Владимир Яцюк
Positive Technologies

Что умеет обновленный MaxPatrol EDR

Снова инцидент, а почему?

Не отреагировали вовремя

×

Не подключили источники или собрали не всё

Не устранили уязвимости

↗

Не было инструментов и процессов

Защитите конечные устройства: чек-лист

> Сбор данных

- События собираются со всех устройств?
- Достаточно ли этих событий для выявления атак?
- Вы можете оперативно корректировать профиль мониторинга?
- У вас есть информация о самих узлах?
  Кто за ними работает?
  Какой софт на них установлен?
  Как они настроены?
- А если сотрудники работают удаленно?

> Выявление

- Есть ли у вас инструменты для оперативного выявления угроз?
- Вы уверены в качестве обнаружения?
- Можете обработать весь поток инцидентов и уведомлений?
- Достаточно ли быстро можете проанализировать ситуацию и подтвердить инцидент?

> Реагирование

- Есть ли инструменты для реагирования? Достаточно ли вариантов действий?
- Можете ли локализовать инцидент быстро?
- Нужно ли привлекать ИТ или внешнего подрядчика?
- Можете ли автоматизировать реагирование?
- А в тех случаях, когда у агента нет связи с сервером?

В чем сила, EDR?

обнаружение
полнота сбора
точность
корреляция
потребление
YARA
интеграции
реагирование
скорость
мониторинг подключения
модули
шаблоны
автоматизация
удобство
алерты
экспертиза
политики
автономность
IoC
управляемость
карантин
изоляция
простота администрирования
API
сканирование

Динамичное развитие в 2025

8.0

- Обновили и ускорили интерфейс
- Упростили развертывание агентов
- Снизили потребление ресурсов
- Поддержали несколько новых ОС
- Научили агент делать дампы процессов
- Добавили полезные настройки серверов
- Исправили многие неприятные баги

8.2

- Облегченная установка с собственным хранилищем

Июнь 2025 | Июль 2025 | Август 2025 | Сентябрь 2025 | **Октябрь 2025** | Ноябрь 2025 | Декабрь 2025

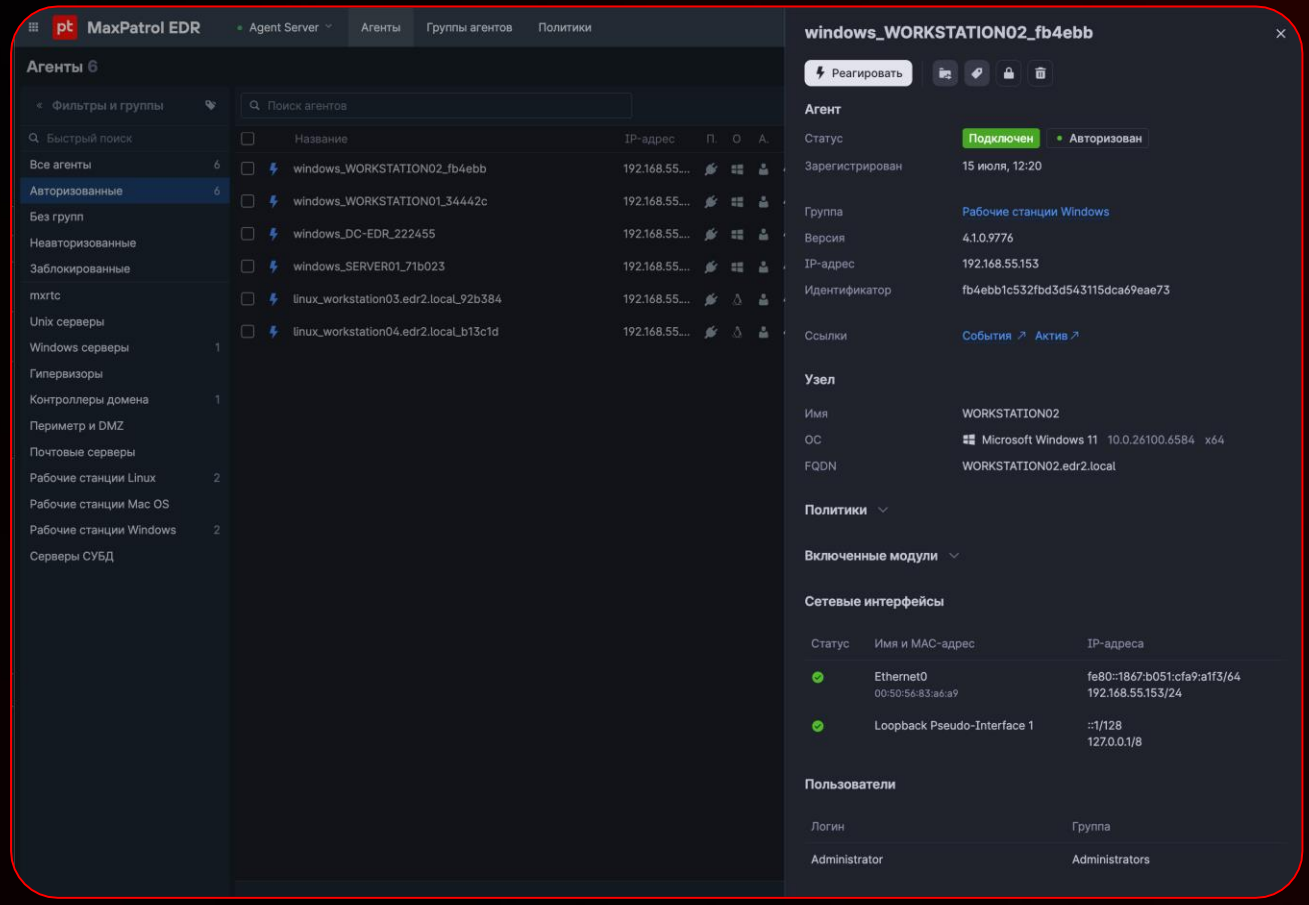
8.1

- Сделали UI реагирования еще удобнее
- Дали аналитикам больше контекста при реагировании
- Расширили возможности работы с файлами
- Сделали карточку агента более информативной
- Добавили деталей в карточку задания PT Sandbox
- Еще улучшили производительность
- Расширили возможности интеграции по Syslog

9.0

Новый интерфейс и оптимизация

- Поддержан актуальный фреймворк и дизайн-система
  - Koobiq 18
  - Angular 18
- EDR вынесен в отдельный интерфейс
- Новая, информативная карточка агента
- Темная тема

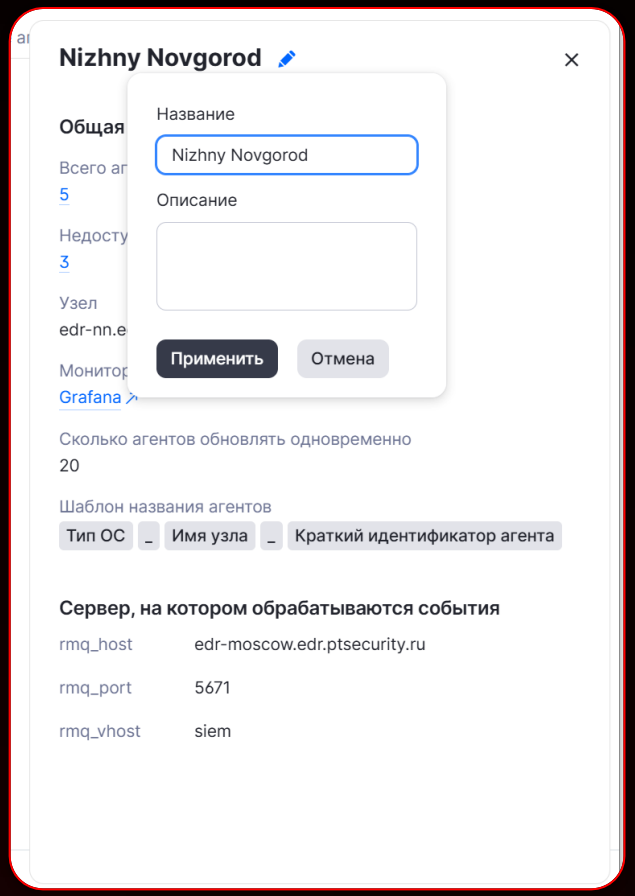


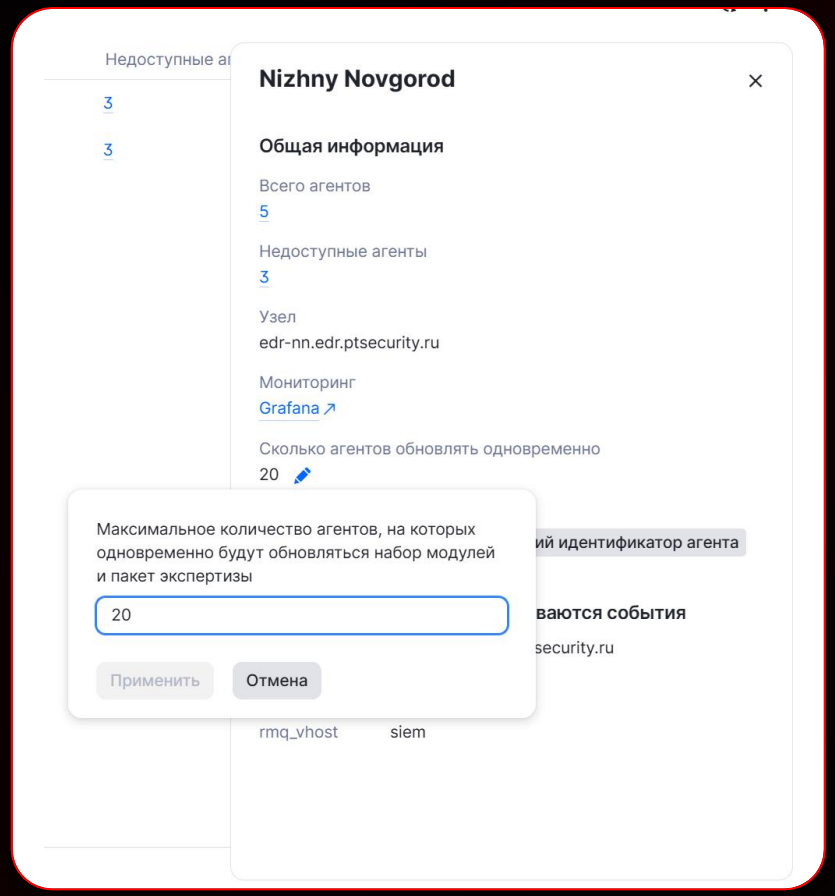
Управляйте серверами агентов

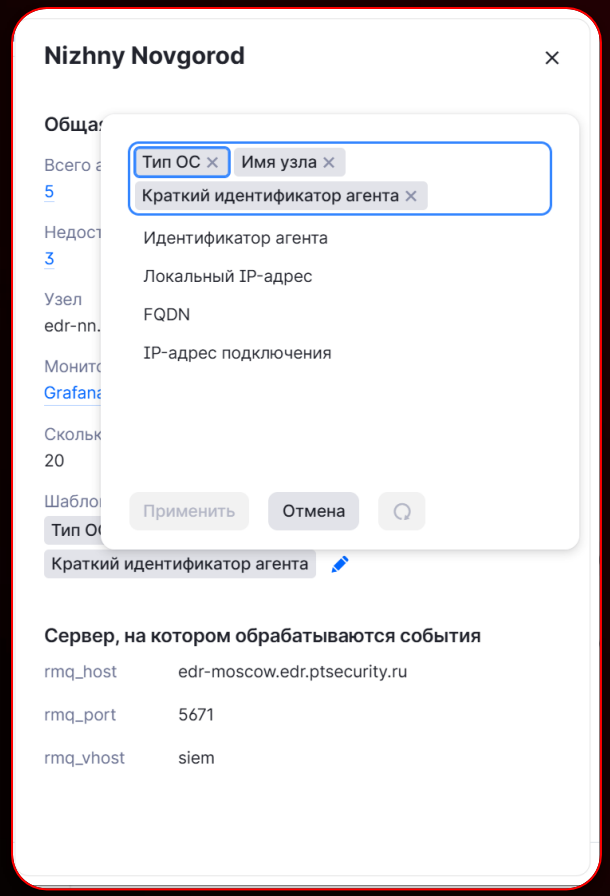
> Добавили:

- Состояние подключения сервера агентов
- Удобный список серверов агентов
- Редактируемые имя и описание серверов
- Переход в мониторинг (Grafana) в один клик
- Редактируемые шаблоны именования агентов
- Возможность ограничения
  - количества обновляемых агентов (для сервера)
  - нагрузки на сеть (для группы)

Управляйте серверами агентов



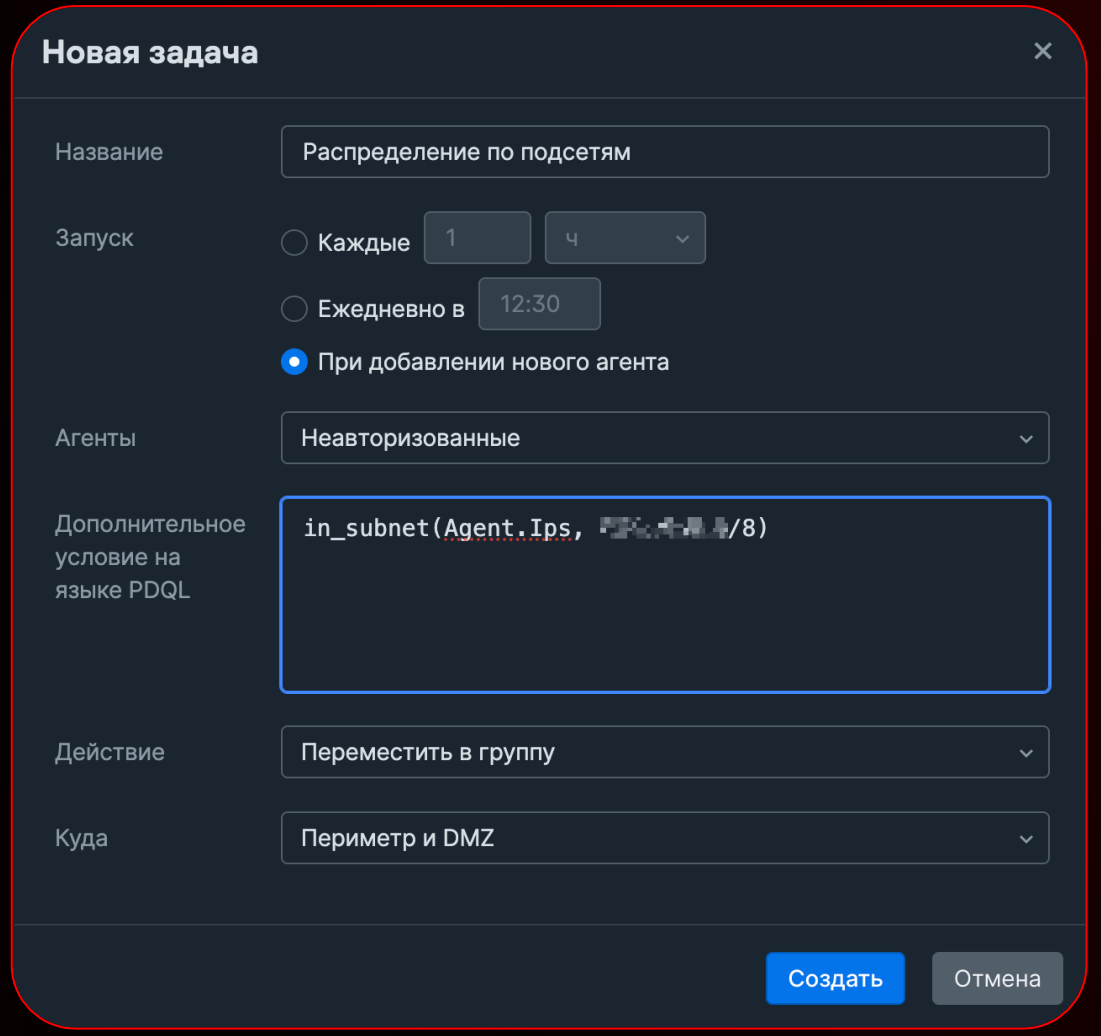




Автоматизируйте управление агентами

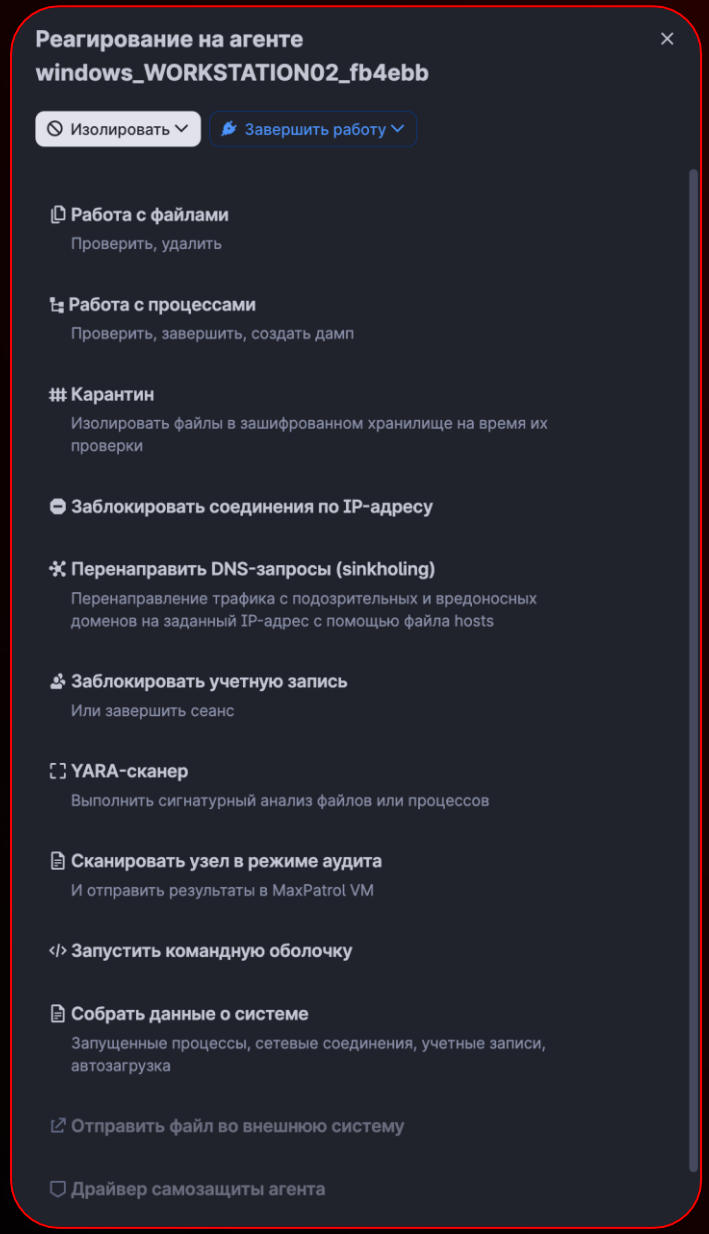
- Готовые Ansible скрипты для:
  - Установки агентов
  - Удаления агентов
  - Обновления агентов
  - Переподключения агентов к другому серверу агентов

- Фильтр по подсетям для планировщика задач



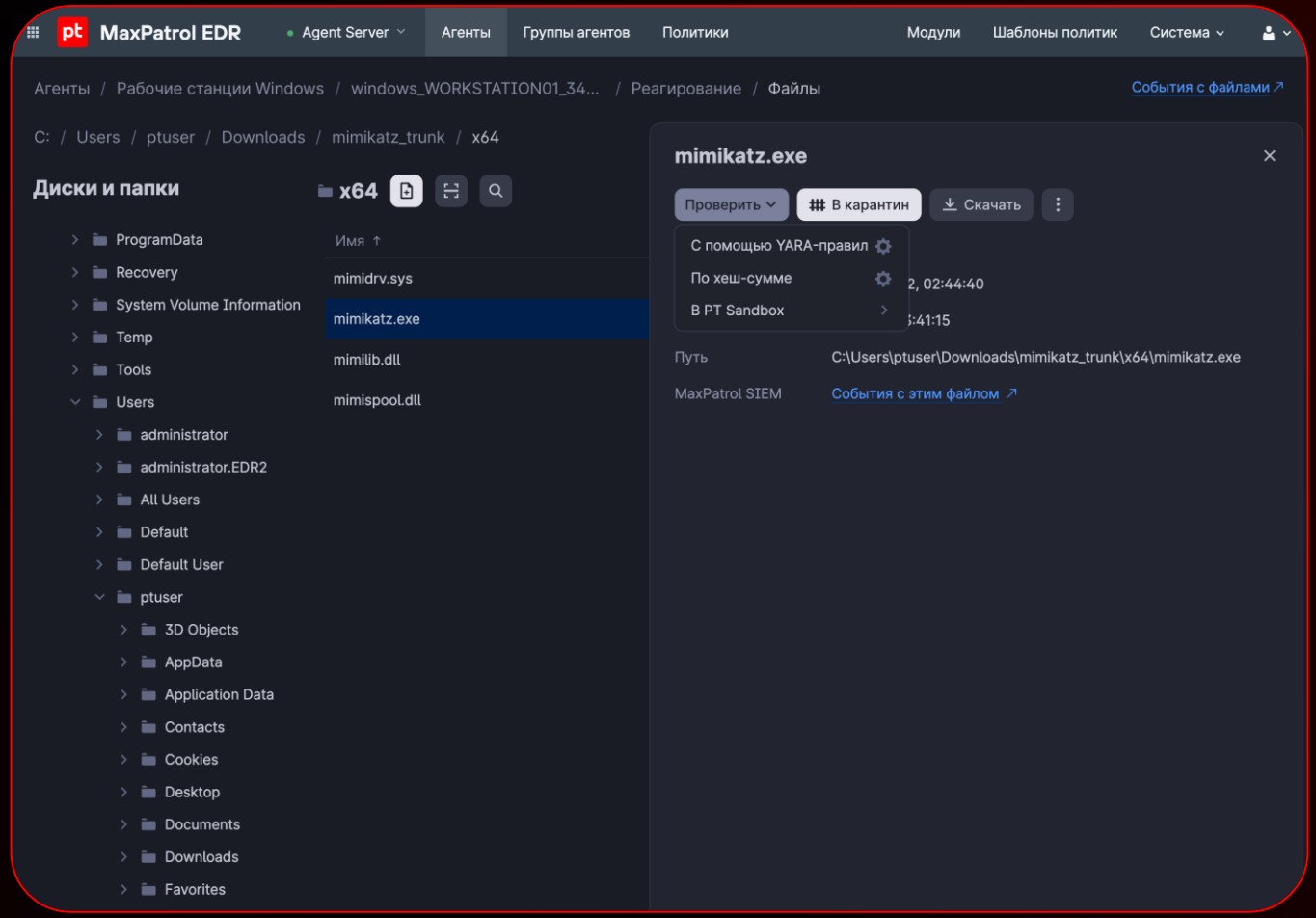
Обновленное меню реагирования

- Упростили и ускорили путь пользователя
- Изоляция и завершение работы – 3 клика
- Вынесли в карточку управление самозащитой



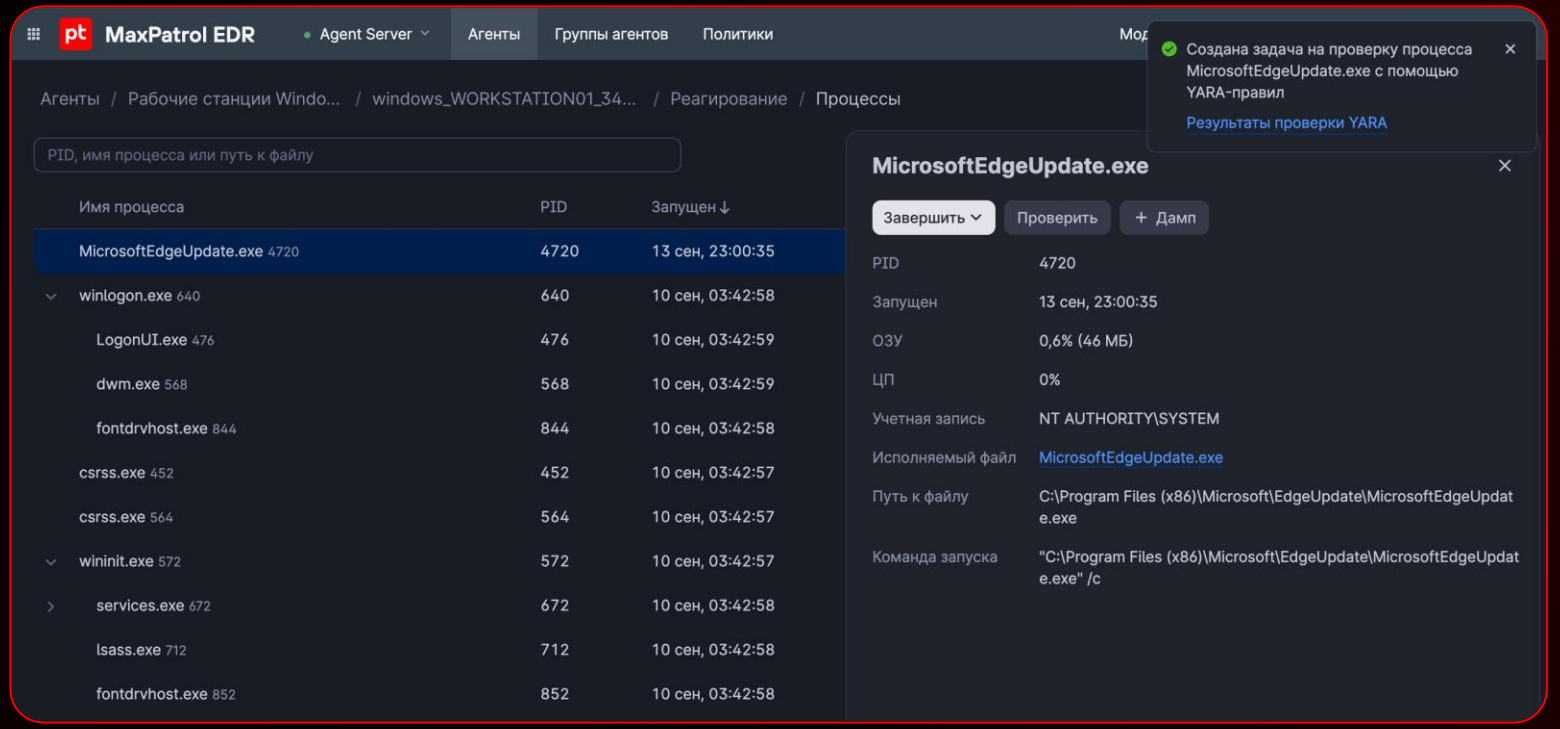
Работайте с файлами

- Больше не нужно переключаться между модулями
- Контекст перед глазами аналитика
- Доступны все операции с файлами
- Загрузка и скачивание файлов
- Переход к событиям в один клик



Работайте с процессами

- Запущенные процессы с информацией: имя, идентификатор, параметры запуска
- Все операции с процессами в одном окне
- Быстрый переход к исполняемым файлам и операциям над ними
- Переход к событиям в один клик



Простые рецепты

Инвентаризация и сбор событий

- Минимум ресурсов на внедрение
- Минимальное влияние на производительность

Сбор данных и реагирование вручную

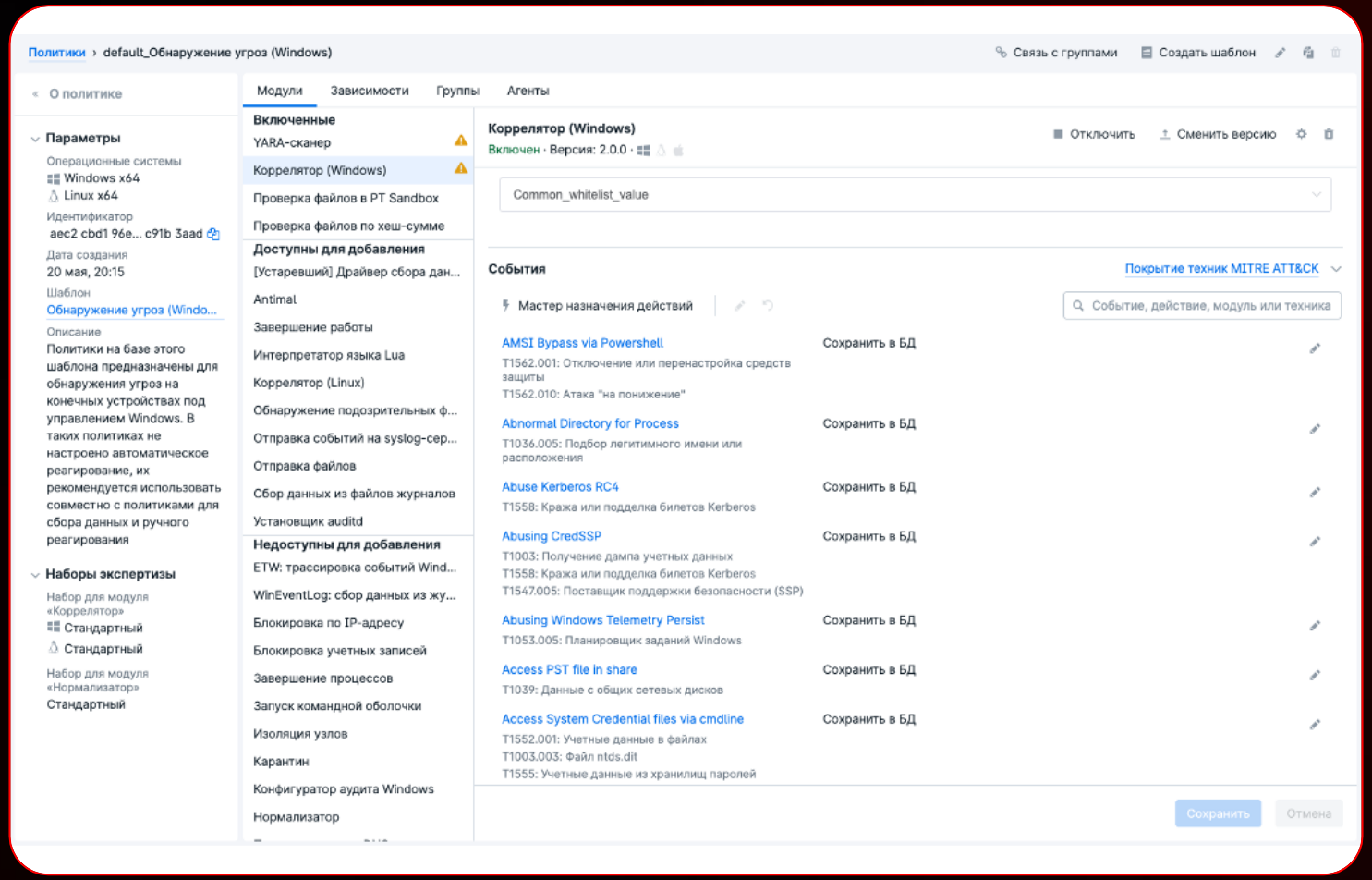
- Баланс между затратами на внедрение, функциональностью и нагрузкой на устройства

Сбор, обнаружение, реагирование

- Нужно «приучить» к инфраструктуре
- Агент EDR сильнее влияет на производительность устройства

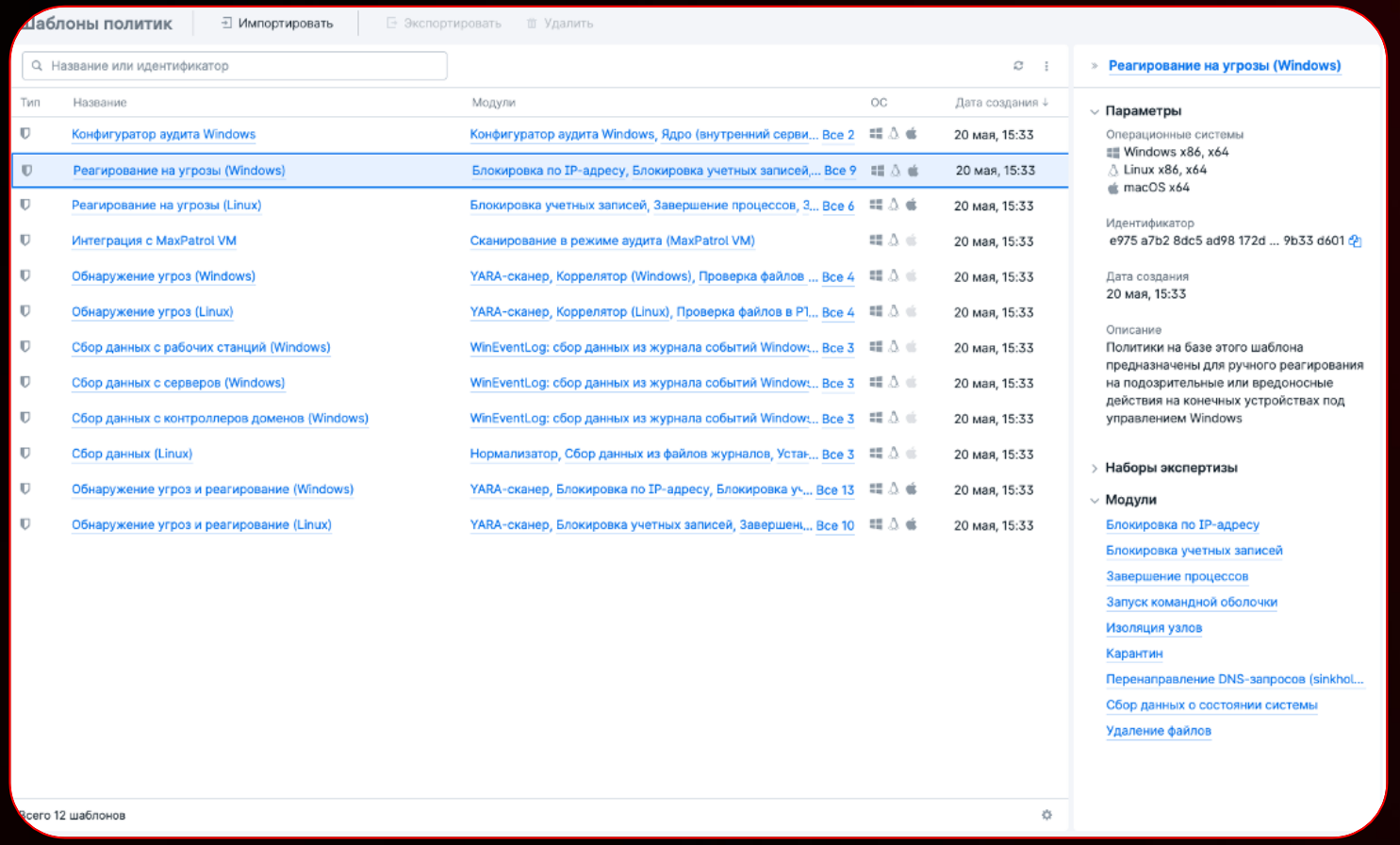
Политики MaxPatrol EDR

- Определяют набор модулей, устанавливаемых на агенты
- Хранят настройки, с которыми работают модули
- Можно сделать индивидуальными для каждой группы устройств
- Автоматизируют реагирование и сбор контекстных данных
- Упрощают взаимодействие между ИБ и ИТ департаментами:
  - Регулируют, каким образом и в каких случаях можно реагировать
  - Унифицируют профили сбора событий



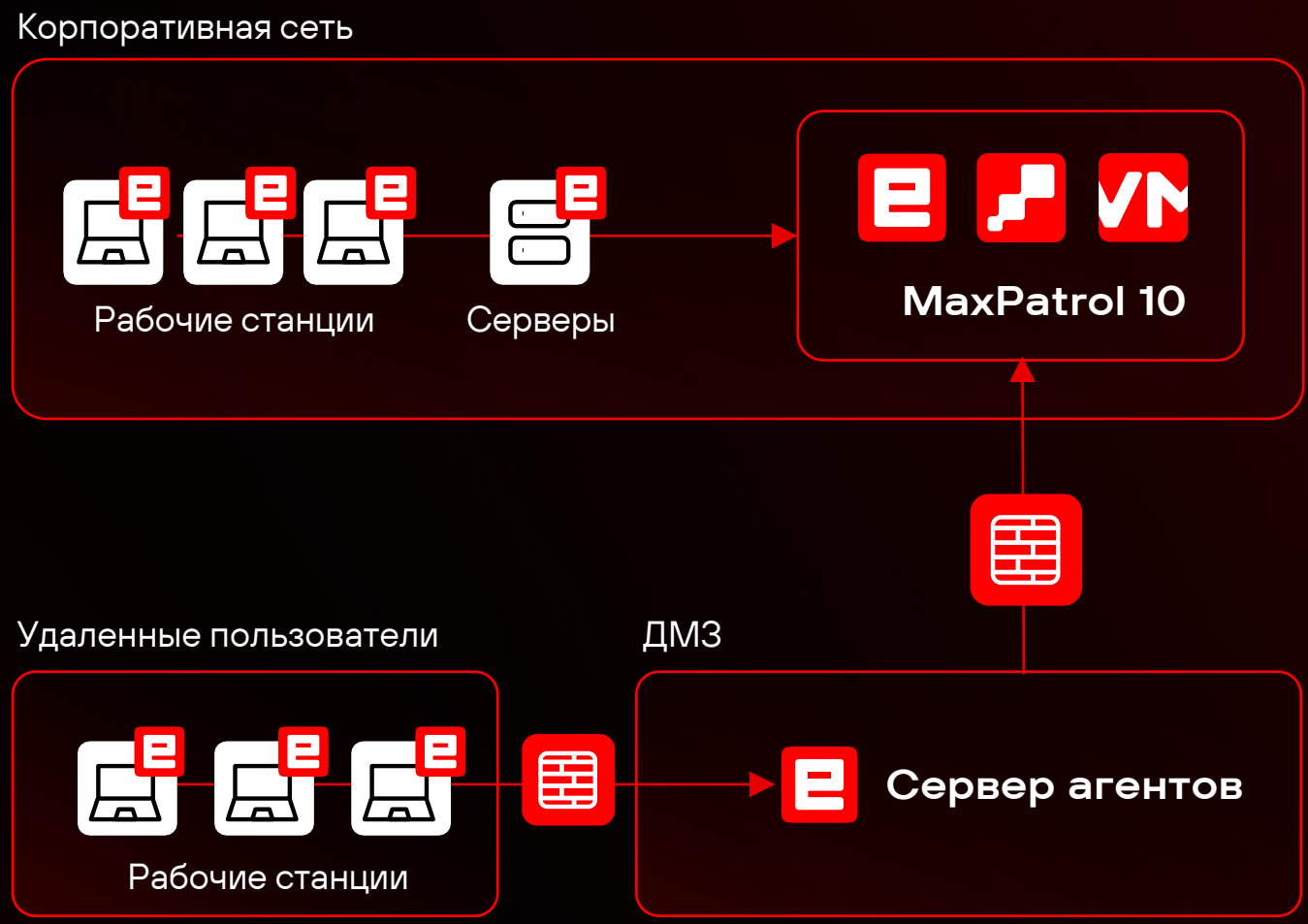
Настраивайте продукт не за часы, а за минуты

- Преднастроенные шаблоны «из коробки»
- Превращайте любую политику в шаблон
- Применяйте шаблон к любой политике
- При необходимости экспортируйте или импортируйте шаблон



Управляйте сбором данных

- Конфигурируйте и собирайте:
  - Windows Eventlog
  - Sysmon
  - ETW
  - Auditd
  - eBPF** (Q3-Q4 2025)
  - Логи из файлов журналов
- В том числе с устройств вне домена или периметра
- Сбор событий – непрерывно
  Сканирование – по расписанию
- Для сканирования не нужны учетные записи с повышенными привилегиями
- Более простая маршрутизация: все данные передаются через соединение агента



Реагируйте вручную (+ API)

- Полная или частичная сетевая изоляция узлов
- Завершение процессов, получение дампа памяти процесса
- Удаление файлов
- Блокировка соединений с IP адресами
- Перенаправление сетевых соединений (синкхолинг)
- Блокировка учетных записей пользователей
- Карантин файлов
- Запуск командной оболочки

Гибкость настройки и управления нагрузкой

- Настраиваемые политики реагирования
- Модули реагирования в режиме ожидания потребляют минимум ресурсов

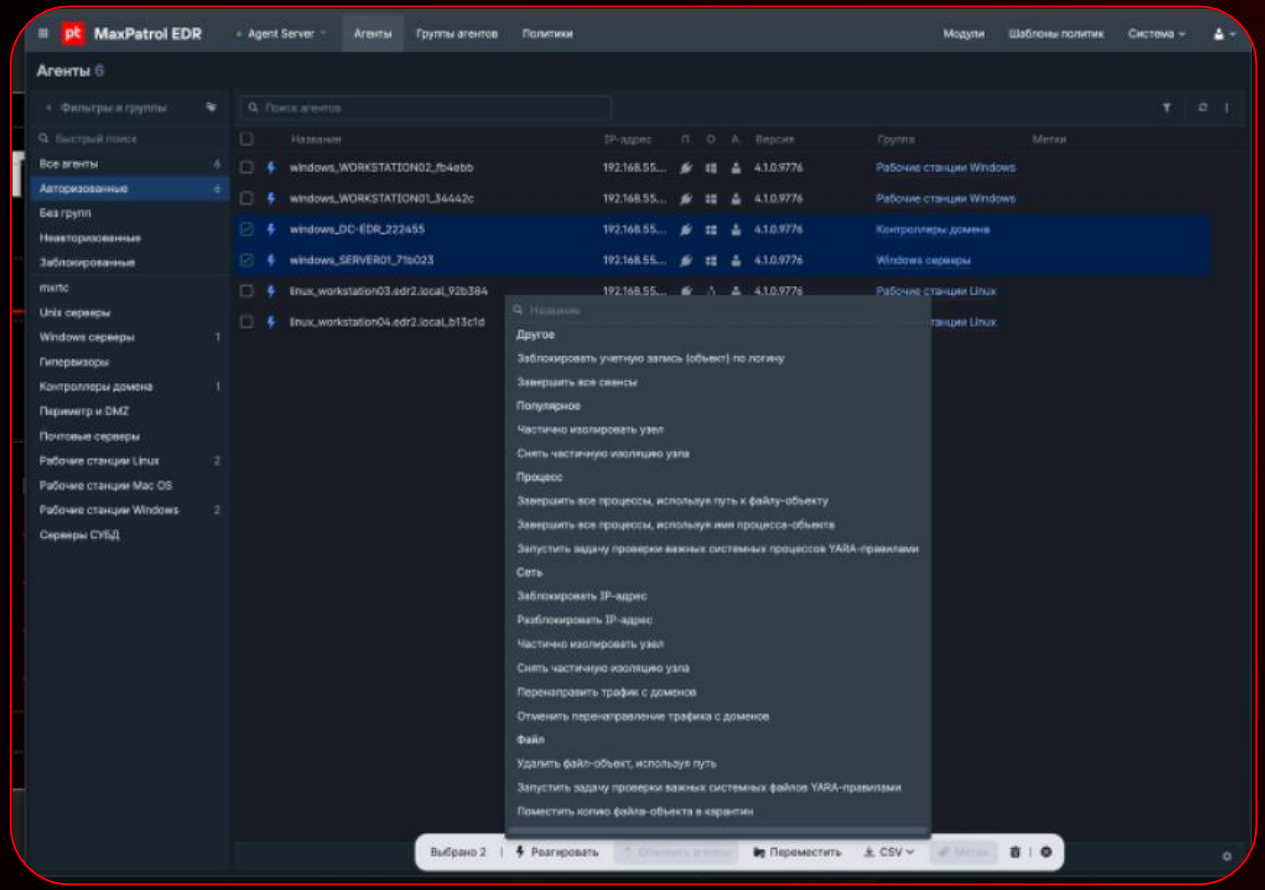
Контроль устройств, находящихся вне корпоративной сети

- Реагирование на устройствах вне корпоративного периметра

Полный перечень доступных модулей на операционных системах

Реагируйте на множестве агентов

- Просто начать и удобно продолжить
  - В журнале реагирования отображаются статусы задач — понятная обратная связь по всем устройствам
  - Можно повторить выполнение действий
  - В пару кликов можно другое действие для выбранной группы или для некоторых агентов



Обнаруживайте угрозы

- Поведенческий анализ прямо на устройствахс помощью узлового коррелятора
- Статический анализ YARA-правилами для сканирования файлов и процессов
- Мониторинг появления опасных файлов и взаимодействия с ними
- Обнаружение наиболее актуальных вредоносных образцов по контрольным суммам
- Механизмы обнаружения работают на агенте, возможна работа в автономном режиме
- Дополнительные проверки артефактов во внешних системах (PT Sandbox)

Обнаруживает популярные техники из матрицы MITRE ATT&CK

- **700+ правил** для Windows
- **150+ правил** для Linux

Предоставляет возможность гранулярной настройки системы

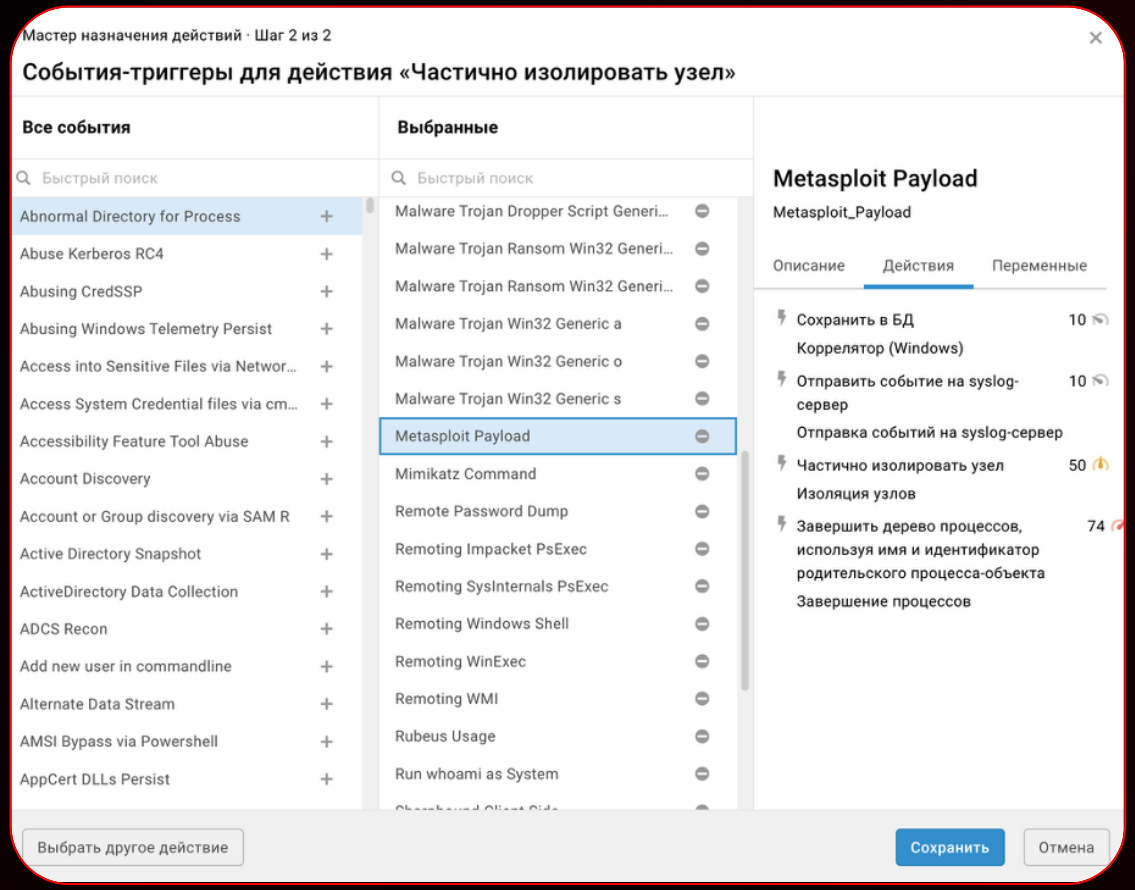
- Баланс между глубиной детекта и нагрузкой на устройство
- Уникальные политики обнаружения для разных групп активов

Автоматизируйте реагирование

Экономия времени и ресурсов

Можно назначить разные сценарии для разных групп агентов

Действия выполнятся даже в автономном режиме*

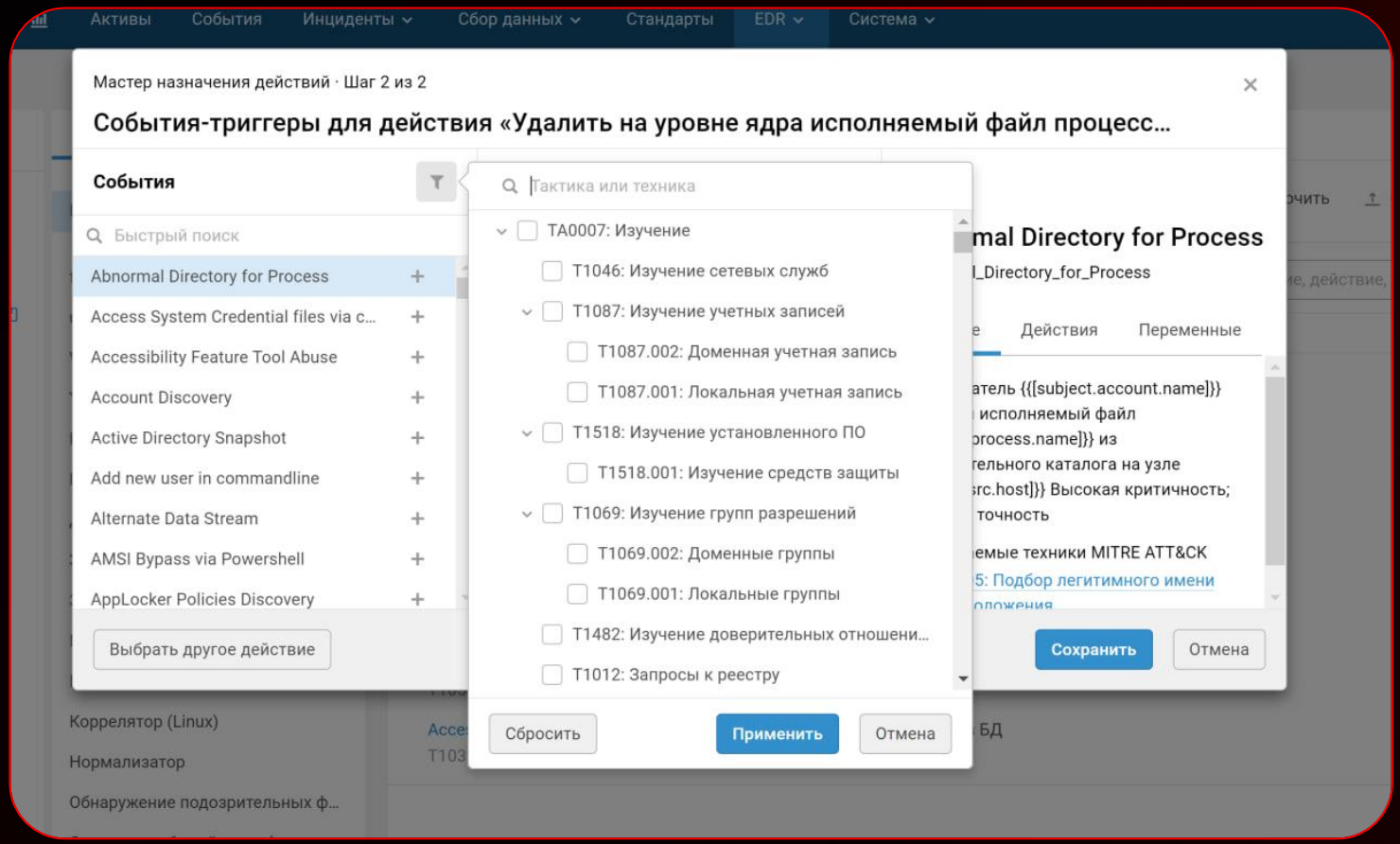


* Если не подразумевают взаимодействие с внешними системами

Автоматизируйте реагирование

Фильтрация по техникам MITRE

При настройке политик удобно фильтровать корреляционные правила по техникам, которые они покрывают.



Совсем скоро!
Новинки и планы MaxPatrol Endpoint Security

Комплексная защита устройств от всех видов угроз

MaxPatrol Endpoint Security

NEW! Предотвращение известных угроз с MaxPatrol EPP

1. Обнаружение и устранение ВПО и шифровальщиков **на базе антивирусных технологий**
2. Контроль устройств и приложений для ограничения векторов атак (в разработке)
3. Автоматические восстановление поврежденных шифровальщиком файлов (в разработке)

Выявление сложных угроз и реагирование на них MaxPatrol EDR

1. На ранних этапах выявляет атаки, которые могут пропустить другие средства защиты устройств
2. Собирает максимум данных с узлов и обнаруживает киберугрозы
3. Останавливает злоумышленника за считанные секунды, помогает расследовать и предотвращать атаки

Планы до конца года

- **Антивирусный движок в продукте!**
- Упростить процесс настройки политик.
  Перейти от подробной настройки модулей к простым переключателям.
  Доставлять рекомендуемые конфигурации сбора по аналогии с обновлением правил
- Дать возможность инсталляции без MaxPatrol SIEM, с собственной базой событий
  Для 1000 агентов снижение требований CPU и RAM – примерно в 3-4 раза
- Упростить управление агентами при установке с помощью меток.
  Метки можно будет использовать для фильтрации агентов в планировщике
- Внедрить легковесный движок для обнаружения вредоносов и руткитов
- Добавить сбор событий Linux с помощью eBPF
- Научить агентов работать с пользовательскими IoC
- Добавить кнопку «скачать логи агента» в карточку агента в консоли

Задать вопрос по теме выступления

habrahabr.ru/company/pt

pt@ptsecurity.com

ptsecurity.com

Спасибо