите версию модуля, которую вы хотите импортировать.
6. Если вы хотите перезаписать на сервере файлы и конфигурации загружаемых версий модуля, установите флажок **Перезаписать модуль**.

   Если вы не установите этот флажок и на сервере уже есть хотя бы одна загружаемая версия модуля, то не импортируется ни одна из версий.
7. Нажмите **Импортировать**.

См. также

Манифест установки MaxPatrol EDR (см. раздел 6.2)

18.5.2. Удаление версии модуля

Вы можете удалить любую версию модуля из репозитория. Если на агентах установлен модуль этой версии, то он продолжит работу. При этом добавить эту версию в другие политики будет невозможно.

- Чтобы удалить версию модуля:

  1. В главном меню выберите раздел **Модули**.
  2. Нажмите на название модуля.
  3. Выберите версию модуля, которую вы хотите удалить.
  4. Нажмите , выберите пункт **Только версию <Номер версии>** и подтвердите удаление.

18.5.3. Удаление модуля

Вы можете полностью удалить модуль из репозитория. В этом случае он перестанет работать на всех агентах, на которых был установлен.

- Чтобы удалить модуль:

  1. В главном меню выберите раздел **Модули**.
  2. Нажмите на название модуля.
  3. Выполните одно из следующих действий:

     - Если у модуля есть только одна версия, нажмите и подтвердите удаление.
     - Если у модуля есть несколько версий, нажмите , выберите пункт **Модуль целиком** и подтвердите удаление.

18.6. 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 18.6.1);

— выбрав для действия события, при регистрации которых его нужно выполнять (см. раздел 18.6.2).

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

Назначение действий на событие модуля (см. раздел 18.6.1)

Массовое назначение действия на события модуля (см. раздел 18.6.2)

18.6.1. Назначение действий на событие модуля

- Чтобы назначить действия на событие модуля:

  1. В главном меню выберите **Политики**.
  2. Выберите политику.
  3. В списке **Включенные** выберите модуль, на события которого вы хотите назначить действия.
  4. В блоке параметров **События** напротив нужного события нажмите .

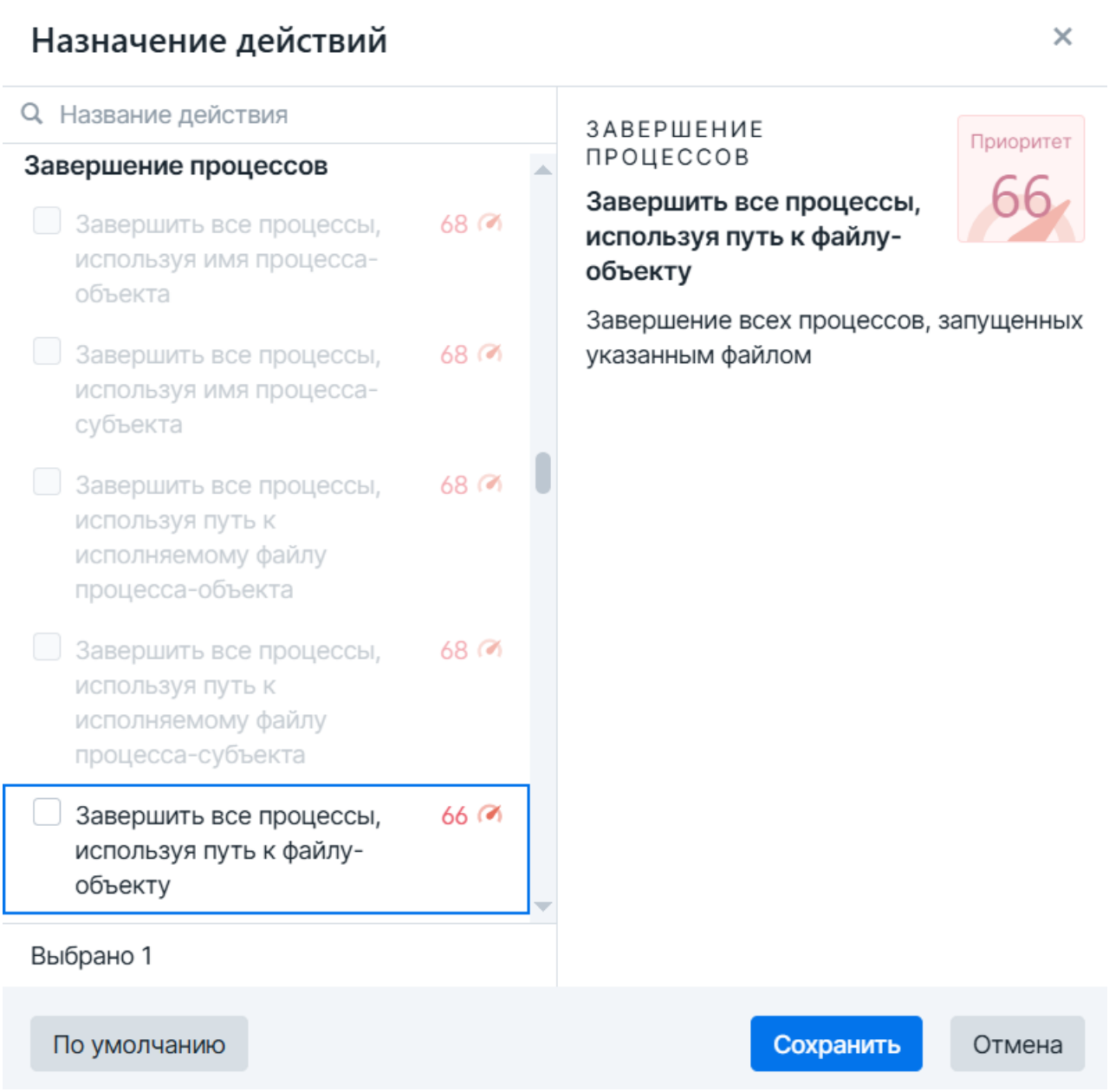

Рисунок 7. Назначение действий

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

18.6.2. 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 выберите **Политики**.
  2. Выберите политику.
  3. В списке **Включенные** выберите модуль, на события которого вы хотите назначить действия.
  4. Нажмите **Мастер назначения действий**.

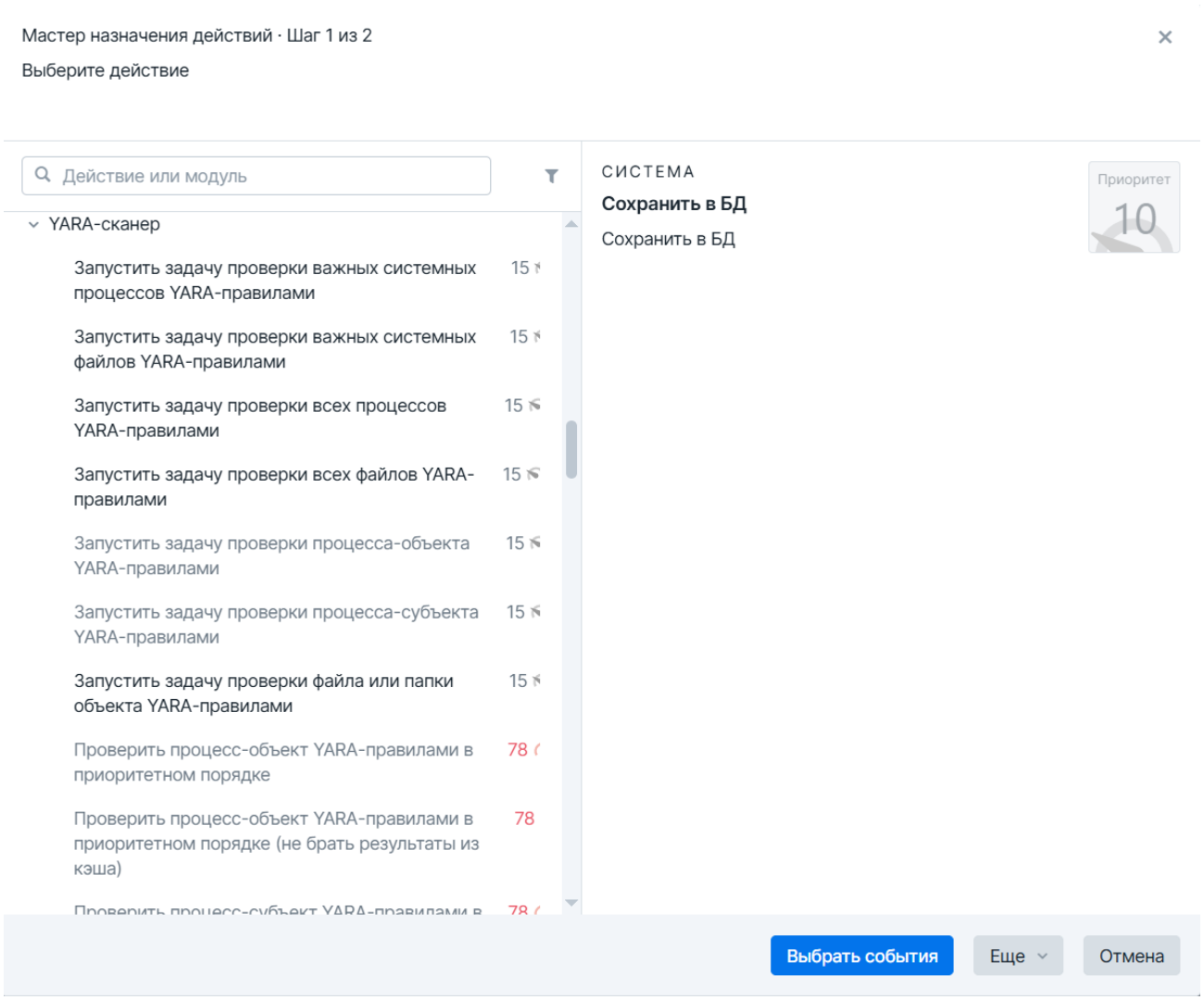

Рисунок 8. Выбор действия

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

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

  6. Нажмите **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**.

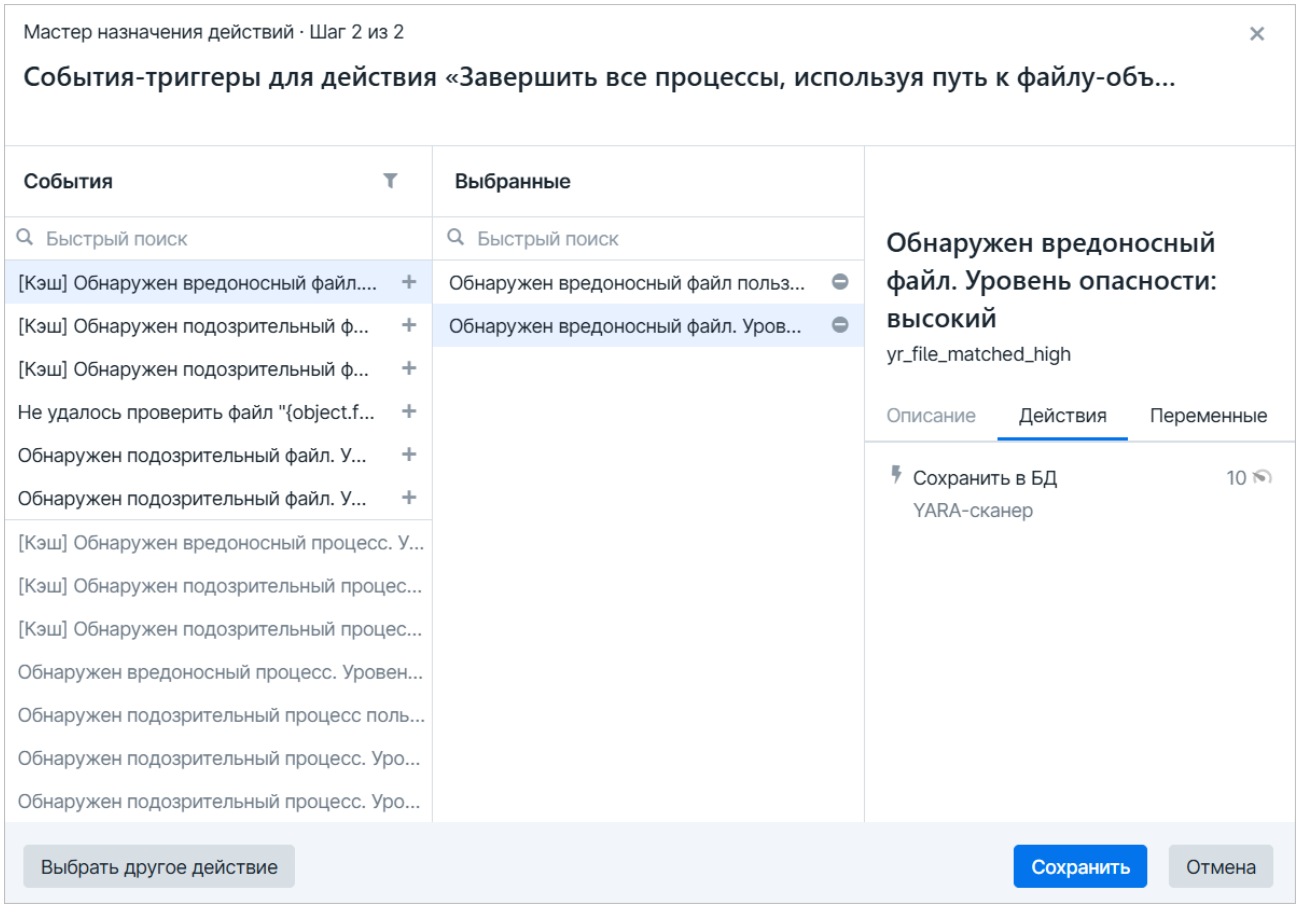

Рисунок 9. Выбор событий

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

19. Настройка модулей и работа с ними

Далее приведена подробная информация о каждом модуле, а также даны инструкции по настройке и работе с ними.

В этом разделе

19.1. Системные модули

В этом разделе приведена информация о системных модулях.

Ядро (внутренний сервис)

Этот модуль предоставляет библиотеку среды выполнения для работы модулей и является обязательным в системе.

19.2. Модули доставки и установки

В этом разделе приведена информация по модулям доставки и установки.

В этом разделе

19.2.1. Установщик Sysmon

Модуль «Установщик Sysmon» устанавливает и конфигурирует утилиту Sysmon. Удаление модуля с агента не повлияет на конфигурацию Sysmon на конечном устройстве.

> **Внимание!** Конфигурация утилиты Sysmon подготовлена экспертами Positive Technologies. При необходимости вы можете изменить конфигурацию под особенности вашей инфраструктуры. Исключение большого количества событий может существенно повлиять на работу модуля «Коррелятор».

Таблица 23. Параметры модуля «Установщик Sysmon»

Параметр или блок параметров	Описание
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

19.2.2. Установщик auditd

Модуль «Установщик auditd» устанавливает и конфигурирует компонент auditd. При удалении модуля с агента на конечном устройстве очищаются файлы с конфигурацией и правилами компонента.

Внимание! В CentOS Stream 10 невозможна установка компонента auditd с помощью модуля «Установщик auditd».

Примечание. Модуль «Установщик auditd» не рекомендуется использовать на узлах, где уже применяется другое ПО для управления правилами и конфигурацией компонента auditd.

Таблица 24. Параметры модуля «Установщик auditd»

Параметр или блок параметров	Описание
Правила	Правила обработки событий, содержимое файла `/etc/audit/audit.rules`
Конфигурация auditd	Конфигурация auditd, содержимое файла `/etc/audit/auditd.conf`
Заменить конфигурацию и правила auditd на агенте	Заменять ли файлы `audit.rules` и `auditd.conf` на конечном устройстве, если они отличаются от заданных в политике. Проверка выполняется каждые 10 минут

19.2.3. Конфигуратор аудита Windows

Модуль «Конфигуратор аудита Windows» настраивает расширенную политику аудита Windows на контроллерах доменов, серверах и рабочих станциях. Базовая конфигурация политик аудита в модуле подготовлена экспертами Positive Technologies. Такая конфигурация позволяет MaxPatrol EDR получать необходимую информацию для своевременного

обнаружения и предотвращения атак на узлах. Модуль каждые 30 минут проверяет параметры политик аудита в операционной системе и обновляет их, если они отличаются от заданных в MaxPatrol EDR.

Внимание! Перед использованием модуля нужно заранее определить инструмент управления конфигурацией расширенной политики аудита Windows. Если на узлах используется групповая политика, во избежание конфликтов конфигурации не рекомендуется устанавливать модуль «Конфигуратор аудита Windows».

Внимание! Для работы модуля на агенте должен быть установлен модуль «Ядро (внутренний сервис)».

Примечание. Рекомендации по настройке политик аудита вы можете найти в документации Microsoft.

19.3. Модули сбора

В этом разделе приведена информация о модулях сбора.

В этом разделе

19.3.1. WinEventLog: сбор данных из журнала событий Windows

Модуль «WinEventLog: сбор данных из журнала событий Windows» передает данные из журнала событий Windows в модуль «Нормализатор» и сторонние системы.

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

1. В главном меню выберите **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «WinEventLog: сбор данных из журнала событий Windows».
4. Если требуется, в блоке параметров **Каналы журналов** добавьте каналы журнала событий Windows, которые будут обрабатываться модулем.

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

5. Если из канала необходимо обрабатывать только некоторые события, введите запрос на языке XPath 1.0 к структуре необработанного события.

   Например, если требуется обрабатывать только события с идентификаторами `4698` или `4654`, запрос должен быть следующим: `*[System[EventID=4698 or EventID=4654]]`.

6. Если из обработки необходимо исключить определенные события, которые записываются в канал, введите запрос на языке XPath 1.0 к структуре необработанного события.

   Например, если требуется исключить события, которые связаны с пользователем `Administrator`, запрос должен быть следующим: `*[EventData[Data='Administrator']]`.

   Примечание. Исключения добавляются только для тех событий, которые записываются в выбранный канал.

7. Нажмите **Сохранить**.

19.3.2. ETW: трассировка событий Windows

Модуль «ETW: трассировка событий Windows» запускает в Windows сеанс трассировки событий и подписывается на события трех провайдеров: Microsoft-Windows-WMI-Activity, Microsoft-Windows-Kernel-Process и Microsoft-Windows-Win32k. Необработанные данные передаются в модуль «Нормализатор», а также при необходимости в MaxPatrol SIEM и в сторонние системы (см. раздел 15.5). Собираемые события позволяют получить расширенную информацию об активности в операционной системе и выявить в ней подозрительное и вредоносное поведение.

Базовая конфигурация модуля подготовлена экспертами Positive Technologies. При необходимости в параметрах модуля вы можете отменить подписку на определенные типы событий или настроить их фильтрацию по идентификаторам.

Если модуль по каким-либо причинам не смог запустить сеанс трассировки событий, то попытка будет повторена через 30 секунд. После пяти неудачных попыток в системе будет зарегистрировано событие «Не удалось запустить сеанс трассировки событий (ETW)».

Внимание! Для работы модуля на агенте должен быть установлен модуль «Ядро (внутренний сервис)».

19.3.3. Сбор данных из файлов журналов

Модуль «Сбор данных из файлов журналов» передает данные из заданных журналов в модуль «Нормализатор» и сторонние системы. Список журналов, которые будут обрабатываться модулем, задается в параметрах модуля. Поддерживаются файлы журналов из Linux и Windows. Если вы хотите обрабатывать из журнала только некоторые события или, наоборот, исключить определенные события, вы можете сделать это с помощью регулярных выражений (regex).

Примечание. Журнал модуля на конечном устройстве может занимать до 2,5 ГБ.

19.3.4. Сбор данных о состоянии системы

Модуль «Сбор данных о состоянии системы» собирает информацию о состоянии операционной системы агента в момент регистрации события ИБ или по запросу пользователя. Это помогает проанализировать ситуацию на конечном устройстве и выбрать подходящее реагирование. С помощью модуля можно создать дамп памяти процесса, а также получить списки:

— запущенных процессов;

— активных сетевых соединений;

— учетных записей;

— автозагрузки.

Таблица 25. Параметры модуля «Сбор данных о состоянии системы»

Параметр или блок параметров	Описание
Защищать архив паролем	Использовать ли пароль для архива с данными
Пароль для архива	Пароль, который будет установлен для скачанного архива с данными
Размер хранилища данных на сервере, МБ	Размер хранилища собранных данных (в мегабайтах) на сервере без учета дампов процессов. При заполнении хранилища из него будут удаляться самые старые данные
Размер хранилища дампов на агенте, МБ	Размер хранилища созданных дампов процессов на агенте (в мегабайтах). При заполнении хранилища из него будут удаляться самые старые дампы. После скачивания дампа он удаляется из хранилища на агенте
Размер хранилища дампов на сервере, МБ	Размер хранилища созданных дампов процессов на сервере (в мегабайтах). При заполнении хранилища из него будут удаляться самые старые дампы

Сбор данных

► Чтобы собрать данные о состоянии системы вручную:

1. В главном меню выберите **Агенты**.
2. Нажмите на название агента, на котором вы хотите собрать данные.
3. Выберите модуль «Сбор данных о состоянии системы».
4. Нажмите ⚙.

5. В раскрывающемся списке выберите, какие данные вы хотите собрать.
6. Нажмите **Собрать данные**.

Просмотр данных

- Чтобы просмотреть данные:

1. В главном меню выберите **Агенты**.
2. Нажмите на название агента, на котором установлен модуль «Сбор данных о состоянии системы».
3. Выберите модуль «Сбор данных о состоянии системы».
4. Нажмите ⚙.
5. Выберите вкладку с типом данных.
6. В списке слева выберите отчет о собранных данных.

   Примечание. Если после сбора данных в параметрах политики был изменен параметр **Пароль для архива**, то просмотреть собранные данные в интерфейсе MaxPatrol EDR невозможно.

Скачивание архива с данными

- Чтобы скачать архив с данными:

1. В главном меню выберите **Агенты**.
2. Нажмите на название агента, на котором установлен модуль «Сбор данных о состоянии системы».
3. Выберите модуль «Сбор данных о состоянии системы».
4. Нажмите ⚙.
5. Выберите вкладку с типом данных.
6. Установите флажки напротив отчетов, которые вы хотите скачать.

   Примечание. Если после сбора данных в параметрах политики был изменен параметр **Пароль для архива**, то скачать собранные данные невозможно.
7. Нажмите **Скачать**.

Вы также можете скачать архив с одним отчетом по кнопке ⬇.

Создание дампа памяти процесса

После создания дамп будет сохранен в хранилище на агенте.

- Чтобы создать дамп процесса:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, на котором установлен модуль «Сбор данных о состоянии системы».
  3. Выберите модуль «Сбор данных о состоянии системы».
  4. Нажмите ⚙.
  5. Введите идентификатор процесса и нажмите **Создать дамп**.

Скачивание дампа памяти процесса

Вы можете скачать только один дамп за один раз. Также невозможно скачивание дампа вместе с другими собранными данными в архиве.

- Чтобы скачать дамп процесса:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, на котором установлен модуль «Сбор данных о состоянии системы».
  3. Выберите модуль «Сбор данных о состоянии системы».
  4. Нажмите ⚙.
  5. В журнале выберите дамп и нажмите **Скачать дамп**.

     Скачивание дампа начнется после завершения пересылки дампа в хранилище на сервере агентов.

     Примечание. Отправка на сервер дампов большого размера может занимать длительное время.

19.3.5. Нормализатор

Модуль «Нормализатор» выполняет нормализацию необработанных событий от модулей «WinEventLog: сбор данных из журнала событий Windows», «ETW: трассировка событий Windows» и «Сбор данных из файлов журналов» для последующей обработки и анализа в других модулях и отправки в MaxPatrol SIEM. Системные события, для которых нет правил нормализации, будут отправлены в MaxPatrol SIEM в необработанном виде. Кроме того, в параметрах модуля вы можете полностью отключить нормализацию событий. В этом случае все события будут передаваться в необработанном виде и вы сможете нормализовать их в MaxPatrol SIEM собственными правилами.

Внимание! Для работы некоторых модулей требуются нормализованные события. При отключении нормализации модули «Коррелятор» и «Обнаружение подозрительных файлов» работать не будут. Модуль «Проверка файлов по хеш-сумме» будет работать только по событиям ИБ от других модулей. Также невозможна отправка необработанных событий на syslog-сервер с помощью соответствующего модуля.

19.4. Модули обнаружения

В этом разделе приведена информация о модулях обнаружения.

В этом разделе

19.4.1. Коррелятор

Далее приведена информация о модуле «Коррелятор» и инструкции по его настройке.

В этом разделе

19.4.1.1. О модуле «Коррелятор»

Модуль «Коррелятор» выполняет корреляцию потока событий от модуля «Нормализатор». При обнаружении вредоносных или подозрительных действий регистрирует события ИБ (корреляционные события). Кроме того, при регистрации определенных корреляционных событий в MaxPatrol 10 автоматически регистрируются инциденты. В системе есть два отдельных коррелятора для Windows и Linux.

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».

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».

Покрываемые техники MITRE ATT&CK

При настройке модулей «Коррелятор (Windows)» и «Коррелятор (Linux)» для каждого события отображаются покрываемые техники из матрицы MITRE ATT&CK. Это помогает правильно настроить автоматическое реагирование и выбрать одинаковые действия для одинаковых техник.

Вы также можете просмотреть всю матрицу MITRE ATT&CK, на которой отмечены техники, покрываемые MaxPatrol EDR. При необходимости вы можете отфильтровать техники по операционной системе, перейти к описанию техники или тактики на сайте attack.mitre.org, а также выгрузить матрицу в формате JSON или XLSX.

► Чтобы просмотреть покрываемые техники,

в главном меню выберите **Система** → **Матрица MITRE ATT&CK**.

19.4.1.2. Работа с исключениями

Вы можете добавлять исключения для правил корреляций. Это позволит уменьшить количество ложных срабатываний правил, которые могут возникать из-за особенностей вашей инфраструктуры. Исключения реализуются двумя способами: с помощью табличных списков из PT KB и с помощью условий в формате регулярных выражений (regex) в параметрах модуля.

Исключения с помощью табличных списков

Вы можете управлять исключениями в модуле «Коррелятор» с помощью стандартных табличных списков базы знаний PT KB: Common_blacklist_regex, Common_blacklist_value, Common_IP_Subnet_Whitelist, Common_whitelist_auto, Common_whitelist_auto_swap, Common_whitelist_auto_thresholds, Common_whitelist_for_labeling, Common_whitelist_for_labeling_regex, Common_whitelist_regex и Common_whitelist_value. После добавления записей в эти табличные списки они будут учтены модулем после установки пакета экспертизы в MaxPatrol SIEM и синхронизации с MaxPatrol EDR (выполняется автоматически каждые 30 минут). Подробная информация о работе с табличными списками в MaxPatrol 10 приведена в справке по этому продукту.

Примечание. Записи в табличные списки могут также добавляться на основе данных события ИБ. В этом случае для их актуализации в MaxPatrol EDR не требуется установка пакета экспертизы в MaxPatrol SIEM.

Примечание. Записи в остальных табличных списках будут обновляться при обновлении пакета экспертизы (см. раздел 8) в MaxPatrol EDR.

При необходимости вместо стандартных табличных списков вы можете использовать собственные с такой же структурой (например, если у вас есть отдельный список с разрешенными IP-адресами и они не дублируются в стандартном списке). Для этого вам нужно выбрать пользовательский список вместо стандартного в параметрах модуля.

Исключения с помощью регулярных выражений

- Чтобы добавить исключение:

  1. В главном меню выберите **Политики**.
  2. Выберите политику.
  3. В списке **Включенные** выберите модуль «Коррелятор».
  4. В блоке параметров **Список исключений** нажмите **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`.

     Внимание! Переменные `event_src.id`, `event_src.ip`, `event_src.rule`, `event_src.fqdn`, `event_src.hostname`, `event_src.host`, `recv_ipv4`, `recv_host` использовать для исключений невозможно.

     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.

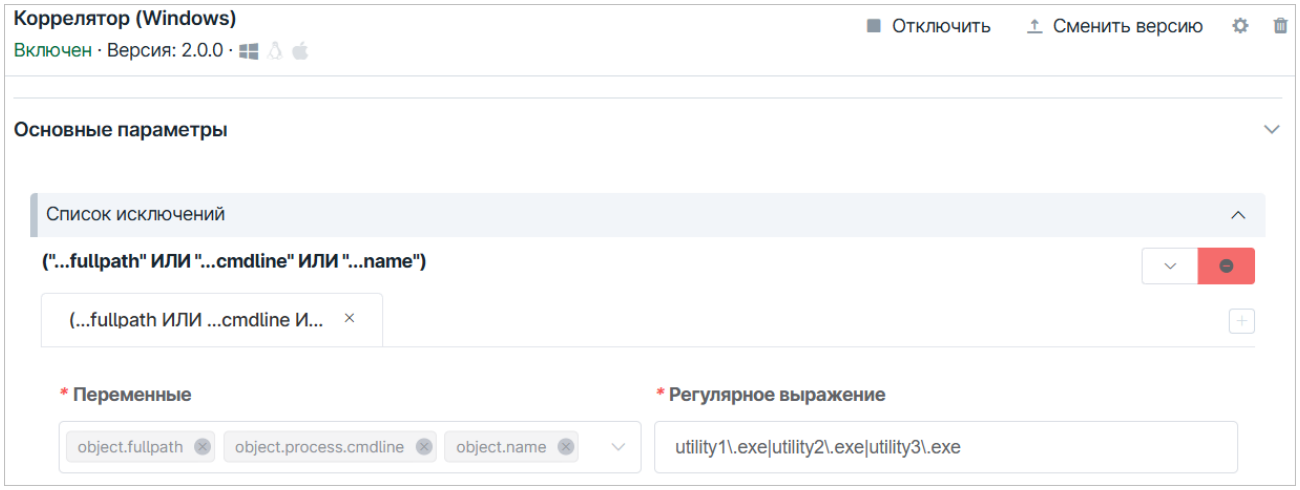

Рисунок 10. Добавление исключения

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.
9. Нажмите **Сохранить**.

19.4.2. YARA-сканер

Далее приведена информация о модуле «YARA-сканер» и инструкции по работе с ним.

В этом разделе

19.4.2.1. О модуле «YARA-сканер»

Модуль «YARA-сканер» выполняет сигнатурный анализ на основе YARA-правил. При обнаружении вредоносных или подозрительных файлов и процессов выносит вердикты и регистрирует события ИБ. Сканирование может запускаться вручную, автоматически по

расписанию или при регистрации подходящего события. Если при запуске проверки по расписанию на агенте уже выполняется сканирование, проверка будет запущена после завершения всех текущих задач.

Таблица 26. Параметры модуля «YARA-сканер»

Параметр или блок параметров	Описание
Максимальный размер файла для проверки, МБ	Максимальный размер файла (в мегабайтах), которой может быть проверен модулем. Ограничение актуально: — при автоматическом реагировании — в этом случае в системе будет зарегистрировано событие «Не удалось проверить файл: превышен максимальный размер»; — ручной проверке, если проверяется более одного файла одновременно, — в этом случаи крупные файлы будут пропущены без регистрации события. Файл, размер которого превышает заданный, вы можете проверить, запустив вручную проверку только этого файла (см. раздел 19.4.2.3)
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. Задать путь вы можете в форматах DOS и UNC, а также с помощью переменных окружения. **Примечание.** Агент MaxPatrol EDR запускается под системной учетной записью, поэтому значение переменной окружения `%userprofile%` — `C:\Windows\System32\config\systemprofile`
Список исключений для YARA-правил	Список идентификаторов YARA-правил, которые не будут использоваться для проверок
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

Параметр или блок параметров	Описание
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
Запуск	Периодичность запуска проверки по расписанию
День недели	Дни недели, в которые будет запускаться проверка по расписанию
Месяцы	Месяцы, в которые будет запускаться проверка по расписанию
День месяца	Дни месяца, в которые будет запускаться проверка по расписанию
Время в часовом поясе агента	Время в часовом поясе агента, в которое будет запускаться проверки по расписанию. **Примечание.** Изменение часового пояса на агенте не повлияет на время запуска ближайшей запланированной проверки. Однако, это изменение будет учтено при запуске последующих проверок или после внесения изменений в расписание в модуле
Область проверки	Область проверки по расписанию
Глубина проверки	Глубина проверки по расписанию: важные системные файлы и процессы (быстрая) или все файлы и процессы (полная)

19.4.2.2. 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. 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 18.6), которые не будут брать результаты из кэша.

19.4.2.3. Запуск проверки вручную

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).

По умолчанию для проверки выбраны правила YARA, заданные в конфигурации политики. Вы можете вставить или импортировать свои правила для проверки.

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

► Чтобы запустить проверку:

1. В главном меню выберите **Агенты**.
2. Нажмите на название агента, на котором вы хотите запустить проверку.
3. Выберите модуль «YARA-сканер».
4. Нажмите ⚙.
5. Нажмите **Новая проверка**.
6. Задайте параметры проверки.
7. Нажмите **Начать проверку**.

19.4.2.4. Просмотр результатов проверки

Вы можете просмотреть список вредоносных файлов и процессов, которые были найдены с помощью правил YARA. Для каждого файла и процесса указано правило, которым они были обнаружены, и его точность (от 0 до 15). Чем выше точность правила, тем меньше ложных срабатываний оно выдает.

- Чтобы просмотреть результаты проверки:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, на котором запускалась проверка модулем «YARA-сканер».
  3. Выберите модуль «YARA-сканер».
  4. Нажмите ⚙.
  5. Нажмите на дату и время начала проверки.

     Отобразятся результаты проверки.

19.4.2.5. Просмотр правил

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

- Чтобы просмотреть правила:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, на котором установлен модуль «YARA-сканер».
  3. Выберите модуль «YARA-сканер».
  4. Нажмите ⚙.
  5. Выберите раздел **Правила**.

19.4.3. Проверка файлов по хеш-сумме

Модуль «Проверка файлов по хеш-сумме» ищет хеш-суммы файлов (MD5 и SHA-256) в базе данных новых угроз. На такие угрозы еще не срабатывают YARA-правила и для них не написаны правила корреляции. Автоматическое действие проверки файла может быть назначено на подходящие события от модулей сбора. MaxPatrol EDR регулярно получает обновления базы данных новых угроз.

В конфигурации модуля задается максимальный размер файла, который может быть проверен (в мегабайтах). Это ограничение относится только к автоматическому реагированию.

- Чтобы вручную проверить файл по хеш-сумме:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, файл с которого вы хотите проверить.
  3. Выберите модуль «Проверка файла по хеш-сумме».

4. Нажмите  .
5. Введите полный путь к файлу.
6. Нажмите **Проверить**.

19.4.4. Обнаружение подозрительных файлов

Модуль «Обнаружение подозрительных файлов» анализирует нормализованные события и обнаруживает появление в системе подозрительных файлов. Файл считается подозрительным, если его расширение специально задано в конфигурации модуля, а также он был обнаружен в заданной папке или был создан заданным процессом.

Таблица 27. Параметры модуля «Обнаружение подозрительных файлов»

Параметр или блок параметров	Описание
Максимальный размер файла для проверки, МБ	Максимальный размер файла (в мегабайтах), который будет учитываться модулем
Правила обнаружения для Windows → Расширения	Список расширений файлов в Windows, которые будут учитываться модулем
Правила обнаружения для Windows → Системные папки	Системные папки Windows, в которых будет отслеживаться появление файлов
Правила обнаружения для Windows → Папки	Список папок в Windows, в которых будет отслеживаться появление файлов
Правила обнаружения для Windows → Процессы	Список процессов в Windows, которые будут отслеживаться на предмет создания файлов
Правила обнаружения для Linux → Расширения	Список расширений файлов в Linux, которые будут учитываться модулем
Правила обнаружения для Linux → Каталоги	Список каталогов в Linux, в которых будет отслеживаться появление файлов
Правила обнаружения для Linux → Процессы	Список процессов в Linux, которые будут отслеживаться на предмет создания файлов

19.5. Модули реагирования

В этом разделе приведена информация о модулях реагирования.

В этом разделе

19.5.1. Удаление файлов

- Чтобы удалить файл на конечном устройстве:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, установленного на конечном устройстве.
  3. Выберите модуль «Удаление файлов».
  4. Нажмите ⚙.
  5. Нажмите **Выбрать действие** и в раскрывшемся меню выберите действие.
  6. Введите путь к файлу.
  7. Нажмите **Выполнить действие**.

19.5.2. Завершение процессов

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).

Примечание. В конфигурации модуля «Завершение процессов» вы можете задать список исполняемых файлов процессов, которые не будут завершаться модулем.

- Чтобы завершить процессы на конечном устройстве:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, установленного на конечном устройстве.
  3. Выберите модуль «Завершение процессов».
  4. Нажмите ⚙.
  5. Нажмите **Выбрать действие** и в раскрывшемся меню выберите **Завершить все процессы, используя имя**.
  6. Введите имя процесса в формате `{"proc_name": "<Имя процесса>"}`.
  7. Нажмите **Выполнить действие**.

19.5.3. Блокировка учетных записей

Модуль «Блокировка учетных записей» блокирует и завершает сеансы локальных учетных записей в операционной системе. Длительность блокировки задается в параметрах соответствующего действия.

Примечание. Для работы модуля на конечных устройствах под управлением операционной системы Linux требуется утилита who.

Таблица 28. Параметры модуля «Блокировка учетных записей»

Параметр или блок параметров	Описание
Исключения	Список учетных записей, которые не будут блокироваться и сеансы которых не будут завершаться
Длительность блокировки, мин (параметр действий)	Время в минутах, на которое будет заблокирована учетная запись. По умолчанию 120 минут

Блокировка локальных учетных записей

Вы можете вручную заблокировать и разблокировать локальную учетную запись в операционной системе. Длительность блокировки определяется соответствующим параметром для действия «Заблокировать учетную запись (объект) по логину» в конфигурации политики.

- Чтобы заблокировать учетную запись:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, в операционной системе которого вы хотите заблокировать учетную запись.
  3. Выберите модуль «Блокировка учетных записей».
  4. Нажмите ⚙.
  5. Напротив учетной записи в списке нажмите **Заблокировать**.

  Учетная запись заблокирована.

- Чтобы досрочно разблокировать учетную запись,

  нажмите **Разблокировать**.

Завершение сеансов локальных учетных записей

Вы можете вручную завершить сеанс локальной учетной запись в операционной системе.

Примечание. Завершить сеанс учетной записи root в Linux невозможно.

- Чтобы завершить сеанс учетной записи:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, в операционной системе которого вы хотите завершить сеанс учетной записи.
  3. Выберите модуль «Блокировка учетных записей».
  4. Нажмите ⚙.
  5. Напротив учетной записи в списке нажмите **Завершить сеанс**.

Вы также можете завершить все активные сеансы по кнопке **Завершить активные сеансы**.

19.5.4. Изоляция узлов

Модуль «Изоляция узлов» блокирует сетевой трафик на узлах. 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.

Внимание! Для работы версии модуля 3.0.0 на агенте должен быть установлен модуль «Ядро (внутренний сервис)» (см. раздел 19.1). Версия модуля 2.0.0 работает только в Windows.

Примечание. В конфигурации модуля вы можете настроить исключения — параметры сетевого трафика, который не будет блокироваться модулем. Добавлять в исключения сервер MaxPatrol EDR не требуется: обмен данных с ним не будет блокироваться.

- Чтобы изолировать узел, на котором установлен агент:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента.
  3. Выберите модуль «Изоляция узлов».
  4. Нажмите ⚙.
  5. Выберите способ изоляции узла.
  6. Настройте время, через которое изоляция узла будет снята автоматически.
  7. Нажмите **Изолировать**.

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

  Узел изолирован.

- Чтобы досрочно снять частичную изоляцию узла,

  нажмите **Снять изоляцию**.

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

19.5.5. Блокировка по IP-адресу

Модуль «Блокировка по IP-адресу» блокирует все сетевые соединения по IP-адресу. Адрес может быть заблокирован на уровне политики, агента или на обоих уровнях. Блокировка полезна, если вы обнаружили подозрительное соединение и хотите его прервать. Если IP-адрес 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 выберите **Агенты**.
  2. Нажмите на название агента, на котором вы хотите заблокировать IP-адрес.
  3. Выберите модуль «Блокировка по IP-адресу».
  4. Нажмите ⚙.
  5. Введите IP-адрес в формате IPv4, IPv6 или подсеть в нотации CIDR.
  6. Нажмите **Заблокировать**.

  IP-адрес заблокирован на агенте.

- Чтобы разблокировать IP-адрес на агенте,

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

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

19.5.6. Завершение работы

Модуль «Завершение работы» завершает работу конечного устройства, переводит его в спящий режим или перезагружает. Эти действия позволяют остановить развитие атаки, если другие способы не помогли, а также, например, применить параметры для устранения уязвимостей. Выполнить действия вы можете сразу или через заданное время — в этом случае пользователю конечного устройства будет отправлено уведомление о завершении работы или перезагрузке. В параметрах модуля вы можете задать исключения — узлы, на которых действия выполняться не будут.

Примечание. Перевод конечного устройства в спящий режим всегда будет выполняться без задержки.

- Чтобы вручную завершить работу устройства, перевести его в спящий режим или перезагрузить:

  1. В главном меню выберите **Агенты**.
  2. Выберите агент, на котором вы хотите выполнить действие.
  3. Выберите модуль «Завершение работы».
  4. Нажмите ⚙.
  5. Если действие нужно выполнить сразу, снимите флажок **Уведомить пользователя за N минут**.
  6. Нажмите кнопку, соответствующую необходимому действию, и подтвердите операцию.

19.5.7. Перенаправление DNS-запросов (sinkholing)

Далее приведена информация о модуле «Перенаправление DNS-запросов (sinkholing)» и инструкции по работе с ним.

В этом разделе

О модуле «Перенаправление DNS-запросов (sinkholing)» (см. раздел 19.5.7.1)

Настройка модуля «Перенаправление DNS-запросов (sinkholing)» (см. раздел 19.5.7.2)

Перенаправление DNS-запросов вручную (см. раздел 19.5.7.3)

19.5.7.1. О модуле «Перенаправление DNS-запросов (sinkholing)»

Модуль «Перенаправление DNS-запросов (sinkholing)» перенаправляет трафик с подозрительных и вредоносных доменов на заданный IP-адрес с помощью файла `hosts`.

Таблица 29. Параметры модуля «Перенаправление DNS-запросов (sinkholing)»

Параметр или блок параметров	Описание
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. **Примечание.** В файл `hosts` будут добавлены записи со всеми сочетаниями заданных префиксов и доменов

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

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

  1. В главном меню выберите **Политики**.
  2. Выберите политику.
  3. В списке **Включенные** выберите модуль «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 **Сохранить**.

19.5.7.3. Перенаправление DNS-запросов вручную

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 конфигурации модуля (см. раздел 19.5.7.2) в политике.

- Чтобы перенаправить DNS-запросы с домена:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, на котором вы хотите перенаправлять DNS-запросы.
  3. Выберите модуль «Перенаправление DNS-запросов (sinkholing)».
  4. Нажмите ⚙.
  5. Введите один или несколько доменов, трафик с которых нужно перенаправлять.
  6. Нажмите **Добавить**.

  DNS-запросы с домена перенаправлены.

- Чтобы отменить перенаправление DNS-запросов,

  напротив домена в списке нажмите **Удалить**.

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

19.5.8. Карантин

Далее приведена информация о модуле «Карантин» и инструкции по работе с ним.

В этом разделе

19.5.8.1. О модуле «Карантин»

Модуль «Карантин» изолирует подозрительные файлы в зашифрованном хранилище на время их проверки с помощью YARA-правил или в PT Sandbox. При этом в карантин помещается не сам файл, а его копия. Из-за этого в целях безопасности исходный файл рекомендуется удалять модулем «Удаление файла». Сценарий настройки системы с модулем «Карантин» может быть следующим:

1. На подходящие события модуля «Коррелятор» назначаются действия «Поместить копию файла в карантин», «Отправить файл на проверку в PT Sandbox» и «Удалить файл».
2. На событие «Файл проверен в PT Sandbox. Вердикт: безопасный» назначается действие «Восстановить файл из карантина».
3. Если файл признан вредоносным, файл удаляется из карантина по ротации, вручную или выгружается для исследования экспертами.

Таблица 30. Параметры модуля «Карантин»

Параметр или блок параметров	Описание
Пароль для архива	Пароль, который будет установлен для скачанного из карантина архива с файлами
Исключения → Папки и файлы	Путь до файла или путь до папки, файлы в которой не будут помещаться в карантин
Исключения для расширений файлов	Список расширений файлов, которые не будут помещаться в карантин
Максимальный размер файла в карантине, МБ	Максимальный размер файла, который может быть помещен в карантин (в мегабайтах)
Размер хранилища, МБ	Размер хранилища файлов в карантине (в мегабайтах). При заполнении хранилища из него будут удаляться самые старые файлы
Запасная папка для восстановления	Папка, в которую будет восстановлен файл, если его невозможно восстановить в изначальную папку

19.5.8.2. Изоляция файла вручную

Вы можете поместить копию подозрительного файла в карантин на время его проверки. После этого в целях безопасности рекомендуется удалить сам файл (см. раздел 19.5.1).

- Чтобы поместить копию файла в карантин:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, на котором вы хотите поместить файл в карантин.

3. Выберите модуль «Карантин».
4. Нажмите ⚙.
5. Введите путь к файлу.
6. Нажмите **Изолировать файл**.

19.5.8.3. Восстановление файла из карантина

Если вы убедились, что файл безопасный, вы можете вручную восстановить его из карантина.

- Чтобы вручную восстановить файл из карантина:

1. В главном меню выберите **Агенты**.
2. Нажмите на название агента, на котором вы хотите восстановить файл из карантина.
3. Выберите модуль «Карантин».
4. Нажмите ⚙.
5. Напротив файла в списке нажмите ↻.

Примечание. Если в конфигурации политики после помещения файла в карантин был изменен пароль для архива, то файл восстановлен не будет. В таком случае для восстановления файла необходимо вернуть старый пароль.

19.5.8.4. Удаление файла из карантина

Если файл признан вредоносным, он будет окончательно удален из карантина по ротации. Вы также можете окончательно удалить его вручную.

- Чтобы окончательно удалить файл:

1. В главном меню выберите **Агенты**.
2. Нажмите на название агента, на котором вы хотите окончательно удалить файл.
3. Выберите модуль «Карантин».
4. Нажмите ⚙.
5. Напротив файла в списке нажмите 🗑.

Вы также можете удалить все файлы из карантина по кнопке **Удалить все** или несколько выбранных по кнопке **Удалить выбранные**.

19.5.8.5. Скачивание файла из карантина

Если файл признан вредоносным, вы можете скачать его из карантина и передать на исследование экспертам. Скачанный файл будет помещен в архив с паролем, который задается в конфигурации (см. раздел 19.5.8.1).

- Чтобы скачать файл из карантина:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, на котором вы хотите скачать файл из карантина.
  3. Выберите модуль «Карантин».
  4. Нажмите ⚙.
  5. Напротив файла в списке нажмите ⬇.

Вы также можете скачать архив со всеми файлами в карантине. Для этого вам нужно выделить файлы в списке и нажать кнопку **Скачать архив**.

19.5.9. Запуск командной оболочки

Модуль «Запуск командной оболочки» позволяет выполнять команды в PowerShell или Bash на конечном устройстве из веб-интерфейса MaxPatrol EDR. Это помогает проводить расследование инцидентов, собирать необходимые данные и устранять нарушения независимо от того, где находится конечное устройство. Все выполненные команды сохраняются в журнал.

Таблица 31. Параметры модуля «Запуск командной оболочки»

Параметр или блок параметров	Описание
Защищать архив паролем	Использовать ли пароль для архива с журналом выполненных команд
Пароль для архива	Пароль, который будет установлен для скачанного архива с журналом

Выполнение команд в оболочке

- Чтобы выполнить команду в оболочке:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, на котором вы хотите выполнить команду.
  3. Выберите модуль «Запуск командной оболочки».
  4. Нажмите ⚙.

5. Нажмите **Запустить**.
6. Введите команду и нажмите клавишу Enter.

Скачивание журнала выполненных команд

- Чтобы скачать журнал выполненных команд:
  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, на котором установлен модуль «Запуск командной оболочки».
  3. Выберите модуль «Запуск командной оболочки».
  4. Нажмите ⚙.
  5. Выберите вкладку **Журнал**.
  6. Выберите одну или несколько записей в журнале.
  7. Нажмите ⬇.

19.5.10. Интерпретатор языка Lua

Модуль «Интерпретатор языка Lua» предоставляет возможность для выполнения произвольного кода на языке Lua на агенте.

- Чтобы выполнить произвольный код на языке Lua:
  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, на котором вы хотите выполнить код.
  3. Выберите модуль «Интерпретатор языка Lua».
  4. Нажмите ⚙.
  5. Введите код.
  6. Нажмите **Выполнить**.

19.6. Модули интеграции

В этом разделе приведена информация о модулях интеграции.

В этом разделе

Проверка файлов в PT Sandbox (см. раздел 19.6.1)

Сканирование в режиме аудита (MaxPatrol VM) (см. раздел 19.6.2)

Отправка событий на syslog-сервер (см. раздел 19.6.3)

Отправка файлов (см. раздел 19.6.4)

19.6.1. Проверка файлов в PT Sandbox

Далее приведена информация о модуле «Проверка файлов в PT Sandbox» и инструкции по работе с ним.

В этом разделе

19.6.1.1. О модуле «Проверка файлов в PT Sandbox»

Модуль «Проверка файлов в PT Sandbox» отправляет файлы на проверку в PT Sandbox и сохраняет результат проверки в локальные БД всех агентов с такой же 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.

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).

Таблица 32. Параметры модуля «Проверка файлов в PT Sandbox»

Параметр или блок параметров	Описание
Ключ API	Токен доступа к публичному API PT Sandbox. Инструкции по созданию токена доступа PT Sandbox приведены в технической документации продукта
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

Параметр или блок параметров	Описание
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 (доменное имя или IP-адрес с портом без протокола)
Максимальное время ожидания результатов проверки	Время в минутах, в течение которого вам хотелось бы получить результат проверки файла. Если результат не будет получен за заданное время, то будет сгенерировано событие «Истекло время ожидания результата проверки файла». Проверка при этом не отменяется и результат будет получен позднее

19.6.1.2. Настройка модуля «Проверка файлов в PT Sandbox»

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

  1. В главном меню выберите **Политики**.
  2. Выберите политику.
  3. В списке **Включенные** выберите модуль «Проверка файлов в PT Sandbox».
  4. Введите адрес сервера PT Sandbox, на который вы хотите отправлять файлы.
  5. Введите токен доступа к публичному API PT Sandbox.

     Примечание. Подробная инструкция созданию токена доступа приведена в Справочном руководстве по публичному API из комплекта поставки PT Sandbox.
  6. Если требуется, задайте дополнительные параметры модуля.
  7. Если требуется, выберите действия, которые будут выполняться при регистрации событий ИБ (см. раздел 18.6).
  8. Нажмите **Сохранить**.

19.6.1.3. Отправка файлов на проверку в PT Sandbox вручную

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

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, установленного на конечном устройстве.
  3. Выберите модуль «Проверка файлов в PT Sandbox».
  4. Нажмите ⚙.
  5. Введите путь к файлу.
  6. Если требуется, отключите поведенческий анализ файла.

     Без поведенческого анализа проверка пройдет быстрее.
  7. Нажмите **Проверить файл**.

19.6.1.4. 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 выберите **Агенты**.
  2. Нажмите на название агента, на котором установлен модуль «Проверка файлов в PT Sandbox».
  3. Выберите модуль «Проверка файлов в PT Sandbox».
  4. Нажмите ⚙.
  5. Если требуется, измените SQL-запрос.
  6. Выберите базу данных, из которой вы хотите получить данные.
  7. Нажмите **Выполнить запрос**.

19.6.2. Сканирование в режиме аудита (MaxPatrol VM)

Далее приведена информация о модуле «Сканирование в режиме аудита (MaxPatrol VM)» и инструкции по работе с ним.

В этом разделе

19.6.2.1. О модуле «Сканирование в режиме аудита (MaxPatrol VM)»

Модуль «Сканирование в режиме аудита (MaxPatrol VM)» выполняет аудит узлов методом белого ящика. Модуль определяет детальную конфигурацию операционной системы, установленной на узле, перечень установленного программного обеспечения, список открытых портов, перечень зарегистрированных пользователей и передает данные в MaxPatrol VM для формирования перечня уязвимостей и карты сети.

> **Внимание!** В текущей версии MaxPatrol EDR невозможно сканирование в режиме аудита на узлах под управлением следующих ОС: Windows 11, Astra Linux Common Edition 2.12 («Орел»), «РЕД ОС Рабочая станция» 7.3, AlterOS Desktop 7.5, «ОСнова» 2.0 «Оникс», «Альт Сервер» 9, 10.1, 10.2, «Альт Рабочая станция» 10.2 и «МОС» 12.

Таблица 33. Параметры модуля «Сканирование в режиме аудита (MaxPatrol VM)»

Параметр или блок параметров	Описание
Версия MaxPatrol 10	Версия MaxPatrol 10, в которой будут обрабатываться результаты сканирования. Для корректной обработки необходимо выбрать используемую версию MaxPatrol 10. Если вы выберете версию ниже используемой, то в результатах будут неполные данные. Если выше — результаты сканирования обработаны не будут. **Внимание!** Для агентов, установленных на Debian 12 и Ubuntu 24.04 LTS, необходимо всегда выбирать версию версию 27.2 или выше, на Red Hat Enterprise Linux 7 (при использовании MaxPatrol 10 версии 26.2) — версию 25.1
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

Параметр или блок параметров	Описание
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
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

19.6.2.2. Настройка модуля «Сканирование в режиме 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 19.6.2.3). 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 выберите **Политики**.
  2. Выберите политику.
  3. В списке **Включенные** выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».

4. В раскрывающемся списке **Версия MaxPatrol 10** выберите используемую версию MaxPatrol 10.
5. В блоке параметров **Расписание** настройте запуск сканирования по расписанию.
6. Если требуется, задайте дополнительные параметры модуля.
7. Если требуется, выберите действия, которые будут выполняться при регистрации событий ИБ (см. раздел 18.6).
8. Нажмите **Сохранить**.

19.6.2.3. Ручной запуск сканирования

Запуск сканирования на одном 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 выберите **Агенты**.
  2. Нажмите на название агента, на котором вы хотите запустить сканирование.
  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  4. Нажмите ⚙.
  5. Нажмите **Запустить сканирование**.

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

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

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 выберите **Группы агентов**.
  2. Нажмите на название группы, на агентах которой вы хотите запустить сканирование.
  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  4. Нажмите ⚙.
  5. Нажмите **Запустить сканирование**.

19.6.2.4. Отключение запуска сканирования по расписанию

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

Отключения запуска по расписанию на одном агенте

- Чтобы отключить запуск сканирования по расписанию:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, на котором вы хотите отключить запуск сканирования по расписанию.
  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  4. Нажмите ⚙.
  5. Нажмите **Отключить запуск по расписанию**.

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

Отключения запуска по расписанию на всех агентах группы

- Чтобы отключить запуск сканирования по расписанию для группы агентов:

  1. В главном меню выберите **Группы агентов**.
  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 ⚙.
  5. Нажмите **Отключить запуск по расписанию**.

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

19.6.2.5. Просмотр результатов сканирования

Просмотр результатов сканирования на одном агенте

- Чтобы просмотреть результаты сканирования:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, на котором установлен модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  4. Нажмите ⚙.
  5. Выберите раздел **Сканирования**.

     Отобразятся результаты сканирования узла.

Просмотр результатов сканирования на всех агентах группы

- Чтобы просмотреть результаты сканирования:

  1. В главном меню выберите **Группы агентов**.
  2. Нажмите на название группы, на которую назначена политика с модулем «Сканирование в режиме аудита (MaxPatrol VM)».
  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  4. Нажмите ⚙.
  5. Выберите раздел **Сканирования**.

     Отобразятся результаты последнего сканирования всех узлов группы.

19.6.3. Отправка событий на syslog-сервер

Модуль «Отправка событий на syslog-сервер» отправляет системные события и записи о событиях ИБ на syslog-сервер, адрес которого задается в конфигурации. Для автоматической отправки событий ИБ на syslog-сервер в политике должно настроено действие «Отправить событие на syslog-сервер» (см. раздел 18.6). Вы также можете вручную отправлять события из карточки модуля на агенте.

> **Внимание!** Системные события отправляются только в нормализованном виде, поэтому на всех агентах должен быть установлен и включен модуль «Нормализатор». Системные события, для которых нет правил нормализации, не будут отправлены на syslog-сервер.

См. также

Настройка хранения и передачи системных событий (см. раздел 15.5)

19.6.4. Отправка файлов

Модуль «Отправка файлов» отправляет файлы с конечного устройства во внешнюю систему, адрес которой задан в конфигурации. Например, это может быть песочница.

Таблица 34. Параметры модуля «Отправка файлов»

Параметр или блок параметров	Описание
Максимальный размер файла, МБ	Максимальный размер файла, который вы можете отправить во внешнюю систему
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

Отправка файла вручную

- Чтобы отправить файл:

  1. В главном меню выберите **Агенты**.
  2. Нажмите на название агента, файл с которого вы хотите отправить во внешнюю систему.
  3. Выберите модуль «Отправка файлов».
  4. Нажмите  .
  5. Введите путь к файлу.
  6. Нажмите **Отправить файл**.

20. О событиях MaxPatrol EDR

В MaxPatrol EDR существует два типа событий: системные события собираются модулями сбора (см. раздел 19.3) на конечных устройствах, а события ИБ регистрируются модулями в процессе их работы. Все события MaxPatrol EDR отображаются в системе MaxPatrol 10 на вкладке **События**. Для отображения событий только из MaxPatrol EDR вы можете использовать фильтр `generator.type = "xdr"`. Кроме того, из карточки агента вы можете перейти к событиям этого агента.

События MaxPatrol EDR могут объединяться в цепочку. Это помогает проанализировать их последовательность. Например, в одну цепочку могут быть объединены событие ИБ от модуля «Коррелятор» и событие ИБ о реагировании на него. Переходить между событиями цепочки вы можете с помощью ссылок в значении параметров **datafield18** (идентификатор цепочки), **datafield19** (идентификатор события, предшествовавшего этому событию) и **datafield20** (идентификатор пользователя, вызвавшего событие) в карточке события в разделе **Дополнительная информация**. Из карточки события ИБ от модуля «Коррелятор» вы также можете перейти к исходному событию с помощью соответствующий ссылки.

> **Примечание.** Идентификатор в значении параметра **datafield19** соответствует идентификатору предшествовавшего события из значения параметра **uuid** в разделе **Служебные данные**.

21. 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 как на одном агенте, так и на множестве (в случае массовой атаки). Набор доступных способов реагирования зависит от установленных на агенте модулей (см. раздел 19).

Вы можете запускать реагирование:

— на одном агенте — из веб-интерфейса модуля (см. раздел 19);

— на одном или нескольких агентах — на странице **Агенты**;

— на одной или нескольких группах агентов — на странице **Группы агентов**.

Вы также можете реагировать на конкретное событие в системе MaxPatrol 10.

Примечание. Для массового реагирования доступны не все действия модулей.

Массовое реагирование на нескольких агентах

Вы можете выполнить действие сразу на нескольких выбранных агентах. Эти агенты должны быть авторизованы и на них должны работать модули реагирования. Если один или несколько выбранных агентов недоступны, действия на них выполнены не будут. После их подключения вы можете повторно запустить реагирование из журнала.

► Чтобы запустить массовое реагирование на агентах:

1. В главном меню выберите **Агенты**.
2. Выберите несколько агентов, удерживая клавишу Ctrl или Shift.
3. Нажмите **Реагирование** и в раскрывшемся меню выберите необходимое действие.

   Примечание. В меню отображаются действия со всех модулей выбранных агентов. Если на каком-то агенте нет необходимого модуля, то выбранное действие на этом агенте запущено не будет.
4. Если требуется, задайте параметры действия.
5. Нажмите **Запустить**.

Массовое реагирование на группах агентов

Вы можете выполнить действие сразу на всех агентах одной или нескольких групп. Если один или несколько агентов из выбранных групп недоступны, действия на них выполнены не будут. После их подключения вы можете повторно запустить реагирование из журнала.

- Чтобы запустить массовое реагирование на всех агентах группы:

  1. В главном меню выберите **Группы агентов**.
  2. Выберите одну или несколько групп, удерживая клавишу Ctrl или Shift.
  3. Нажмите **Реагирование** и в раскрывшемся меню выберите необходимое действие.

     Примечание. В меню отображаются действия со всех модулей, которые работают на агентах выбранных групп. Если на какую-то группу не назначена политика с необходимым модулем, то выбранное действие на агентах этой группы запущено не будет.
  4. Если требуется, задайте параметры действия.
  5. Нажмите **Запустить**.

Реагирование на событие

При реагировании на событие список доступных действий определяется модулями, которые установлены на узле, и данными, которые передаются в событии.

- Чтобы запустить реагирование на событие:

  1. Перейдите в систему MaxPatrol 10.
  2. В главном меню выберите **События**.
  3. Если требуется, отфильтруйте события в списке.
  4. В списке событий выберите событие, на которое вы хотите отреагировать.
  5. В панели **Сводка** нажмите **Реагировать**.
  6. Выберите необходимое действие.

Журнал реагирования

Вы можете просматривать журнал массового реагирования. Журнал доступен в главном меню **Система** → **Журнал реагирования**. В журнале отображаются сведения и результаты всех запусков массового реагирования. При необходимости вы можете повторить запуск какого-либо действия или выбрать для реагирования другое действие на той же выборке агентов. При выборе в списке записей действия откроется карточка реагирования с подробными результатами на каждом агенте.

См. также

Настройка модулей и работа с ними (см. раздел 19)

22. Администрирование MaxPatrol EDR

В этом разделе приводятся инструкции по администрированию MaxPatrol EDR.

В этом разделе

22.1. 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.

В MaxPatrol EDR предусмотрено два 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.

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

Отмена задачи (см. раздел 22.1.4)

Удаление резервной копии (см. раздел 22.1.5)

22.1.1. Создание резервной копии

- Чтобы создать резервную копию:

  1. В главном меню выберите **Система** → **Резервное копирование и восстановление**.
  2. Нажмите **Создать резервную копию**.
  3. Если требуется, измените название резервной копии.
  4. Если требуется, снимите флажки с тех серверов агентов, конфигурацию которых не требуется добавлять в резервную копию.
  5. Выберите тип резервной копии.
  6. Нажмите **Создать**.

     В систему будет добавлена задача на создание резервной копии.

22.1.2. Импорт резервной копии

Вы можете импортировать резервную копию, созданную в другой системе. Перед импортом вам нужно скопировать архив с резервной копией из каталога `/opt/edr_data/minio/data/edr-modules/backups` в каталог `/opt/edr/backups` на управляющем сервере и перезапустить его.

- Чтобы импортировать резервную копию:

  1. В главном меню выберите **Система** → **Резервное копирование и восстановление**.
  2. Нажмите .
  3. Введите имя архива с резервной копией, которую вы хотите импортировать в систему.
  4. Нажмите **Импортировать**.

     В систему будет добавлена задача на импорт резервной копии.

22.1.3. 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»).

► Чтобы восстановить конфигурацию системы:

1. В главном меню выберите **Система** → **Резервное копирование и восстановление**.
2. Выберите резервную копию.
3. Нажмите ⮌.
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 **Восстановить**.

   В систему будет добавлена задача на восстановление из резервной копии.
6. После завершения задачи на управляющем сервере MaxPatrol EDR перезапустите контейнеры:

   ```
   sudo docker-compose -f /opt/edr/docker-compose.yml up -d vxedr-modules
   ```

22.1.4. 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 выберите **Система** → **Резервное копирование и восстановление**.
2. Выберите задачу, нажав на дату ее создания.
3. Нажмите **Отмена**.

22.1.5. 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 выберите **Система** → **Резервное копирование и восстановление**.
  2. Выберите резервную копию.
  3. Нажмите и подтвердите удаление.

22.2. 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

22.2.1. 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.

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

22.2.2. Создание задачи

- Чтобы создать задачу:

  1. В главном меню выберите **Система** → **Планировщик задач с агентами**.
  2. Нажмите **Создать задачу**.
  3. Введите название задачи.
  4. Выберите, когда нужно запускать задачу.
  5. Выберите, для каких агентов будет выполняться задача.
  6. Если на предыдущем шаге вы выбрали пункт **Из выбранных групп**, выберите группы, для агентов которых будет выполняться задача.
  7. Введите дополнительное условие выполнения задачи на языке PDQL (см. раздел 22.2.3).
  8. Выберите действие, которое необходимо выполнять с агентами.
  9. Если вы выбрали действие **Установить выбранную версию агента**, выберите версию агента, которую нужно установить.
  10. Если вы выбрали действие **Переместить в группу**, выберите группу, в которую нужно переместить агенты.
  11. Нажмите **Создать**.

22.2.3. 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 параметрами `Agent.ConnectedDate` и `Agent.CreatedDate`.

В значении параметров `Agent.ConnectedDate` и `Agent.CreatedDate` вы можете использовать функцию `Now()`, которая определяет текущий момент времени с точностью до секунды. Допустимый формат единиц времени:

- месяц: `mo`, `month`, `months`;
- неделя: `w`, `week`, `weeks`;
- день: `d`, `day`, `days`;

— час: `h`, `hour`, `hours`;

— минута: `mi`, `minute`, `minutes`.

Таблица 35. 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 агентов	`Agent.ConnectedDate <= Now() - 1w` `Agent.ConnectedDate = 2022-08-29T03:27:17`
`Agent.CreatedDate`	Дата и время первого подключения к серверу агентов	`Agent.CreatedDate <= Now()- 5d` `Agent.CreatedDate = Now()- 1w`
`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%'`

Параметр	Описание	Примеры
		`Agent.Ip != 127.0.0.1`
`Agent.OsArch`	Архитектура операционной системы	`Agent.OsArch in ['amd64', '386']` `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.%'`

22.2.4. 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 выберите **Система** → **Планировщик задач с агентами**.
  2. Выберите задачу со статусом **Запланирована** или **Выполняется**.
  3. Нажмите **Остановить**.
- Чтобы запустить остановленную задачу:
  1. В главном меню выберите **Система** → **Планировщик задач с агентами**.
  2. Выберите задачу со статусом **Остановлена**.
  3. Нажмите **Запустить**.

22.2.5. Просмотр результатов задачи

- Чтобы просмотреть результаты выполнения задачи:
  1. В главном меню выберите **Система** → **Планировщик задач с агентами**.
  2. Нажмите на название задачи.

22.2.6. 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 выберите **Система** → **Планировщик задач с агентами**.
  2. Выберите задачу.
  3. Нажмите **Создать копию**.
  4. Измените параметры задачи.
  5. Нажмите **Создать**.

22.2.7. Изменение параметров задачи

Перед изменением задачи вам нужно ее остановить (см. раздел 22.2.4).

- Чтобы изменить параметры задачи:
  1. В главном меню выберите **Система** → **Планировщик задач с агентами**.
  2. Выберите задачу.
  3. Нажмите **Изменить**.
  4. Измените параметры задачи.
  5. Нажмите **Сохранить**.

22.2.8. Удаление задачи

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

- Чтобы удалить задачу:
  1. В главном меню выберите **Система** → **Планировщик задач с агентами**.
  2. Выберите задачу.
  3. Нажмите **Удалить** и подтвердите удаление.

22.3. 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 11. Мониторинг MaxPatrol EDR в Grafana

В этом разделе

Включение передачи данных о состоянии агента (см. раздел 22.3.1)

Просмотр записей в системном журнале (см. раздел 22.3.2)

Работа с дашбордами (см. раздел 22.3.3)

Построение графика метрики (см. раздел 22.3.4)

Смена пароля учетной записи в Elasticsearch (см. раздел 22.3.5)

22.3.1. Включение передачи данных о состоянии агента

По умолчанию передача данных о состоянии агента в сервис Grafana Loki отключена.

Включение передачи данных в Windows

- Чтобы включить передачу данных для агента, установленного в Windows:

  1. Нажмите **Пуск** → **Выполнить**.
  2. В поле **Открыть** введите `regedit` и нажмите **OK**.
  3. В списке выберите **Мой компьютер** → **HKEY_LOCAL_MACHINE** → **SYSTEM** → **CurrentControlSet** → **Services** → **vxagent**.
  4. В значение параметра **ImagePath** добавьте ключ `-tracer=true`.
  5. Перезапустите агент:

     ```
     sc stop vxagent
     sc start vxagent
     ```

Включение передачи данных в Linux

- Чтобы включить передачу данных для агента, установленного в Linux:

  1. Откройте файл `/etc/systemd/system/vxagent.service` для редактирования:

     ```
     sudo nano /etc/systemd/system/vxagent.service
     ```
  2. В группе параметров **Service** в значение параметра **ExecStart** добавьте ключ `-tracer=true`.
  3. Нажмите клавишу F2 и сохраните изменения в файле.
  4. Перезапустите агент:

     ```
     systemctl daemon-reload
     systemctl restart vxagent.service
     ```

22.3.2. 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 производителя.
  2. В панели слева нажмите  .
  3. В раскрывающемся списке сверху выберите источник данных **Loki**.

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

   Например, для поиска записей об ошибках в работе сервера агентов вы можете выбрать идентификатор сервера и уровень записи **ERROR** с помощью меток **server_id** и **level**.
7. Нажмите **Show logs**.

22.3.3. Работа с дашбордами

Дашборд в Grafana — это страница с графиками, диаграммами и прочей статистической информацией о работе той или иной IT-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 производителя.
  2. В левом верхнем углу нажмите **General / Home**.
  3. Выберите дашборд.

22.3.4. 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 производителя.
  2. В панели слева нажмите  .
  3. В раскрывающемся списке сверху выберите источник данных **VictoriaMetrics**.
  4. В поле **Metrics** введите метрику или выберите ее в списке.
  5. Нажмите **Run query**.

22.3.5. Смена пароля учетной записи в Elasticsearch

После установки системы вы можете сменить пароль учетной записи в сервисе Elasticsearch с помощью специального скрипта.

- Чтобы сменить пароль учетной записи в Elasticsearch:

  1. Перейдите в каталог `/opt/edr/` на управляющем сервере:
     ```
     cd /opt/edr/
     ```
  2. Запустите скрипт:
     ```
     sudo ./change_elastic_password.sh
     ```
  3. Введите новый пароль и нажмите клавишу Enter.

     Примечание. Пароль должен быть не короче 6 символов и содержать как минимум одну заглавную латинскую букву, одну цифру и один спецсимвол.

     Скрипт заменит пароль в конфигурационных файлах и перезапустит необходимые контейнеры.
  4. В манифесте `/opt/edr/manifest.json` в блоке параметров `observability` в значении параметра `MASTER_PASSWORD` введите новый пароль.

22.4. 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 22.4.1)

Настройка таблиц с данными (см. раздел 22.4.2)

Обновление данных в таблицах (см. раздел 22.4.3)

22.4.1. 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 выберите **Агенты**.
  2. В правом верхнем углу списка агентов нажмите .
  3. Выберите значения фильтров.

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

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

22.4.3. 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 выберите **Агенты**.
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.

22.5. 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 выберите **Агенты**.
  2. Если требуется, отфильтруйте агенты в таблице (см. раздел 22.4.1) и выберите столбцы для отображения (см. раздел 22.4.2).

     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.

22.6. Управление токенами доступа

Для обеспечения доступа приложений и сервисов к MaxPatrol EDR и безопасной передачи данных предусмотрены токены доступа. Вы можете создавать и отзывать токены доступа на управляющем сервере MaxPatrol EDR.

В этом разделе

22.6.1. Создание токена доступа

- Чтобы создать токен доступа:

  1. На управляющем сервере перейдите в каталог `/opt/edr/`.
     ```
     cd /opt/edr/
     ```
  2. Запустите скрипт для генерации токена:
     ```
     sudo ./register_client --privileges
     pt.edr.ui.services.api.view,pt.edr.ui.groups.api.view,pt.edr.ui.modules.interactive --
     client-id <Идентификатор приложения, которое будет использовать токен>
     ```

Например:

```
sudo ./register_client --privileges
pt.edr.ui.services.api.view,pt.edr.ui.groups.api.view,pt.edr.ui.modules.interactive --
client-id betman
```

Токен создан. Из сообщения скрипта скопируйте токен доступа и используйте его при настройке подключения соответствующего приложения к MaxPatrol EDR.

22.6.2. Отзыв токена доступа

Вы можете отозвать токен доступа, который был создан по ошибке или больше не нужен.

- Чтобы отозвать токен доступа:

1. На управляющем сервере перейдите в каталог `/opt/edr/`.

   ```
   cd /opt/edr/
   ```

2. Запустите скрипт для отзыва токена:

   ```
   sudo ./register_client --remove --client-id <Идентификатор приложения, использующего
   токен>
   ```

22.7. Журналирование изменения параметров контейнеров

Вы можете отслеживать изменение параметров контейнеров MaxPatrol EDR с помощью компонента auditd. Для этого необходимо добавить соответствующие правила журналирования. Журнал auditd хранится в файле `/var/log/audit/audit.log`.

Примечание. Инструкция дана для серверов под управлением Debian.

- Чтобы настроить журналирование:

1. На сервере MaxPatrol EDR установите компонент auditd:

   ```
   sudo apt-get install auditd
   ```

2. Запустите auditd:

   ```
   sudo systemctl start auditd
   sudo systemctl enable auditd
   ```

3. В файл `/etc/audit/rules.d/audit.rules` добавьте следующие строки:

   ```
   -w /run/containerd -p rwxa -k docker_changed
   -w /var/lib/docker -p rwxa -k docker_changed
   -w /etc/docker -p rwxa -k docker_changed
   -w <Полный путь до файла docker.service> -p rwxa -k docker_changed
   -w <Полный путь до файла containerd.sock> -p rwxa -k docker_changed
   -w <Полный путь до файла docker.socket> -p rwxa -k docker_changed
   -w /etc/default/docker -p rwxa -k docker_changed
   -w /etc/docker/daemon.json -p rwxa -k docker_changed
   -w /etc/containerd/config.toml -p rwxa -k docker_changed
   ```

```
-w /etc/sysconfig/docker -p rwxa -k docker_changed
-w /usr/bin/containerd -p rwxa -k docker_changed
-w /usr/bin/containerd-shim -p rwxa -k docker_changed
-w /usr/bin/containerd-shim-runc-v1 -p rwxa -k docker_changed
-w /usr/bin/containerd-shim-runc-v2 -p rwxa -k docker_changed
-w /usr/bin/runc -p rwxa -k docker_changed
```

4. Перезапустите auditd:

```
sudo systemctl restart auditd
```

22.8. Функция seccomp

Функция seccomp доступна для контейнеров MaxPatrol EDR во всех ОС, которые поддерживают модуль безопасности SELinux. Если бинарный файл `sestatus` расположен в каталоге `/usr/sbin/`, то функция seccomp по умолчанию включена. Если бинарный файл расположен в другом каталоге, то для включения функции нужно создать символическую ссылку от расположения бинарного файла `sestatus` до `/usr/sbin/sestatus`. Преднастроенный профиль `seccomp_profile.json` расположен в каталоге `/opt/edr/`.

23. Диагностика и решение проблем

В этом разделе приводятся инструкции по диагностике и решению проблем и устранению ошибок, возникающих при работе с MaxPatrol EDR.

В этом разделе

23.1. Расположение файлов журналов

Для анализа возникшей проблемы службе технической поддержки могут потребоваться файлы журналов. Для сбора файлов необходимо их скопировать, создать из скопированных файлов архив (со сжатием) и отправить его в службу технической поддержки.

Таблица 36. Расположение файлов журналов

Компонент		Расположение журнала
Управляющий сервер		`/var/log/edr/api-server/api.log`
Сервер агентов		`/var/log/edr/agent-server/server.log`
Агент	Windows	`C:\Program Files\Positive Technologies\EDR Agent\agent.log`
	Linux	`/opt/vxagent/logs/agent.log`
	macOS	`/Library/vxagent/logs/agent.log`

Примечание. Журнал установки продукта находится на сервере, с которого выполнялась установка, в файле `/var/log/edr_install.log`.

23.2. 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.

23.3. 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 15.4.6).

23.4. Один и тот же агент отображается на разных серверах агентов

Проблема

На разных серверах агентов отображаются агенты с одинаковым IP-адресом.

Возможные причины

На конечном устройстве агент был переустановлен, в параметрах был задан новый сервер агентов.

Решение

- Чтобы решить проблему,

  удалите агент на старом сервере агентов (см. раздел 15.4.7).

23.5. На одном сервере агентов отображаются два одинаковых агента с разными идентификаторами

Проблема

На одном сервере агентов отображаются два агента с одинаковыми IP-адресом и именем узла в названии.

Возможные причины

Такая ситуация может возникнуть:

— если агенты находятся в разных сетях с одинаковым IP-адресом и именем узла;

— агент установлен на виртуальной машине, которая была создана с помощью клонирования другой виртуальной машины, на которой также установлен агент.

Кроме того, если в сети, в которой находятся агенты, IP-адреса назначаются динамически, то может возникнуть ситуация, при которой в названии нескольких агентов будет одинаковый IP-адрес.

Решение

- Чтобы решить проблему,

  при необходимости переименуйте агенты.

23.6. 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».

23.7. Удаление MaxPatrol EDR завершилось с ошибкой

Проблема

Удаление MaxPatrol EDR 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`.

23.8. 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 выберите **Система** → **Дистрибутивы агентов**.
  3. Скачайте подходящий дистрибутив агента и установите его (см. раздел 15.2).

23.9. 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 15.4.1).
  2. Если ранее установленные агенты не отображаются в веб-интерфейсе MaxPatrol EDR, переустановите их (см. раздел 15.2).

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

23.10. 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.

23.11. Не запускается служба otelcontribcol.EDR-Application.Observability после установки продукта

Проблема

После установки MaxPatrol EDR не запускается служба `otelcontribcol.EDR-Application.Observability`, в журнале системы сообщение:

```
2025-04-08T16:07:42.016Z info service/service.go:163 Shutdown complete.
Error: cannot start pipelines: failed to load TLS config: failed to load CA CertPool: failed to load CA /etc/ssl/certs/rootCA.crt: open /etc/ssl/certs/rootCA.crt: no such file or directory
2025/04/08 16:07:42 collector server run finished with error: cannot start pipelines: failed to load TLS config: failed to load CA CertPool: failed to load CA /etc/ssl/certs/rootCA.crt: open /etc/ssl/certs/rootCA.crt: no such file or directory
```

Возможные причины

Установочный скрипт не смог получить сертификаты PT MC.

Решение

- Чтобы решить проблему:

  1. Скопировать на сервер, с которого осуществляется установка, сертификаты из каталога `/var/lib/deployed-roles/mc-application/managementandconfiguration-<Идентификатор>/certs/` на сервере с PT MC.
  2. В манифест (см. раздел 6.4) в группу параметров `hosts` для сервера, на котором будет установлен компонент `observability`, добавить группу параметров `mc_otel_certs`.
  3. Повторить установку.

Пример конфигурации группы параметров `mc_otel_certs`:

```
"mc_otel_certs": {
"cert": "/home/user/Portal.crt",
"key": "/home/user/Portal.key",
"root_ca": "/home/user/rootCA.crt"
},
```

Внимание! Имя файла корневого сертификата должно быть `rootCA.crt`.

23.12. Не удалось завершить обновление MaxPatrol EDR в Astra Linux

Проблема

Обновление MaxPatrol EDR в Astra Linux прошло неуспешно, не запускается объектное хранилище MinIO.

Возможные причины

В операционной системе превышен лимит inotify.

Решение

- Чтобы решить проблему:

  1. В файл `/etc/sysctl.conf` добавьте следующие строки:
     ```
     fs.inotify.max_user_instances = 768
     fs.inotify.max_user_watches = 824288
     ```
  2. Загрузите параметры ядра:
     ```
     sudo sysctl -p
     ```
  3. В файле `/etc/security/limits.conf` установите следующие ограничения для пользователя root:
     ```
     root      hard      nofile      500000
     root      soft      nofile      500000
     ```
  4. Перезагрузите компьютер.
  5. Повторите обновление.

24. О технической поддержке

Базовая техническая поддержка доступна для всех владельцев действующих лицензий на MaxPatrol EDR в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продукта

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies поставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках технической поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

> **Примечание.** Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются на портале технической поддержки.

Портал технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к порталу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Техническая поддержка на портале предоставляется на русском и английском языках.

Условия предоставления технической поддержки

Для получения технической поддержки необходимо оставить заявку на портале технической поддержки и предоставить следующие данные:

— номер лицензии на использование продукта;

— файлы журналов и наборы диагностических данных, которые требуются для анализа;

— снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг технической поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по технической поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по технической поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 37. Время реакции на заявку

Уровень значимости заявки	**Критерии значимости заявки**	**Время реакции на заявку**
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист технической поддержки сообщает вам:

— о ходе диагностики по заявленной проблеме и ее результатах;

— планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

— предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;

— заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;

— заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.

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 38. 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. Конфигурация локального сервера обновлений

Ниже приведен пример конфигурационного файла `/etc/pt-update-mirror/config.json` с репозиториями MaxPatrol EDR. Если вы обновляете другие продукты с помощью локального зеркала, в блок параметров `products` вам нужно добавить соответствующие репозитории.

```
{
"db-path": "/var/opt/pt/pt-update-mirror",
"log-level": "INFO",
"logrotate": "daily",
"proxy": "",
"proxy-password": "",
"proxy-user": "",
"update-server": "https://update.ptsecurity.com",
"products": {
    "MP.EDR": {
      "synchronizer": "ComponentSynchronyzer",
      "count_number_on_version_parse": 2,
      "minimal_release": "6.0",
      "store_release_versions": 1
    },
    "MP.EDR.KB.7.0": {
      "synchronizer": "DockerSynchronizer",
      "count_number_on_version_parse": 2,
      "store_release_versions": 1
    },
    "MP.EDR.CorrelatorLinuxRules.v26.2": {
      "synchronizer": "ComponentSynchronizer",
      "count_number_on_version_parse": 2,
      "store_release_versions": 1
    },
    "MP.EDR.CorrelatorRules.v26.2": {
      "synchronizer": "ComponentSynchronizer",
      "count_number_on_version_parse": 2,
      "store_release_versions": 1
    },
    "MP.EDR.NormalizerRules.v26.2": {
      "synchronizer": "ComponentSynchronizer",
      "count_number_on_version_parse": 2,
      "store_release_versions": 1
    },
    "EDR.YARARules": {
      "synchronizer": "ComponentSynchronizer",
      "count_number_on_version_parse": 2,
```

```
      "store_release_versions": 1
    },
    "EDR.HashChecker": {
      "synchronizer": "ComponentSynchronizer",
      "count_number_on_version_parse": 2,
      "store_release_versions": 1
    }
  }
}
```

Приложение В. Совместимость модулей и операционных систем

Таблица 39. Совместимость модулей и операционных систем

Модуль	Windows	Linux	macOS[11]
Системные модули			
Ядро (внутренний сервис)	+	+	+
Модули доставки и установки			
Установщик Sysmon	+	—	—
Установщик auditd	—	+	—
Конфигуратор аудита Windows	+	—	—
Модули сбора			
WinEventLog: сбор данных из журнала событий Windows	+	—	—
ETW: трассировка событий Windows	+	—	—
Сбор данных из файлов журналов	+	+	—
Сбор данных о состоянии системы	+	—	—
Нормализатор	+	+	—
Модули обнаружения			
Коррелятор	+	+	—
YARA-сканер	+	+	—
Проверка файлов по хеш-сумме	+	+	—
Обнаружение подозрительных файлов	+	+	—
Модули реагирования			
Удаление файлов	+	+	+
Завершение процессов	+	+	+
Блокировка учетных записей	+	+	—
Изоляция узлов	+	+	—
Блокировка по IP-адресу	+	—	—
Завершение работы	+	+	—

11 Автоматическое реагирование в macOS недоступно.

Модуль	Windows	Linux	macOS[11]
Перенаправление DNS-запросов (sinkholing)	+	+	+
Карантин	+	+	+
Запуск командной оболочки	+	+	—
Интерпретатор языка Lua	+	+	+
Модули интеграции			
Проверка файлов в PT Sandbox	+	+	—
Сканирование в режиме аудита (MaxPatrol VM)	+	+	—
Отправка событий на syslog-сервер	+	+	+
Отправка файлов	+	+	+

Приложение Г. Привилегии пользователей MaxPatrol EDR

Таблица 40. Привилегии пользователей MaxPatrol EDR

Привилегия	Описание
Агенты	
Создание	Не применяется в этой версии MaxPatrol EDR
Удаление	Удаление агентов
Изменение	Обновление, блокировка и изменение параметров агентов
Просмотр	Доступ к странице **Агенты**
Дистрибутивы	Доступ к странице **Дистрибутивы агентов**
Группы агентов	
Создание	Создание групп
Удаление	Удаление групп
Изменение	Изменение параметров групп
Просмотр	Доступ к странице **Группы агентов**
Модули	
Создание	Создание модулей
Удаление	Удаление модулей
Изменение	Изменение модулей
Просмотр	Доступ к странице **Модули** и к параметрам модулей в политиках
Экспорт	Экспорт модулей
Импорт	Импорт модулей
События ИБ	Не применяется в этой версии MaxPatrol EDR
Ручное реагирование	Ручное реагирование на угрозы
Просмотр защищенных параметров	Просмотр защищенных параметров модулей в политиках
Изменение защищенных параметров	Изменение защищенных параметров модулей в политиках
Массовое реагирование	Ручное реагирование на угрозы сразу на нескольких агентах или группах агентов
Политики	

Привилегия	Описание
Создание	Создание политик
Удаление	Удаление политик
Изменение	Изменение политик
Просмотр	Доступ к странице **Политики**
Назначение на группу	Назначение политик на группы агентов
Серверы агентов	
Создание	Не применяется в этой версии MaxPatrol EDR
Удаление	
Изменение	Изменение параметров серверов агентов
Просмотр	Доступ к странице **Серверы агентов**
Система	
Резервное копирование и восстановление конфигурации	Резервное копирование и восстановление конфигурации MaxPatrol EDR
Управление лицензиями	Генерация фингерпринта, загрузка и активация лицензий
Просмотр лицензий	Доступ к странице **Лицензии**
Задачи с агентами (планировщик)	
Создание	Создание задач
Просмотр	Доступ к странице **Планировщик задач**
Изменение	Изменение задач
Удаление	Удаление задач
Шаблоны политик	
Просмотр	Доступ к странице **Шаблоны политик**
Управление	Создание, импортирование и экспортирование шаблонов политик
Пользовательская экспертиза	
Управление	Загрузка, обновление и удаление наборов экспертизы

Глоссарий

агент

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

группа агентов

Один или несколько агентов, 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 — один из лидеров в области 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 около 3000 организаций по всему миру. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.