MaxPatrol EDR версия 5.0

Начало работы

Дата редакции документа: 03.10.2023

Содержание

1. Об этом документе ... 4
2. О MaxPatrol EDR ... 5
3. Архитектура и алгоритм работы MaxPatrol EDR ... 6
4. Вход в MaxPatrol EDR через PT MC ... 7
5. Интерфейс MaxPatrol EDR ... 8
6. Порядок настройки MaxPatrol EDR ... 9
7. Авторизация агента ... 10
8. Шаблоны политик ... 12
9. Создание политики ... 14
10. Настройка модулей в политике ... 15
    - 10.1. Настройка модуля «WinEventLog: сбор данных из журнала событий Windows» ... 15
    - 10.2. Настройка модуля «Проверка файлов в PT Sandbox» ... 16
    - 10.3. Настройка модуля «Сканирование в режима аудита (MaxPatrol VM)» ... 17
    - 10.4. Настройка модуля «Коррелятор» ... 18
        - 10.4.1. Передача данных в модуль «Коррелятор» ... 19
        - 10.4.2. Передача данных в модуль «Коррелятор (Linux)» ... 19
        - 10.4.3. Добавление исключений ... 19
    - 10.5. Настройка модуля «Перенаправление DNS-запросов (sinkholing)» ... 21
11. Настройка автоматического реагирования ... 23
    - 11.1. Назначение действий на событие модуля ... 23
    - 11.2. Массовое назначение действия на события модуля ... 24
12. Назначение политики на группу агентов ... 27
13. Обращение в службу технической поддержки ... 29
    - 13.1. Техническая поддержка на портале ... 29
    - 13.2. Время работы службы технической поддержки ... 29
    - 13.3. Как служба технической поддержки работает с запросами ... 30
        - 13.3.1. Предоставление информации для технической поддержки ... 30
        - 13.3.2. Типы запросов ... 30
        - 13.3.3. Время реакции и приоритизация запросов ... 31
        - 13.3.4. Выполнение работ по запросу ... 33

Глоссарий ... 34

1. Об этом документе

Это руководство содержит информацию и инструкции для первоначальной настройки MaxPatrol Endpoint Detection and Response (далее также — MaxPatrol EDR).

Комплект документации MaxPatrol EDR включает в себя следующие документы:

— Этот документ.

— Руководство администратора — содержит справочную информацию и инструкции по развертыванию, настройке и администрированию MaxPatrol EDR.

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

2. О MaxPatrol EDR

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

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

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

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

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

— удалить файл;

— завершить один или несколько процессов;

— заблокировать сетевой трафик;

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

— отправить файл на проверку в PT Sandbox;

— отправить данные о событиях ИБ на syslog-сервер.

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

3. Архитектура и алгоритм работы MaxPatrol EDR

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

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

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

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

Алгоритм работы MaxPatrol EDR:

1. Сервер агентов передает на агенты модули и их конфигурацию.
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 на сервер агентов.
9. Управляющий сервер получает обновления продукта и пакетов экспертизы с сервера обновлений.

4. Вход в MaxPatrol EDR через PT MC

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

► Чтобы войти в MaxPatrol EDR:

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

   Откроется страница входа в PT MC.

2. Выполните одно из следующих действий:

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

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

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

4. Нажмите кнопку **Войти**.

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

5. Интерфейс MaxPatrol EDR

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

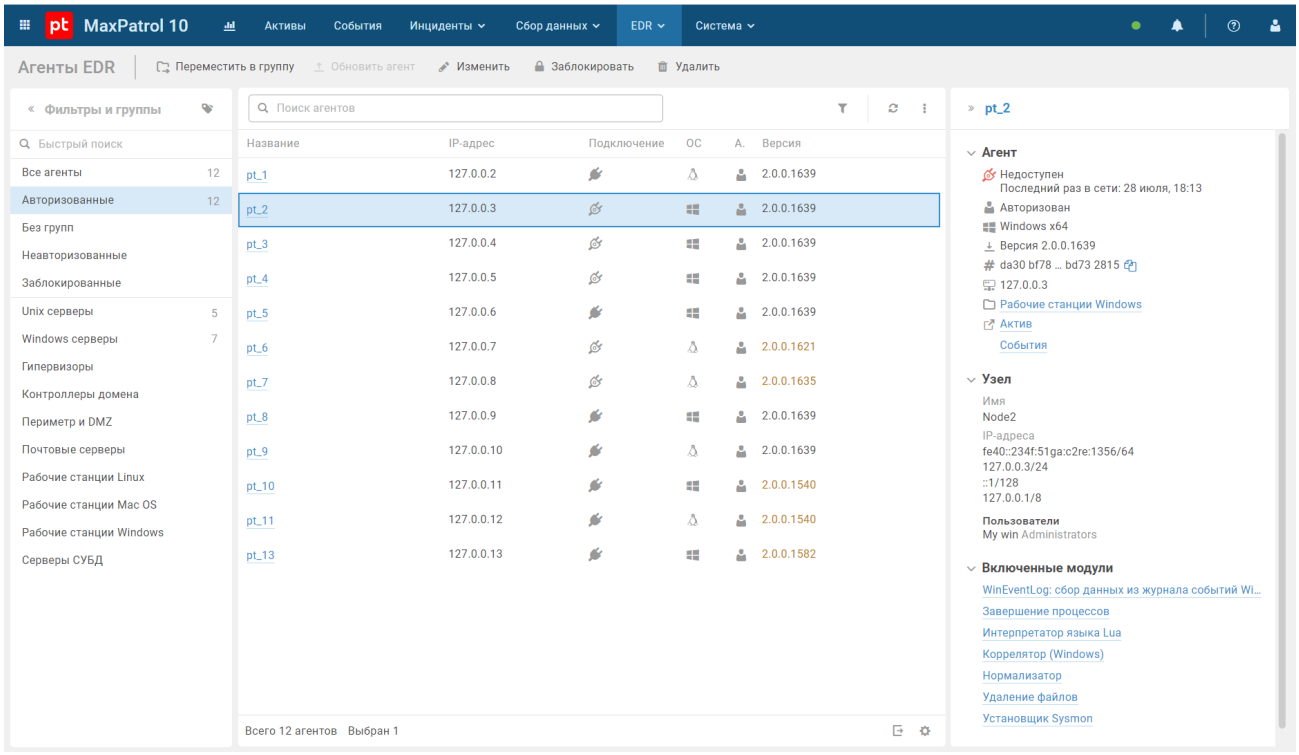

Рисунок 1. Страница **Агенты EDR**

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

6. Порядок настройки MaxPatrol EDR

После установки MaxPatrol EDR и агентов вам нужно:

1. Авторизовать агенты (см. раздел 7). При авторизации агент добавляется в группу. Вы можете использовать стандартные группы или добавить свои.
2. Создать политики с помощью встроенных шаблонов (см. раздел 9).
3. Настроить модули в политиках (см. раздел 10). В частности, вам нужно настроить интеграцию с PT Sandbox, а также модули «Коррелятор» и «WinEventLog: сбор данных из журнала событий Windows».
4. В параметрах политики назначить автоматические действия (см. раздел 11), которые будут выполняться при регистрации событий ИБ.
5. Назначить политики на группы агентов (см. раздел 12). Сразу после назначения политик на агентах будут установлены и запущены модули.

7. 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.

- Чтобы авторизовать агент:

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

     Откроется страница **Агенты EDR**.

  2. Выберите фильтр **Неавторизованные**.

  3. Выберите агент.

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

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

     Откроется всплывающее окно со списком групп.

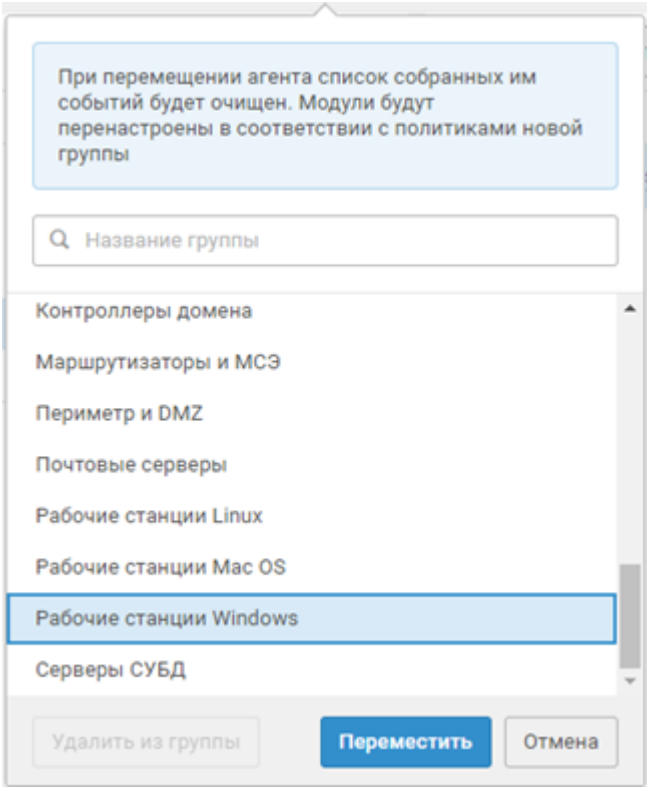

Рисунок 2. Выбор группы

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

Агент авторизован.

8. Шаблоны политик

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

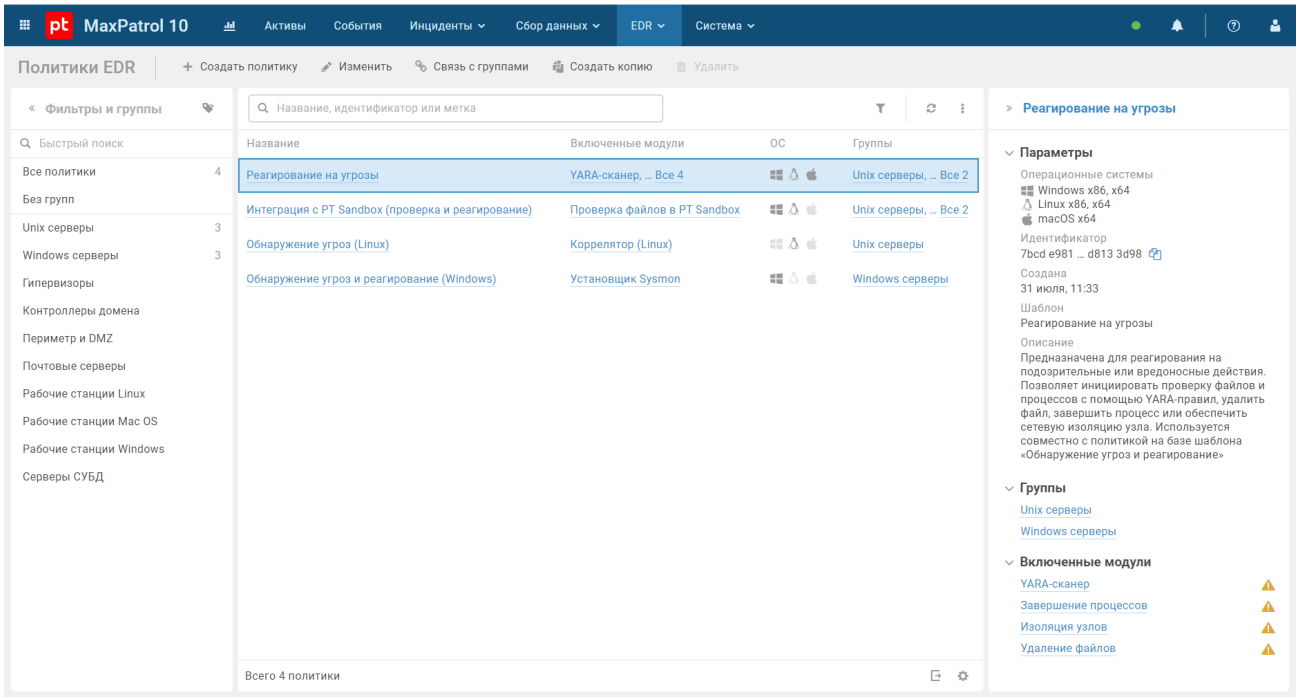

Рисунок 3. Стандартные политики

Таблица 1. Шаблоны политик

Название	Описание	Модули
Обнаружение угроз и реагирование (Windows)	Политики на базе этого шаблона предназначены для обнаружения угроз на агентах под управлением Windows и автоматического реагирования на них. Для обнаружения угроз используются данные утилиты Sysmon (основной источник), журнала безопасности, Windows PowerShell и Windows Defender. При обнаружении подозрительных или вредоносных действий такие политики позволяют инициировать проверку файлов и процессов с помощью YARA-правил, удалить файл, завершить процесс или обеспечить сетевую изоляцию узла. Эти политики используются совместно с политиками, в которые входят модули реагирования, например с политикой на базе шаблона «Реагирование на угрозы»	«Коррелятор (Windows)», «WinEventLog: сбор данных из журнала событий Windows», «Установщик Sysmon», «Нормализатор»

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

9. Создание политики

Вы можете создавать политики на базе шаблонов (см. раздел 8) или пустые. В политиках, которые созданы на базе шаблонов, добавлены модули 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, сконфигурировать их (см. раздел 10) и настроить автоматические действия (см. раздел 11).

- Чтобы создать политику:

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

     Откроется страница **Политики EDR**.

  2. Нажмите кнопку **Создать политику**.

     Откроется окно **Новая политика**.

  3. В раскрывающемся списке **Шаблон** выберите шаблон (см. раздел 8), на базе которого вы хотите создать политику.

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

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

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

  6. Нажмите кнопку **Создать**.

  Политика создана.

Вы также можете создавать копии существующих политик.

10. Настройка модулей в политике

В разделе приведены инструкции по настройке некоторых модулей в политике. При настройке других модулей вы можете использовать описание их параметров.

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

В этом разделе

Настройка модуля «WinEventLog: сбор данных из журнала событий Windows» (см. раздел 10.1)

Настройка модуля «Проверка файлов в PT Sandbox» (см. раздел 10.2)

Настройка модуля «Сканирование в режима аудита (MaxPatrol VM)» (см. раздел 10.3)

Настройка модуля «Коррелятор» (см. раздел 10.4)

Настройка модуля «Перенаправление DNS-запросов (sinkholing)» (см. раздел 10.5)

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

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

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

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

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

   Отобразится список параметров модуля.

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

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

5. Нажмите кнопку **Сохранить**.

Модуль настроен.

10.2. Настройка модуля «Проверка файлов в PT Sandbox»

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

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

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

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

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

   Отобразится список параметров, событий и действия модуля.

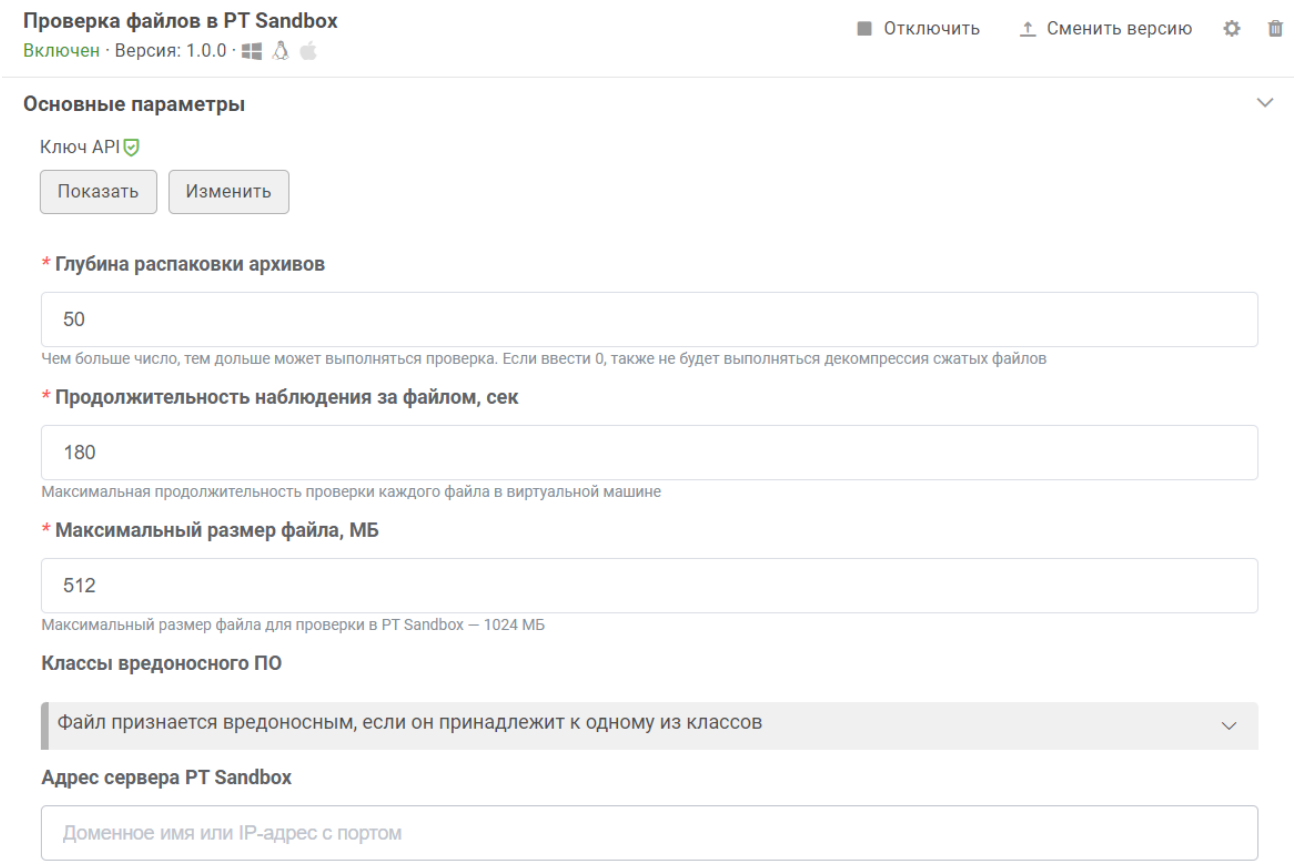

Рисунок 4. Настройка модуля «Проверка файлов в PT Sandbox»

4. В поле **Адрес сервера PT Sandbox** введите адрес сервера PT Sandbox, на который вы хотите отправлять файлы.
5. В поле **Ключ API** введите ключ для доступа к публичному API PT Sandbox.

Примечание. Для генерации ключа API вам нужно выполнить команду `sudo ptmsctl api auth create <Название ключа API>` в консольной утилите PT Sandbox. Подробная инструкция по генерации ключа API приведена в разделе «Генерация ключа API» 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 11).
8. Нажмите кнопку **Сохранить**.

Модуль настроен.

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

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

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

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

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

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

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

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

   Отобразится список параметров, событий и действия модуля.

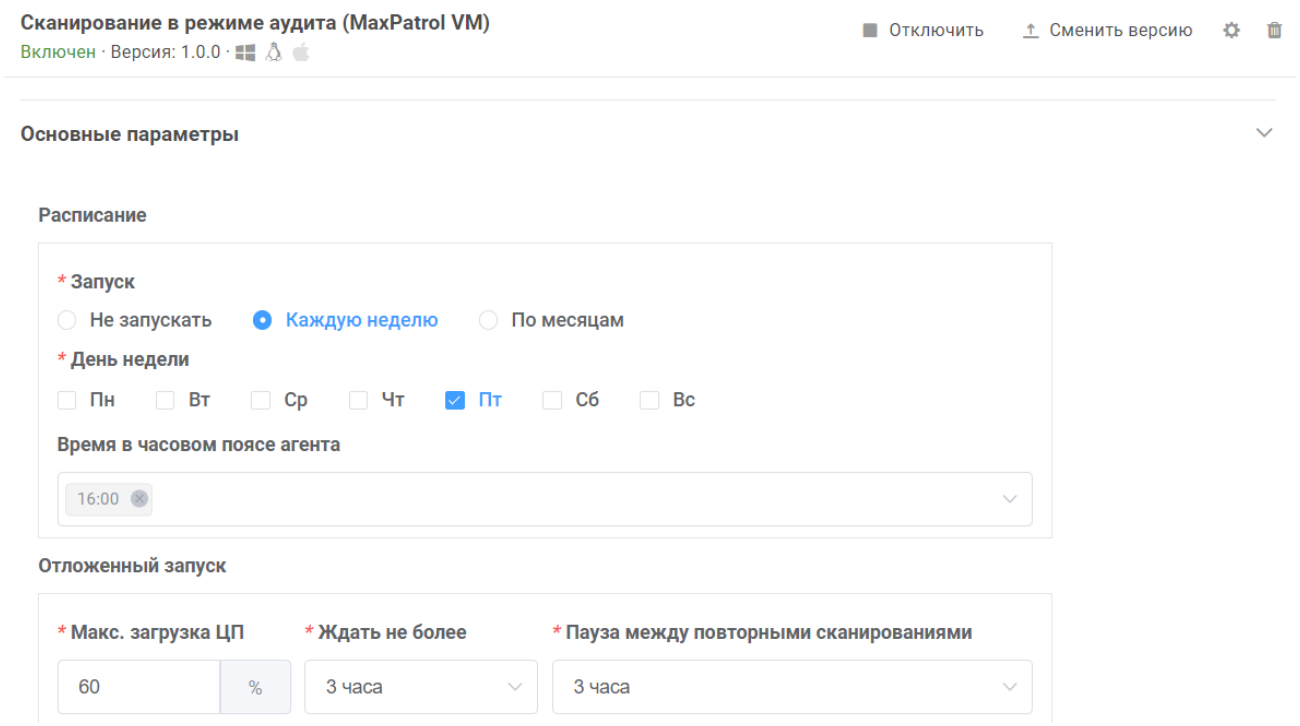

Рисунок 5. Настройка модуля «Сканирование в режиме аудита (MaxPatrol VM)»

4. В блоке параметров **Расписание** настройте запуск сканирования по расписанию.
5. Если требуется, задайте дополнительные параметры модуля.
6. Если требуется, выберите действия, которые будут выполняться при регистрации событий ИБ (см. раздел 11).
7. Нажмите кнопку **Сохранить**.

Модуль настроен.

10.4. Настройка модуля «Коррелятор»

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

В этом разделе

Передача данных в модуль «Коррелятор» (см. раздел 10.4.1)

Передача данных в модуль «Коррелятор (Linux)» (см. раздел 10.4.2)

Добавление исключений (см. раздел 10.4.3)

10.4.1. Передача данных в модуль «Коррелятор»

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

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

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

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

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

— вручную установить и настроить на конечных устройствах компонент auditd;

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

10.4.3. Добавление исключений

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

► Чтобы добавить исключение:

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

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

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

   Отобразится список параметров, событий и действия модуля.

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

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

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

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

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

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

Рисунок 6. Добавление исключения

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

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

8. Если требуется, настройте дополнительные условия.

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

9. Нажмите кнопку **Сохранить**.

Исключение добавлено.

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

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

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

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

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

   Отобразится список параметров, событий и действия модуля.

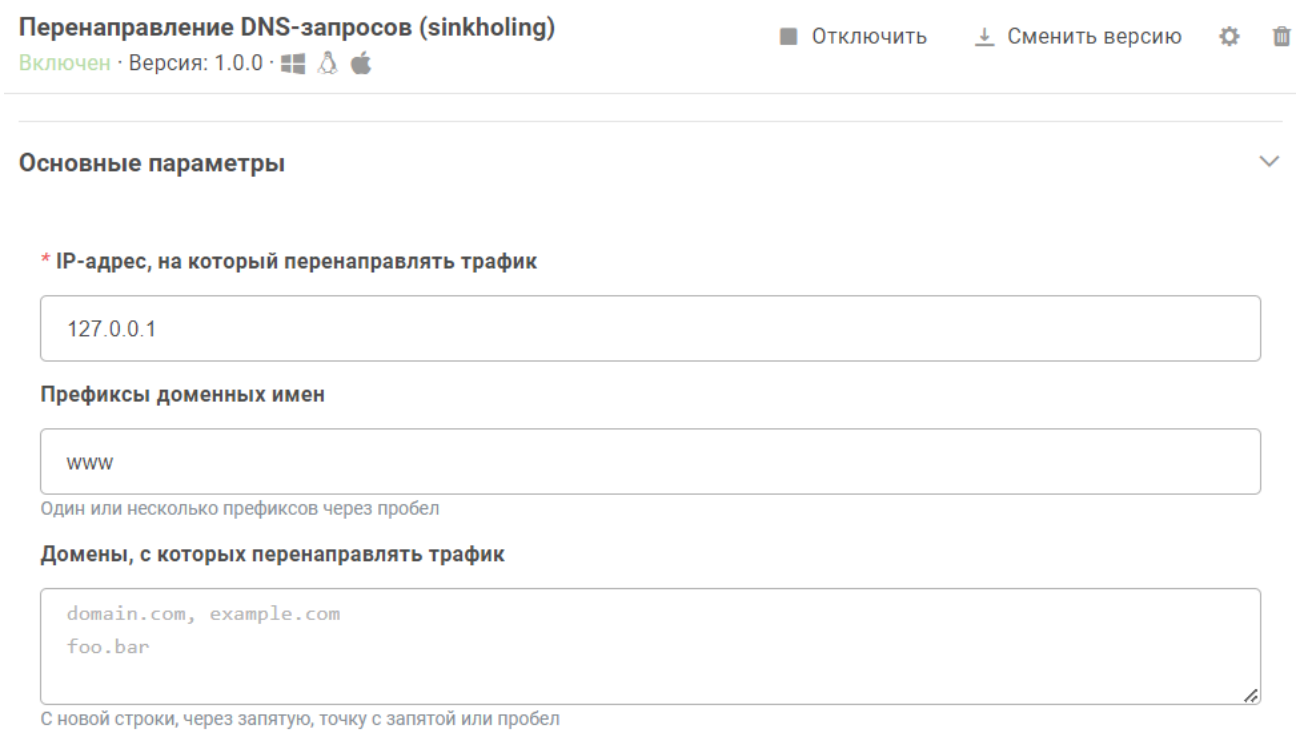

Рисунок 7. Настройка модуля «Перенаправление DNS-запросов (sinkholing)»

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

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

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

Трафик будет перенаправляться со всех адресов заданных доменов.

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

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

7. Нажмите кнопку **Сохранить**.

Модуль настроен.

11. 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 11.1);

— выбрав для действия события, при регистрации которых его нужно выполнять (см. раздел 11.2).

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 11.1)

Массовое назначение действия на события модуля (см. раздел 11.2)

11.1. Назначение действий на событие модуля

► Чтобы назначить действия на событие модуля:

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

   Откроется страница **Политики EDR**.

2. Нажмите на название политики.

   Откроется карточка политики.

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

4. В блоке параметров **События** напротив нужного события нажмите .

   Откроется окно **Назначение действий**.

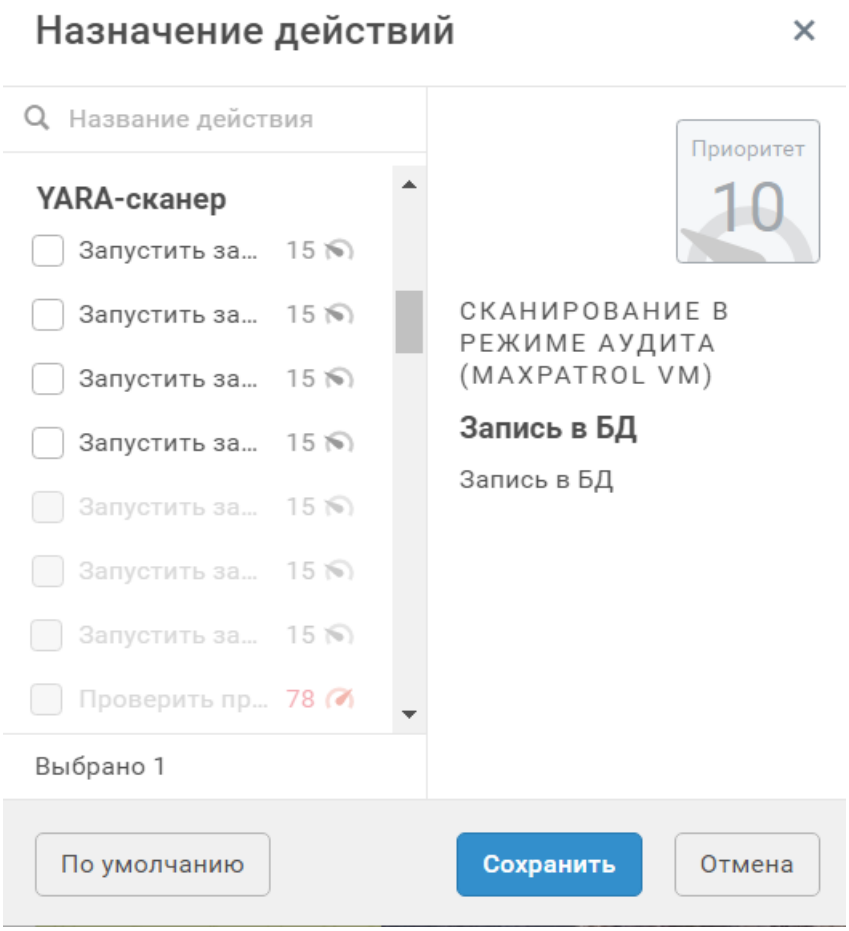

Рисунок 8. Назначение действий

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

Действия назначены.

11.2. Массовое назначение действия на события модуля

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

► Чтобы назначить действие на события модуля:

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

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

   Откроется карточка политики.

3. В списке **Включенные** выберите модуль, на события которого вы хотите назначить действия.
4. В блоке параметров **События** нажмите кнопку **Мастер назначения действий**.

   Откроется окно **Мастер назначения действий**.

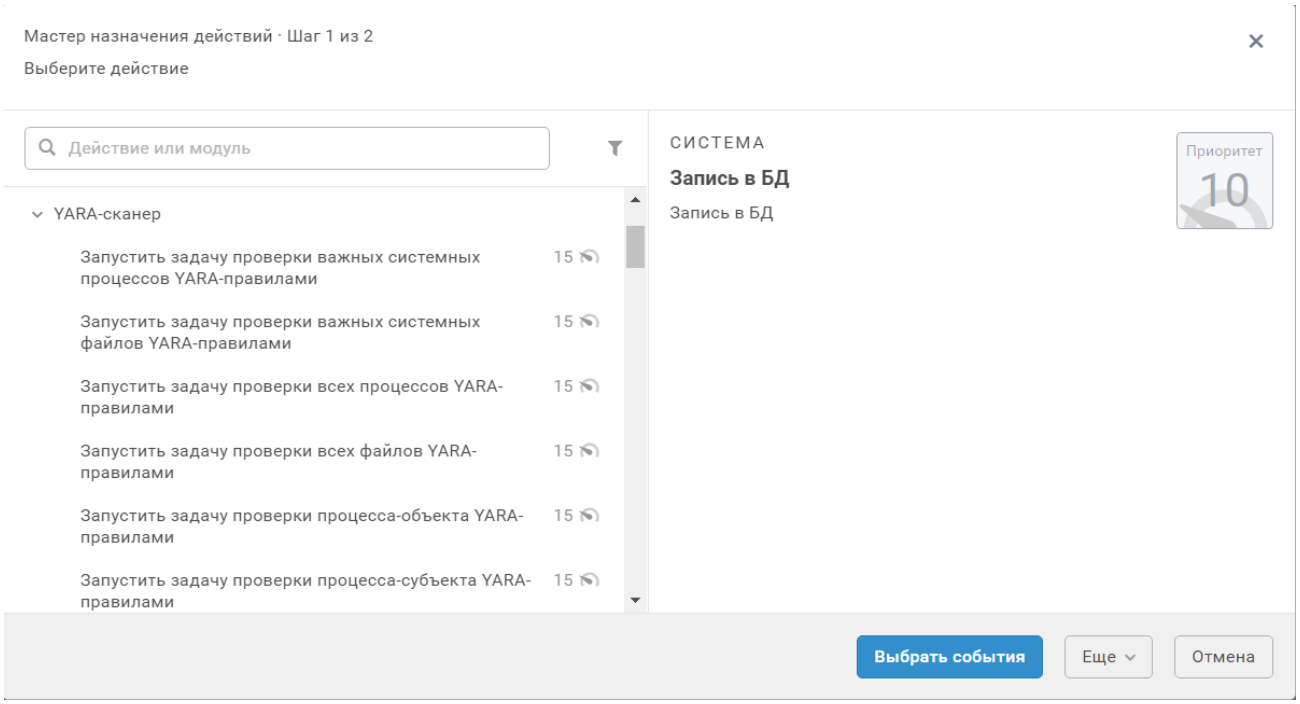

Рисунок 9. Выбор действия

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

   Примечание. Вы можете отфильтровать действия и изменить их группировку по кнопке .
6. Нажмите кнопку **Выбрать события**.

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

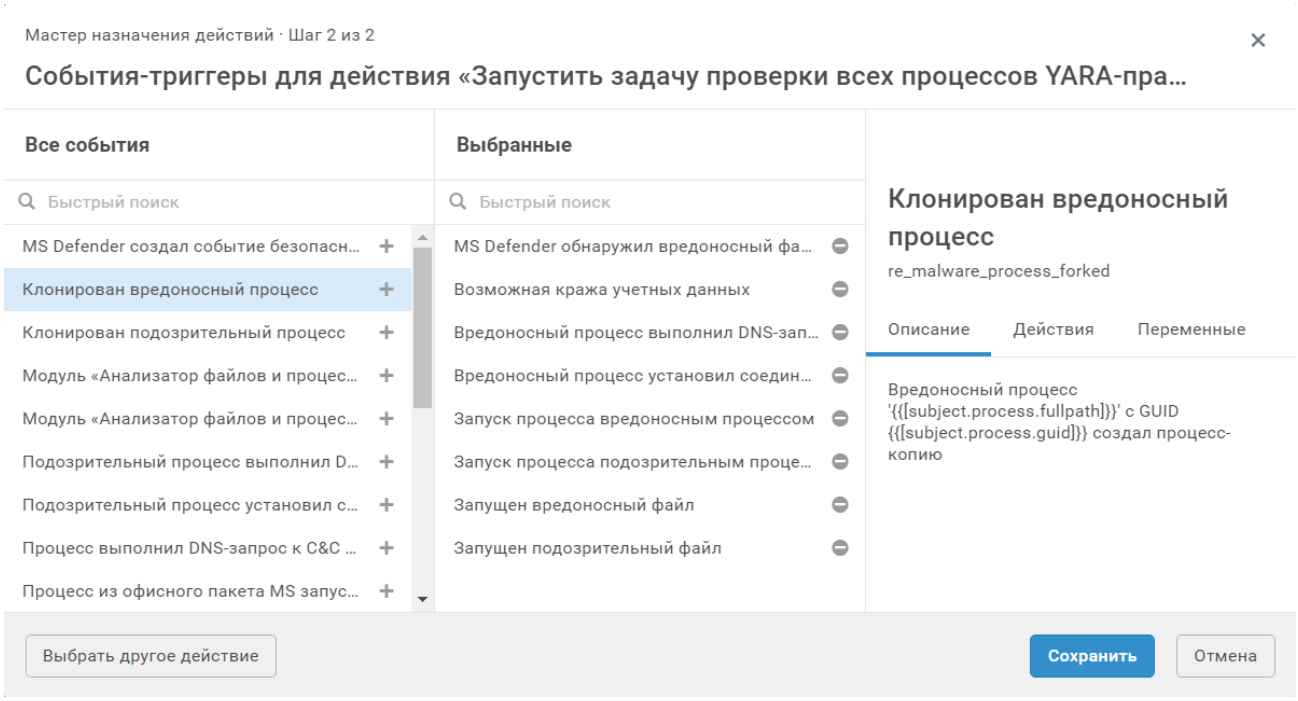

Рисунок 10. Выбор событий

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

Действие назначено на события модуля.

12. Назначение политики на группу агентов

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

- Чтобы назначить политику на группу:

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

     Откроется страница **Политики EDR**.

  2. Выберите политику.

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

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

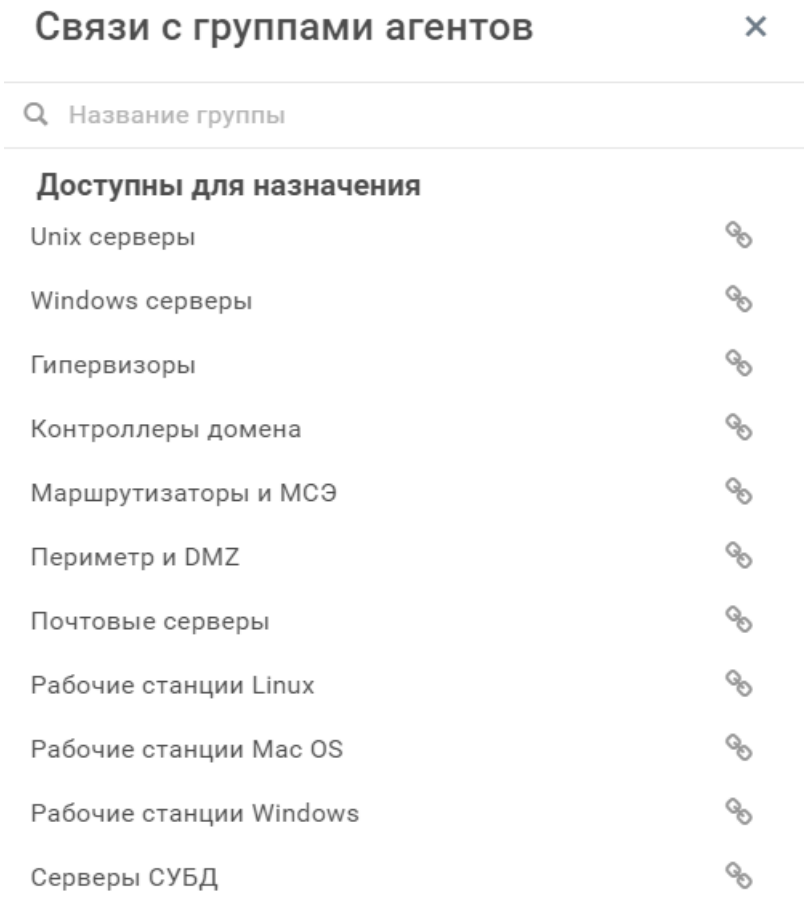

Рисунок 11. Назначение политики на группу агентов

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

Политика назначена на группу.

13. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

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

Вы можете получать техническую поддержку на портале.

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

В этом разделе

Техническая поддержка на портале (см. раздел 13.1)

Время работы службы технической поддержки (см. раздел 13.2)

Как служба технической поддержки работает с запросами (см. раздел 13.3)

13.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

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

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

Техническая поддержка на портале предоставляется на русском и английском языках.

13.2. Время работы службы технической поддержки

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

13.3. Как служба технической поддержки работает с запросами

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

В этом разделе

Предоставление информации для технической поддержки (см. раздел 13.3.1)

Типы запросов (см. раздел 13.3.2)

Время реакции и приоритизация запросов (см. раздел 13.3.3)

Выполнение работ по запросу (см. раздел 13.3.4)

13.3.1. Предоставление информации для технической поддержки

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

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

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

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

13.3.2. Типы запросов

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

Вопросы по установке, повторной установке и предстартовой настройке продукта

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

Вопросы по администрированию и настройке продукта

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

Восстановление работоспособности продукта

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

Обновление продукта

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

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

Устранение дефектов продукта

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

13.3.3. Время реакции и приоритизация запросов

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

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

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 2).

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

Таблица 2. Время реакции на запрос и время его обработки

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

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

13.3.4. Выполнение работ по запросу

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

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

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

Работы по запросу считаются выполненными, если:

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

Глоссарий

агент EDR

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

группа агентов EDR

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

действие модуля

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

зависимость

Условие, которое должно выполняться для корректной работы модуля агента.

конечное устройство

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

модуль агента

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

модуль доставки и установки

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

модуль обнаружения

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

модуль реагирования

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

модуль сбора

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

поведенческий анализ

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

политика конфигурации модулей агентов

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

приоритет действия

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

сервер агентов

Серверное приложение, предназначенное для управления агентами и модулями.

управляющий сервер

Серверное приложение, предназначенное для управления конфигурацией системы.

positive
technologies

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