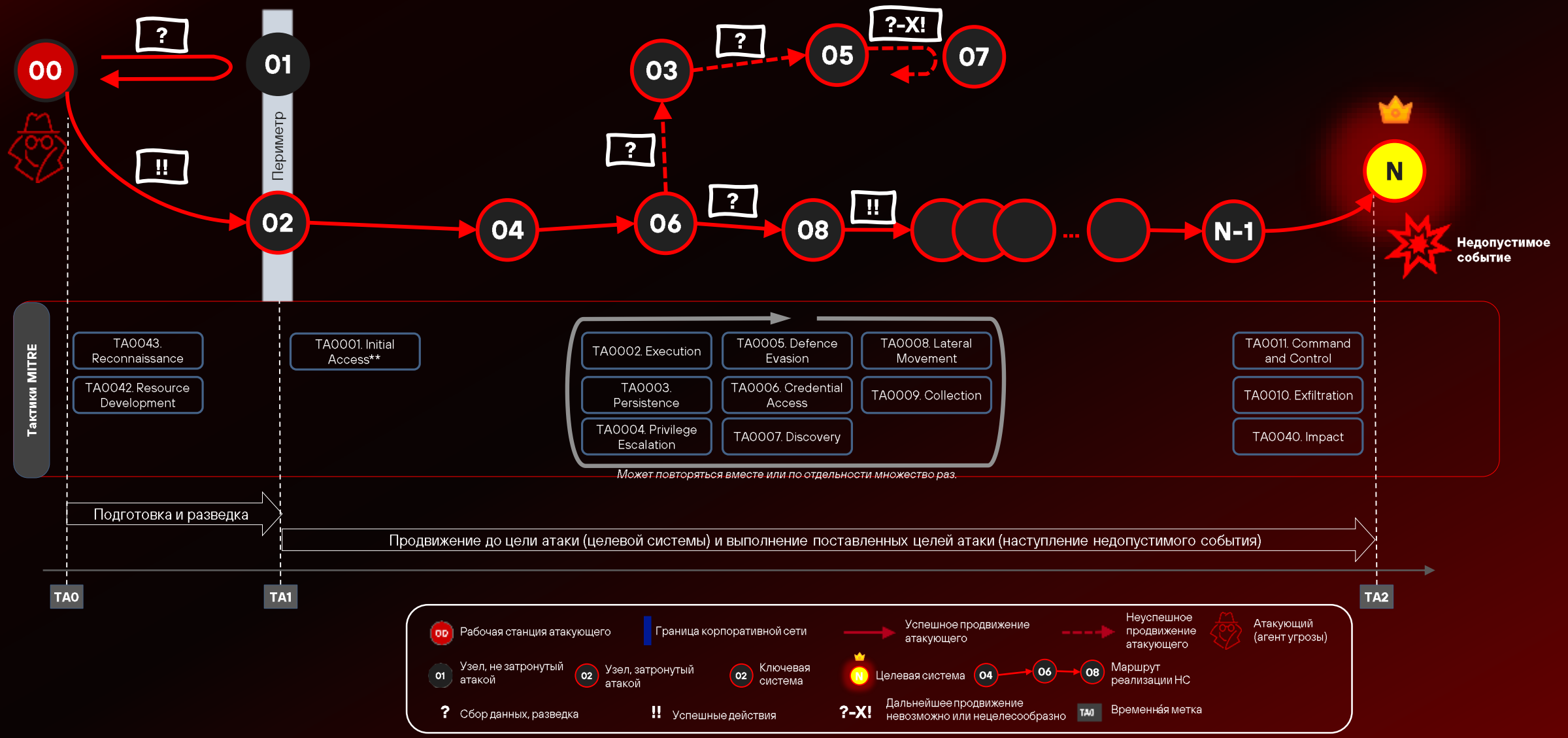
Кирилл Черкинский
Руководитель практики
защиты конечных устройств

Защита конечных устройств с помощью MaxPatrol EDR

Инцидент и цепочка атаки



Что могло пойти не так?

- Не отреагировали вовремя
- Не подключили источники или собрали не всё
- Не устранили уязвимости
- Не было инструментов и процессов

Защита конечных устройств: 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?

Сложный кейс

- Нужно защитить крупное международное мероприятие
- Часть инфраструктуры — удаленные площадки за периметром
- Другая часть регулярно обновляется
- Время решения инцидента — 2 часа

Как хакеры ПРОИГРАЛИ на «Играх Будущего»

Positive Technologies раскрыла подробности защиты мультиспортивного фиджитал-турнира «Игры Будущего» от кибератак

MaxPatrol EDR

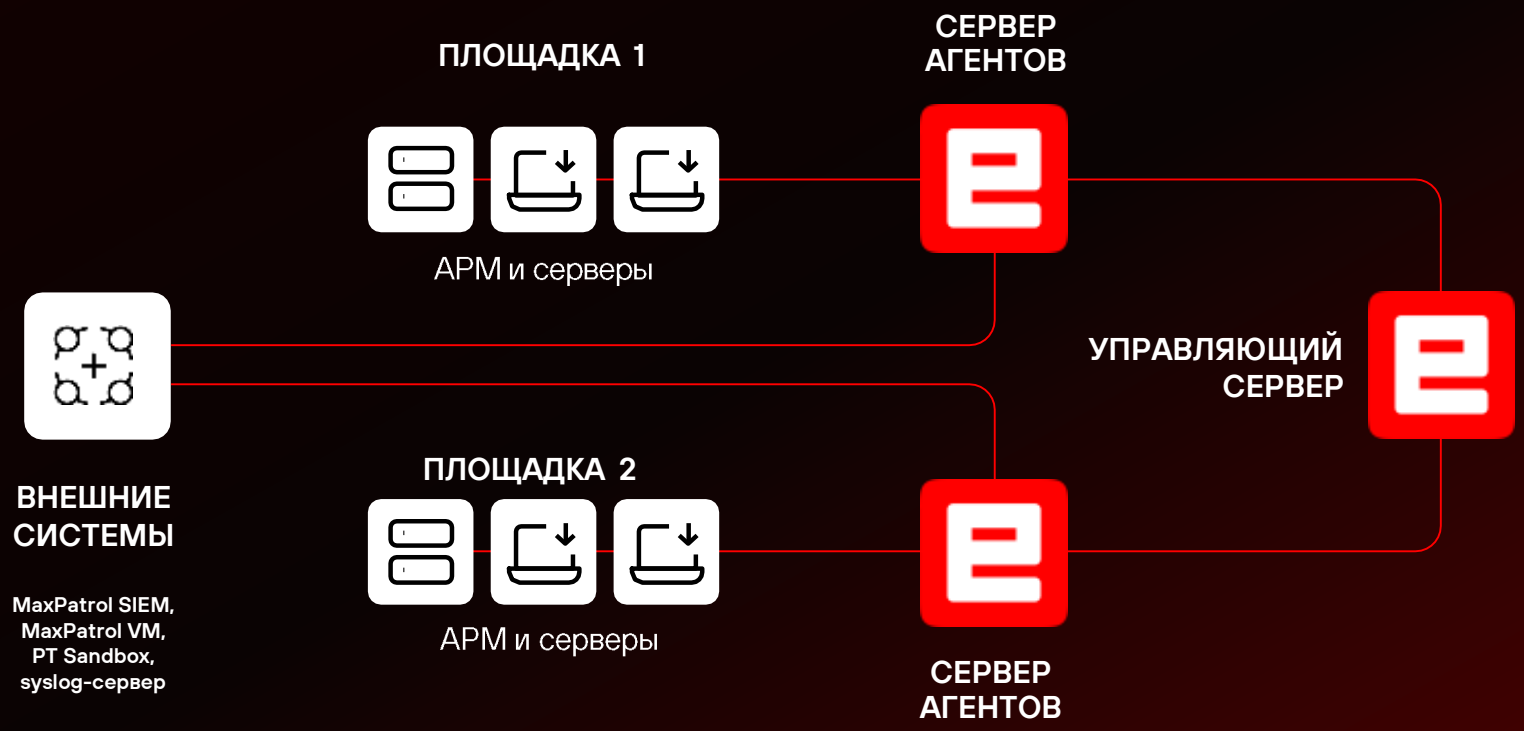
Защитит конечные устройства от сложных и целевых атак

- **На ранних этапах выявляет атаки**, которые могут пропустить другие средства защиты устройств
- **Собирает максимум данных с узлов и обнаруживает киберугрозы**
- **Останавливает злоумышленников за считаные секунды**
- **Единый агент для продуктов Positive Technologies**

Экспертиза Positive Technologies уже на устройствах:

- Автономный поведенческий и корреляционный анализ, реагирование непосредственно на защищаемом устройстве
- Мощный корреляционный движок для поведенческого анализа угроз: 700+ правил PT ESC
- Покрывает 60% техник матрицы MITRE ATT&CK
- 6000+ YARA-правил
- Модули «Обнаружение подозрительных файлов» и «Проверка файлов по хеш-сумме» (65 000+ хеш-сумм в базе данных от PT ESC)
- В связке с PT Sandbox позволяет повысить качество проверки файлов даже из зашифрованных каналов (например, при отправке файла в Telegram)

Как устроен MaxPatrol EDR: архитектура



Как работает MaxPatrol EDR

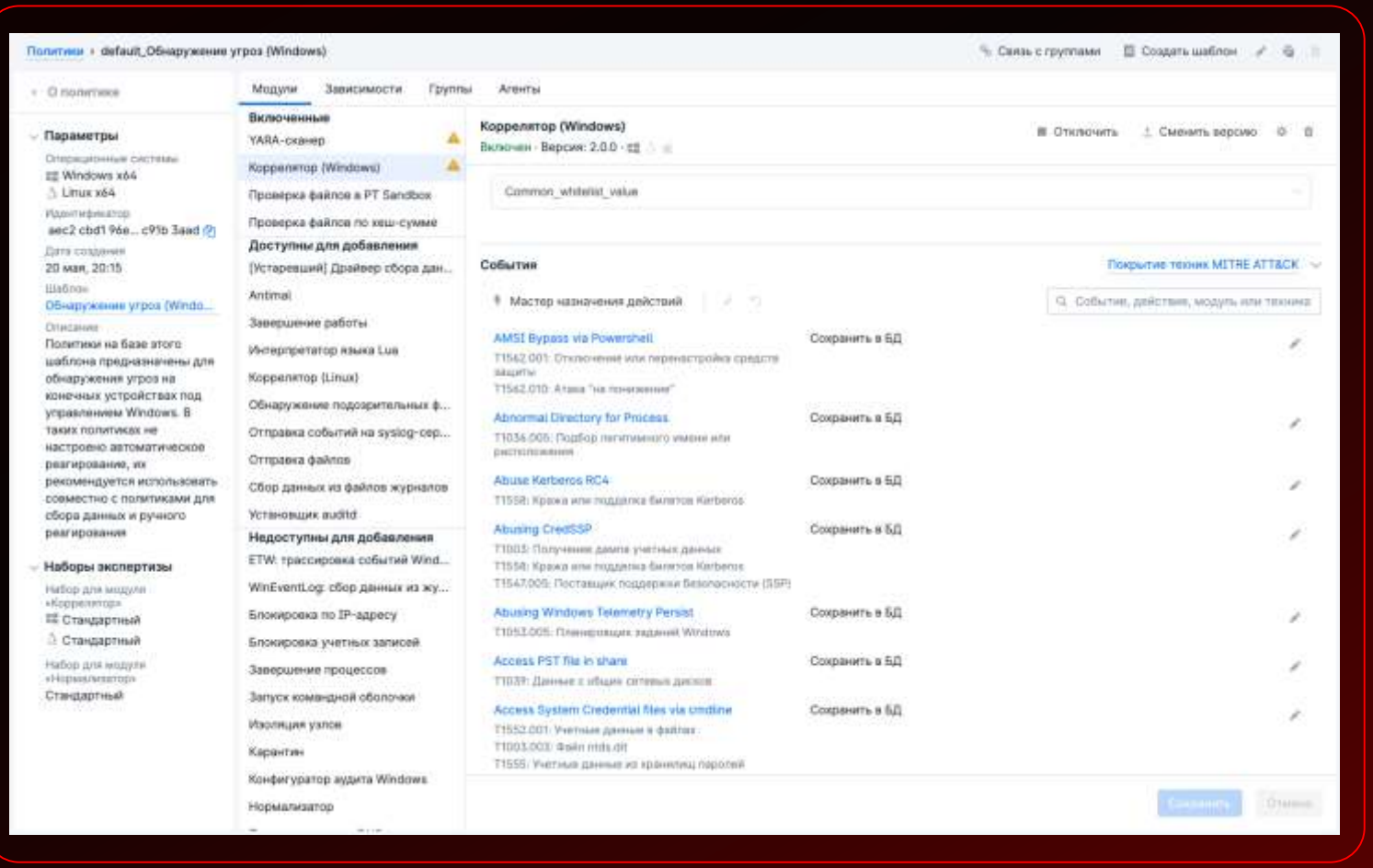
На чем работает MaxPatrol EDR

CentOS 9	РЕД ОС 8	Альт Сервер 9	Astra Linux 1.8	RHEL 9	Ubuntu 24.04
Windows 10	Astra Linux 1.7	Oracle 9	Windows Server 2022	Альт Сервер 10.2	Альт Р. станция 9
РЕД ОС 7.2	Альт Р. станция 10.2	Debian 11	Альт Р. станция 10.1	Мос.ОС 12	CentOS 10
Debian 12	Windows Server 2019	RHEL 8	Ubuntu 22.04	ОСнова 2.0	macOS 14
Ubuntu 20.04	macOS 15	AlterOS 7.5	Windows 11	Альт Сервер 10.1	Astra Linux CE

...и этот список растет с каждым релизом

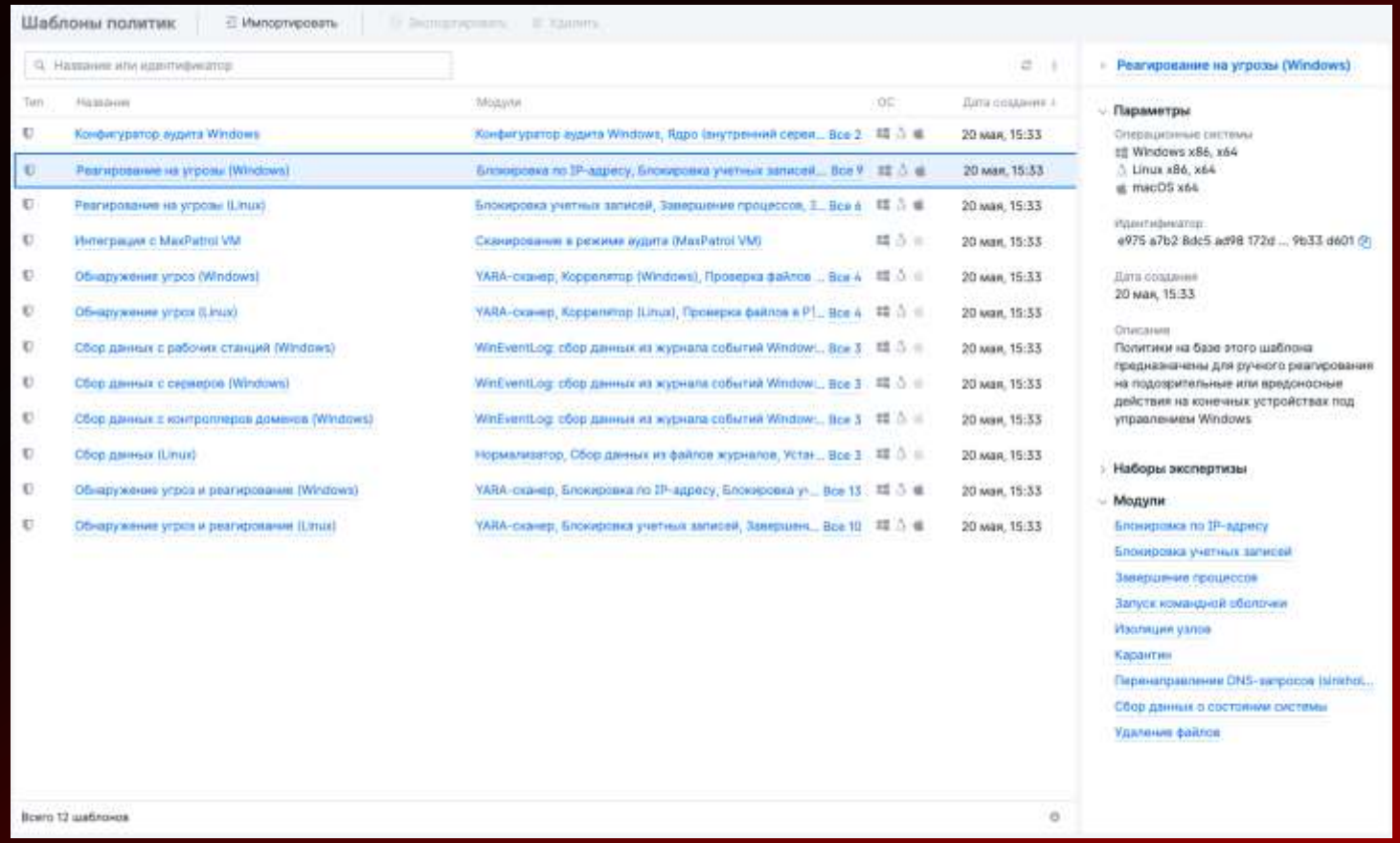
Политики MaxPatrol EDR

- 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

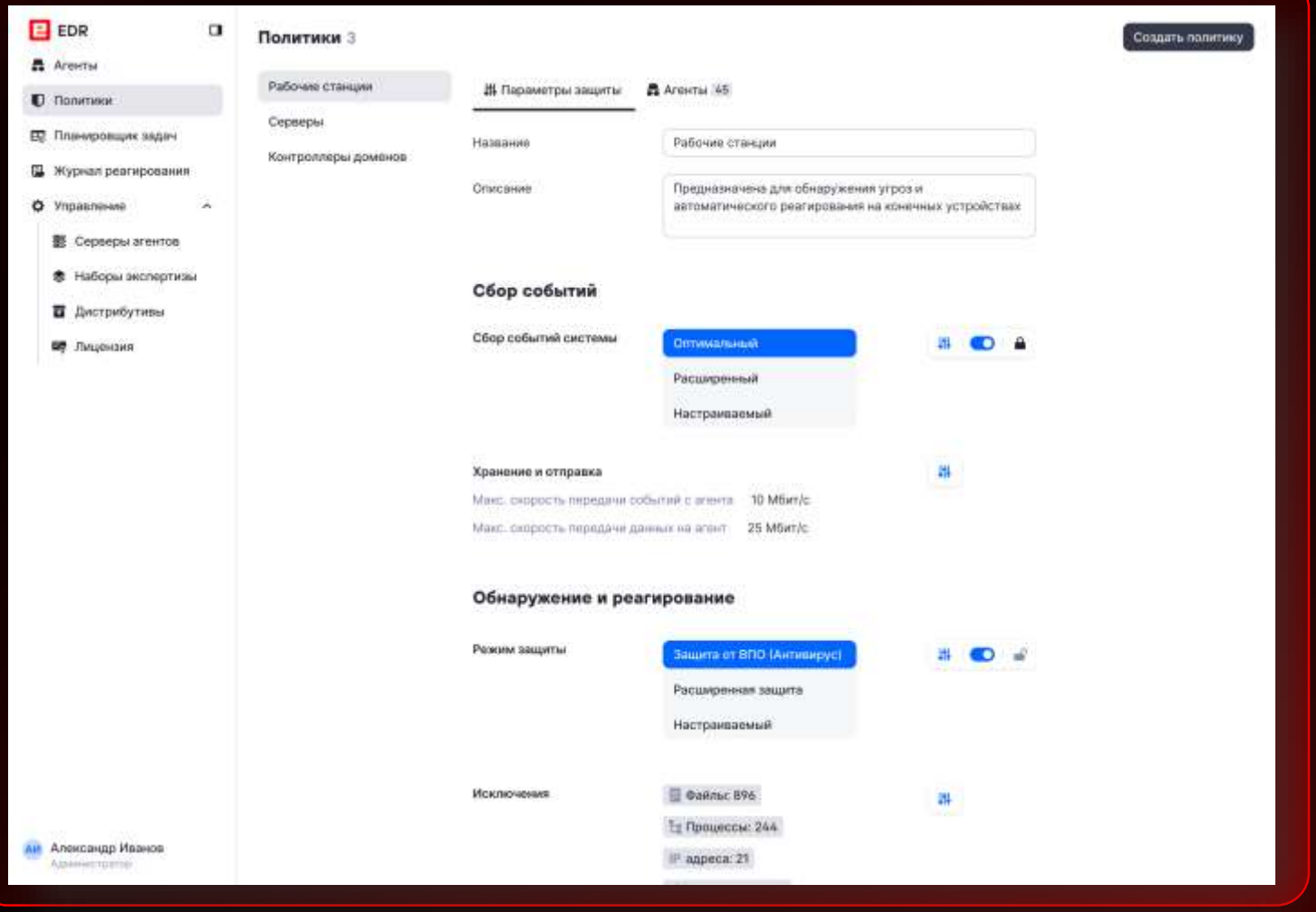


Развертывание не за часы, а за минуты

- Преднастроенные шаблоны «из коробки"
- Превращаем любую политику в шаблон
- Применяем шаблон к любой политике
- При необходимости экспортируем или импортируем шаблон



Обновления в следующих релизах



- Полная переработка логики работы с политиками
- Переход от компоновки политики модулями к выбору нужной функциональности
- Базовые «коробочные» профили не требуют конфигурирования
- Иерархичность политик с защитой параметров от изменения на вложенных уровнях

Готовые 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

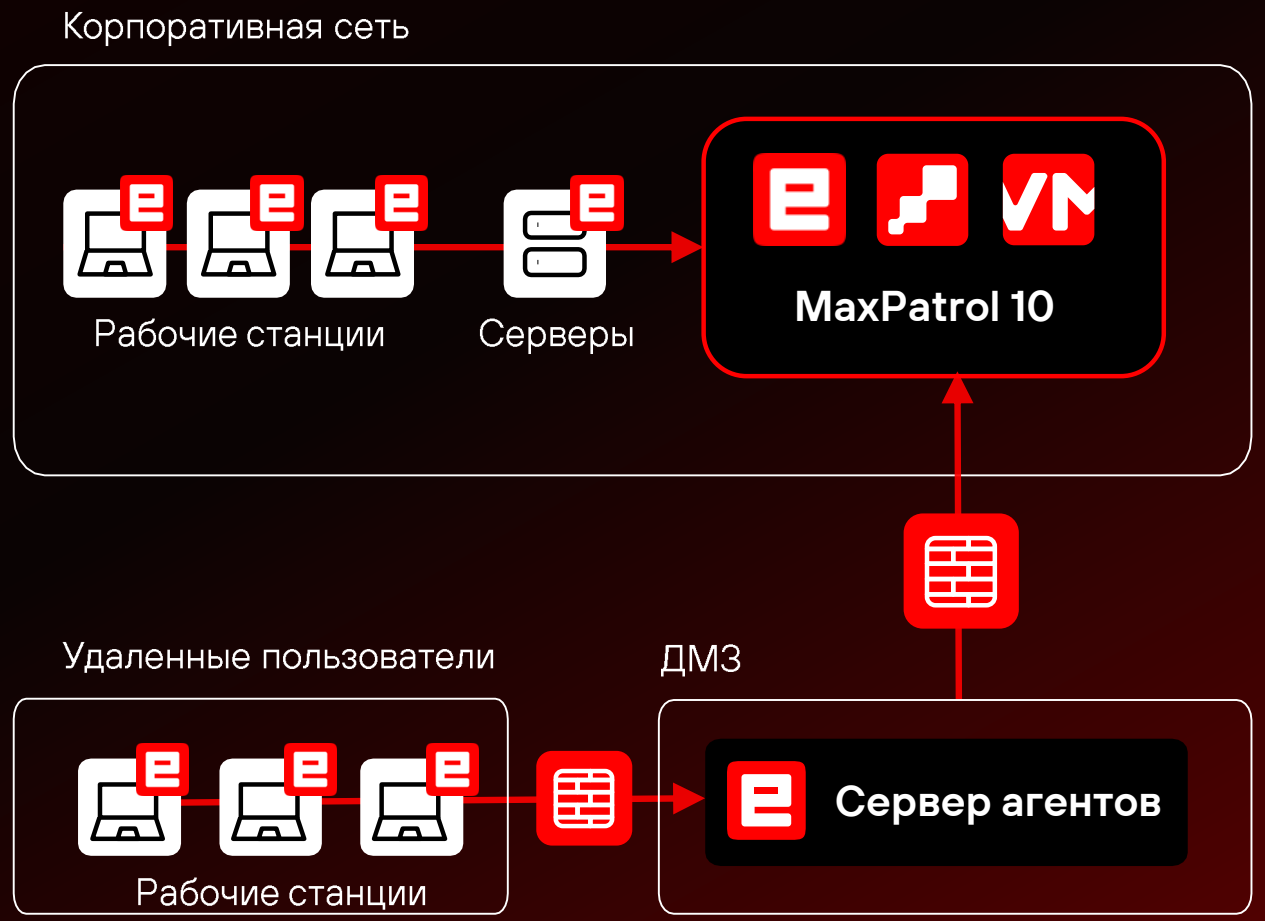
СЦЕНАРИЙ 1

ИНВЕНТАРИЗАЦИЯ И СБОР СОБЫТИЙ

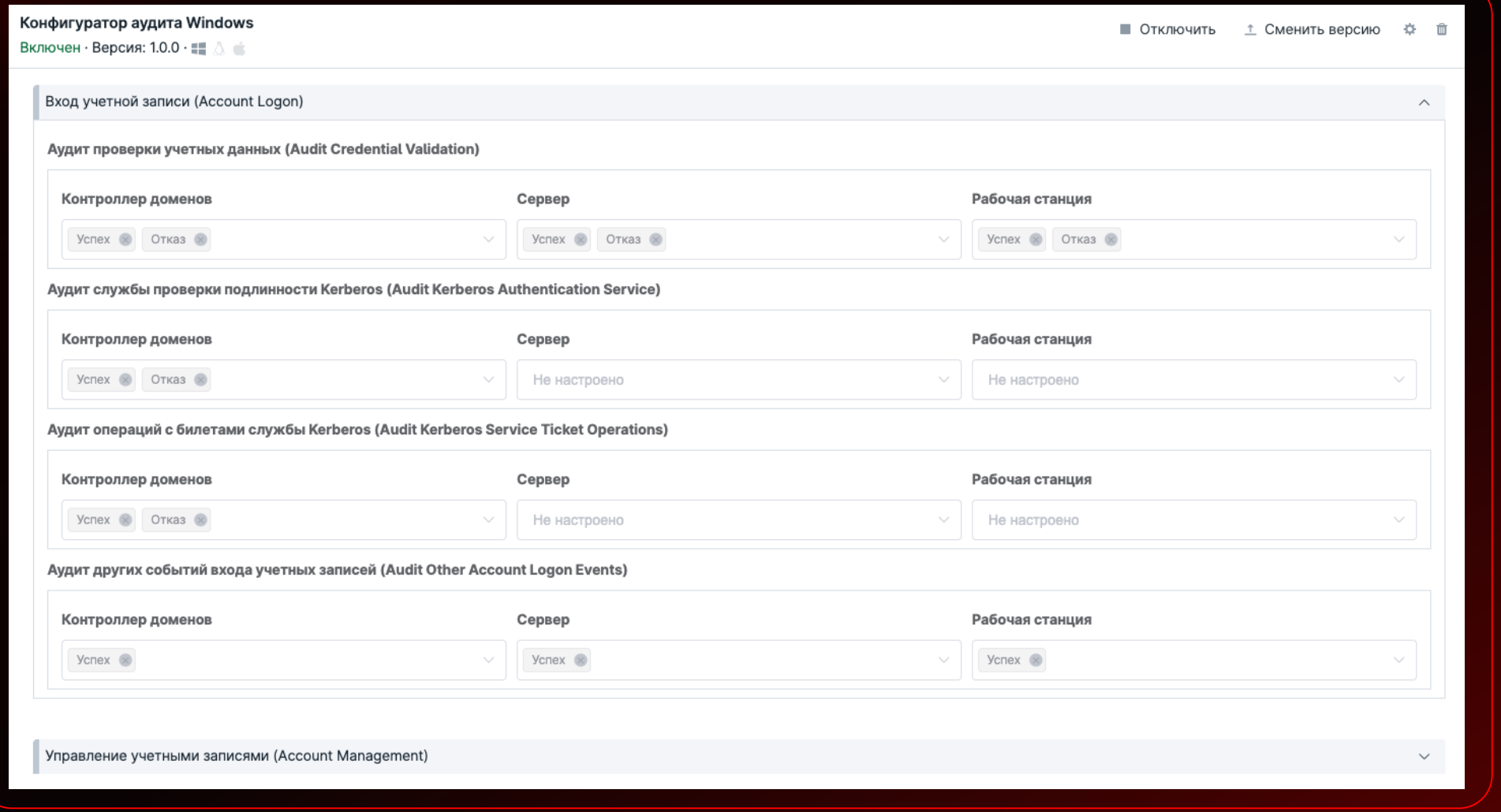
- Агент EDR отправляет события в MaxPatrol SIEM и помогает выстроить процесс управления уязвимостями
- Простое и быстрое внедрение, легкая настройка
- Синхронизация списков исключений с MaxPatrol SIEM

Управляемый сбор данных

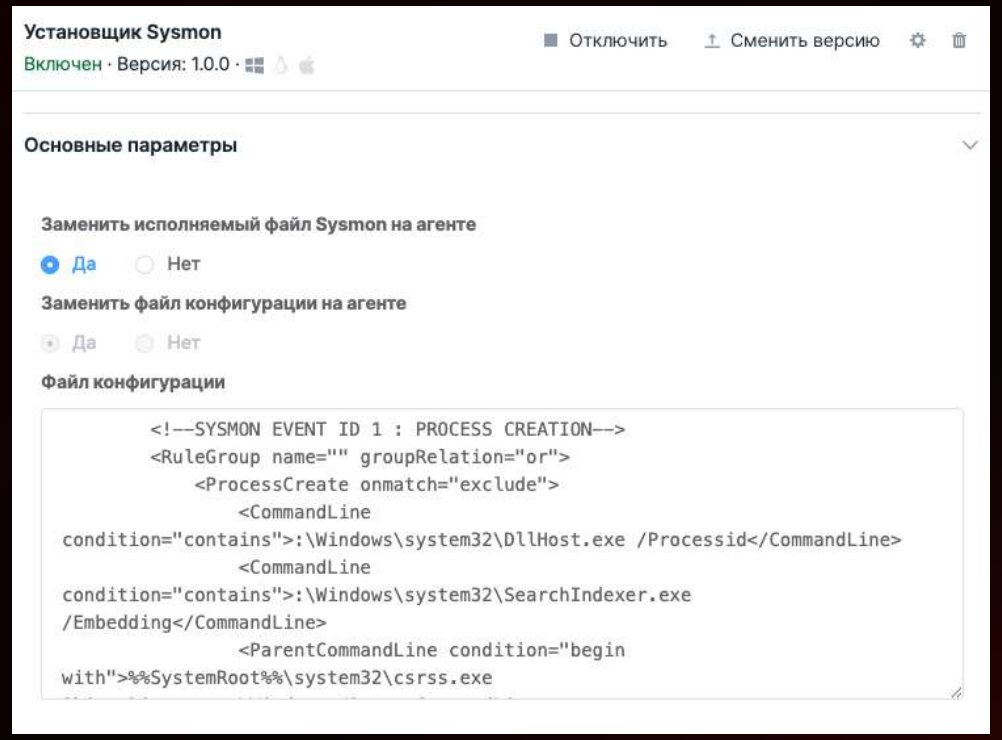
- Конфигурируем и собираем:
  - Windows Eventlog
  - Sysmon
  - ETW
  - Auditd
  - eBPF** (Q3–Q4 2025)
  - Файлы журналов
- В том числе с устройств вне домена или периметра
- Сбор событий — непрерывно, сканирование — по расписанию
- Для сканирования не нужны учетные записи с повышенными привилегиями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

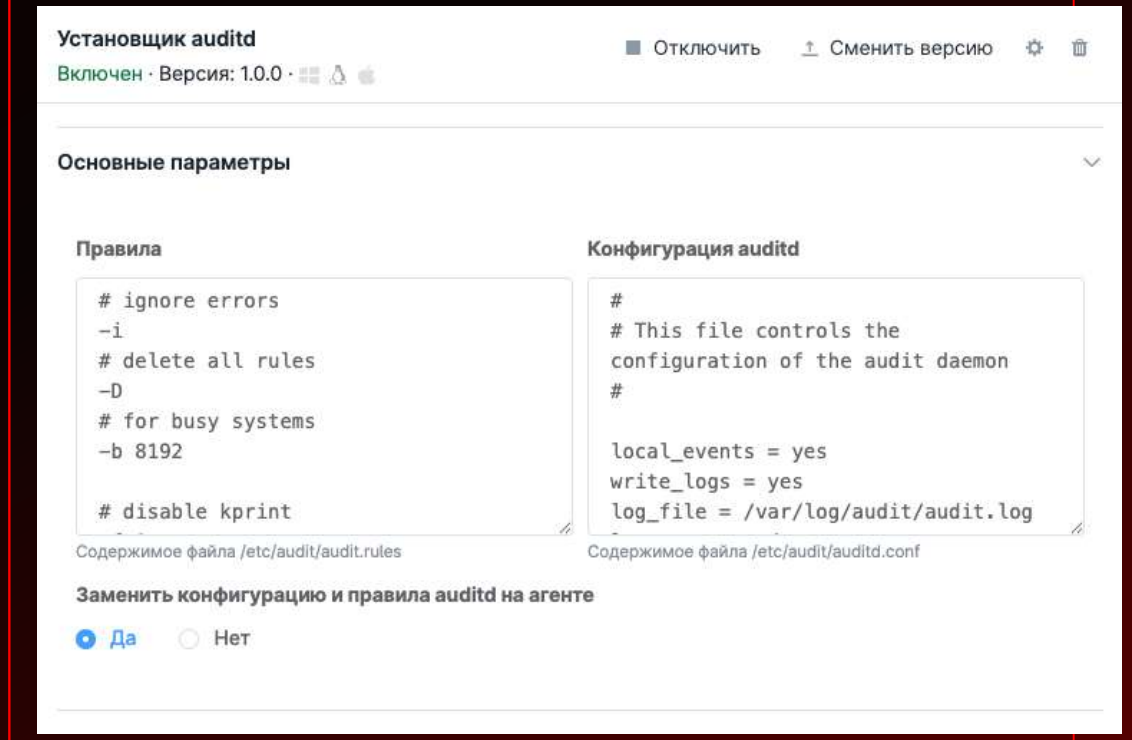


Конфигуратор аудита Windows

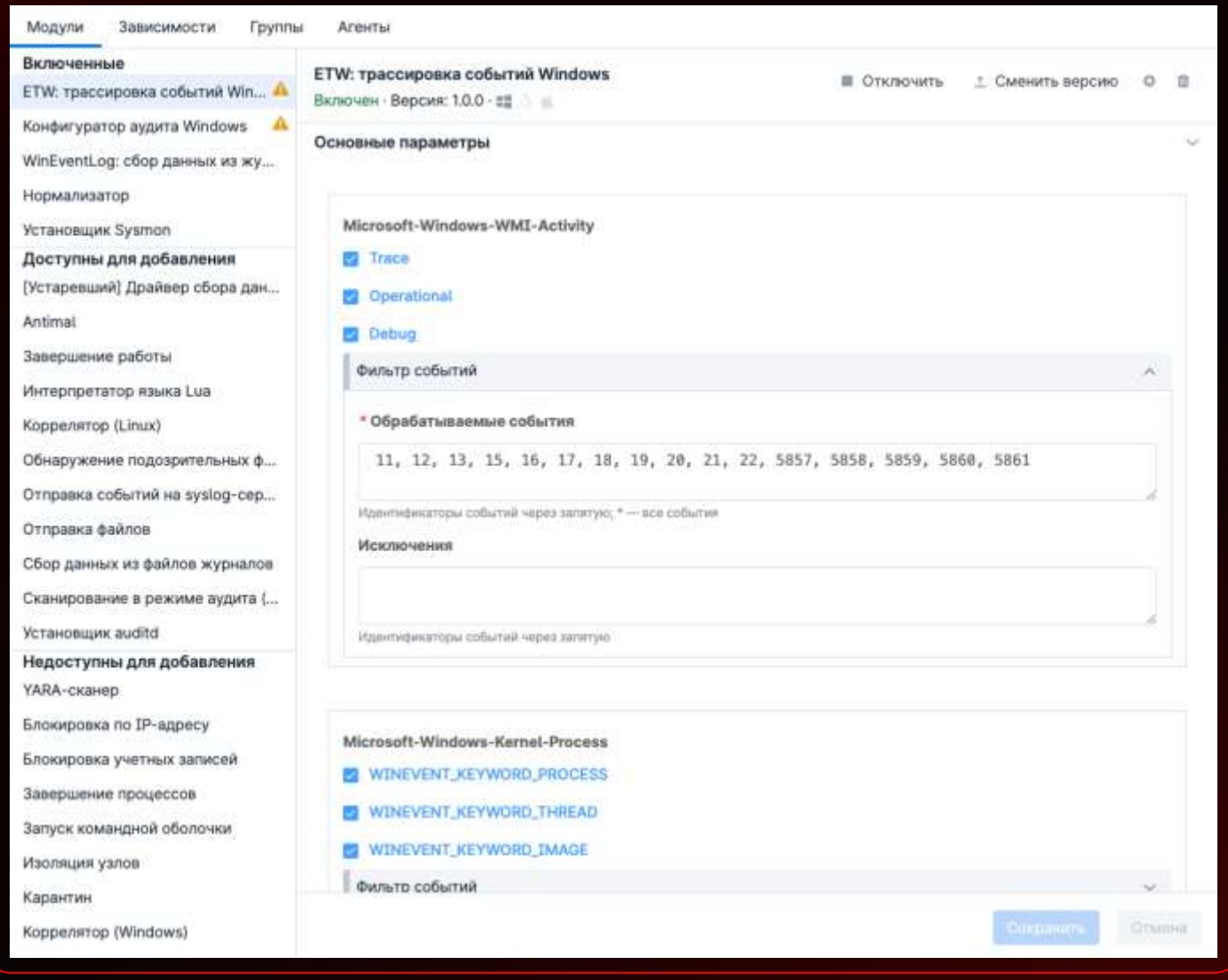


Настройка Sysmon и auditd на уровне политики



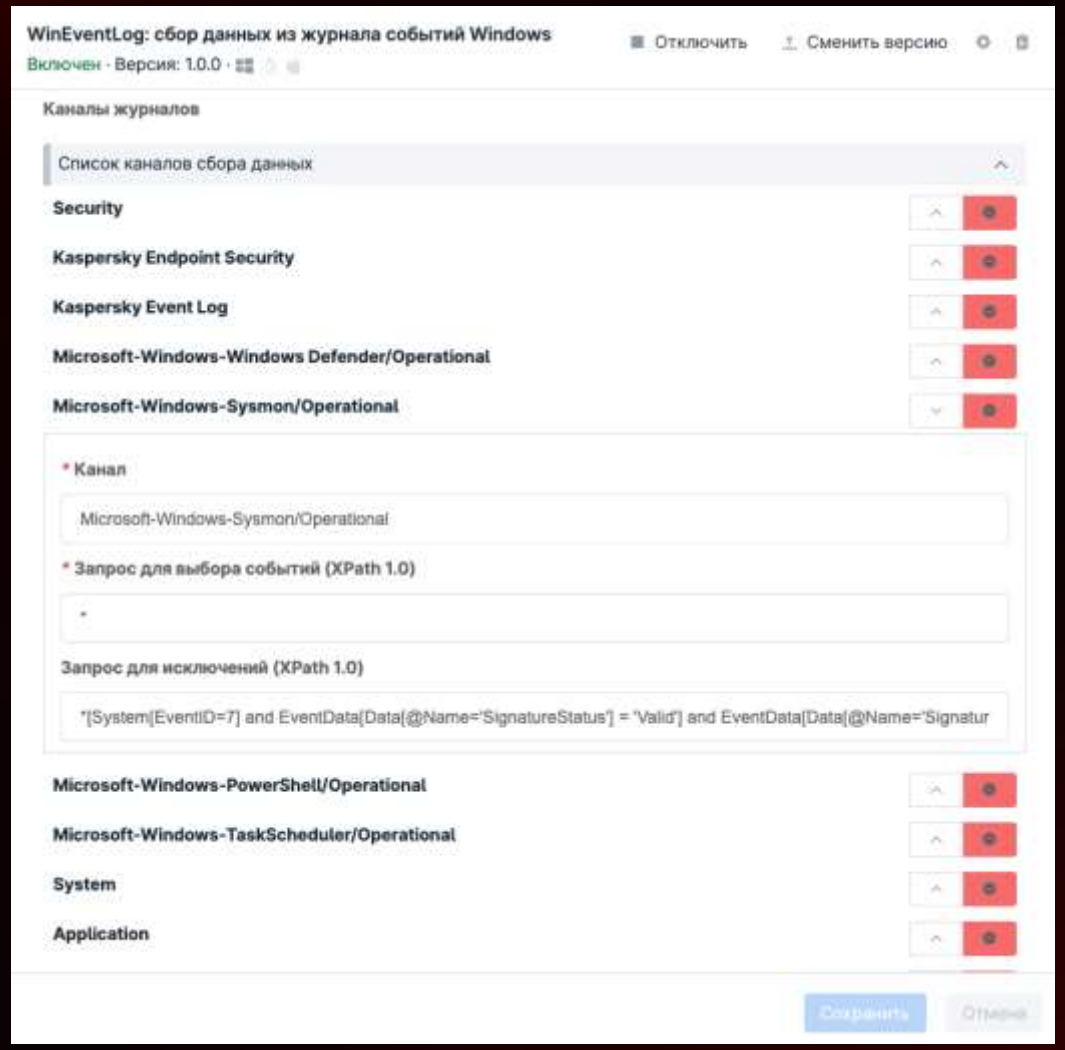


ETW



- Технология ETW — это диагностическое средство ОС Windows, позволяющее получить огромное количество информации о службах, приложениях, драйверах
- Модуль создает ETW-сессию и подписывается на ETW события, публикуемые указанными провайдерами
- Сам проверяет активность созданной ETW сессии
- EDR - единственный поставщик ETW событий для обнаружения

Фильтрация событий



СЦЕНАРИЙ 2

ДОБАВЛЯЕМ РЕАГИРОВАНИЕ

- Модули реагирования только для ручного режима
- Появляется возможность локализовать и устранить инцидент
- Реагирование в два клика из карточки события

Ручное реагирование (+API)

- Полная или частичная сетевая изоляция узлов
- Завершение процессов
- Удаление файлов
- Блокировка соединений по IP-адресам
- Перенаправление сетевых соединений (синкхолинг)
- Блокировка учетных записей пользователей
- Карантин файлов
- Запуск командной оболочки

ГИБКОСТЬ НАСТРОЙКИ И УПРАВЛЕНИЕ НАГРУЗКОЙ

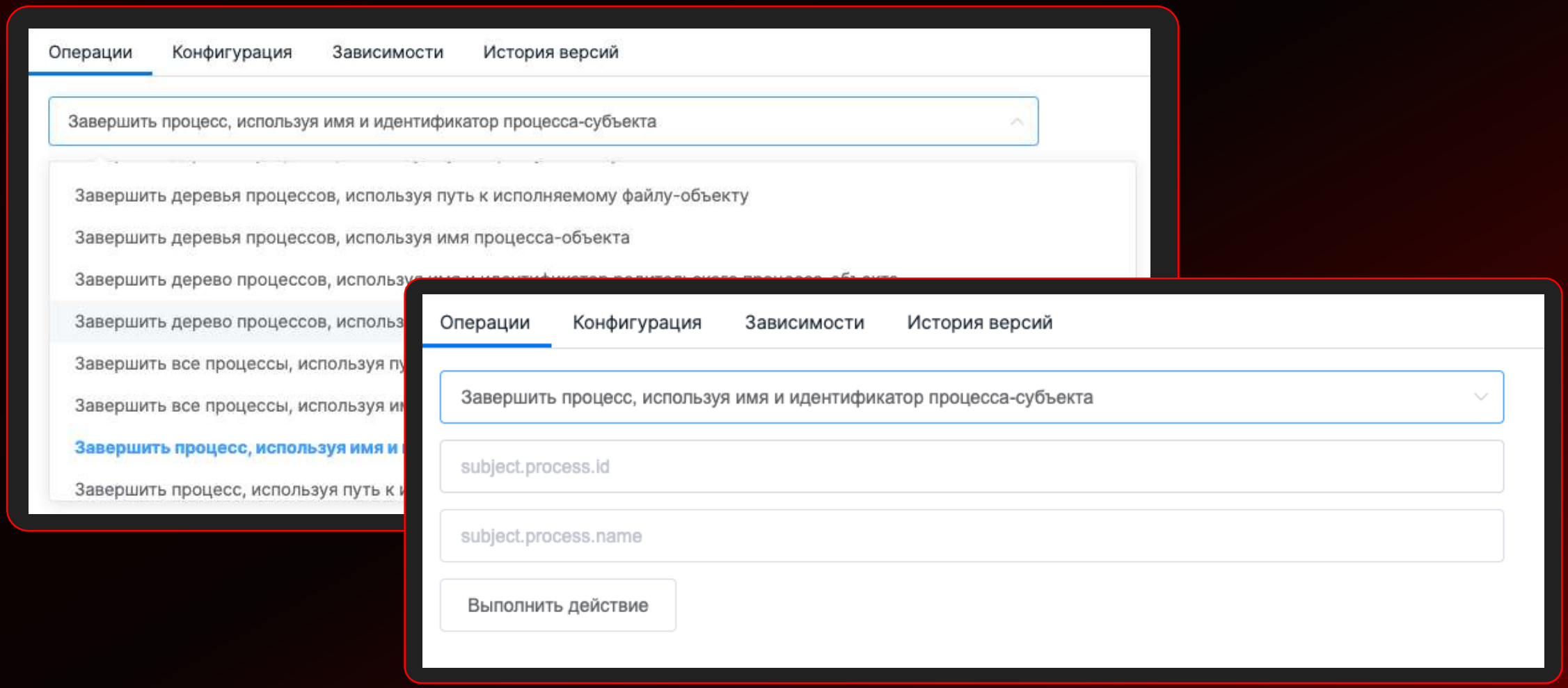
- Настраиваемые политики реагирования
- Модули реагирования в режиме ожидания потребляют минимум ресурсов

КОНТРОЛЬ УСТРОЙСТВ, НАХОДЯЩИХСЯ ВНЕ КОРПОРАТИВНОЙ СЕТИ

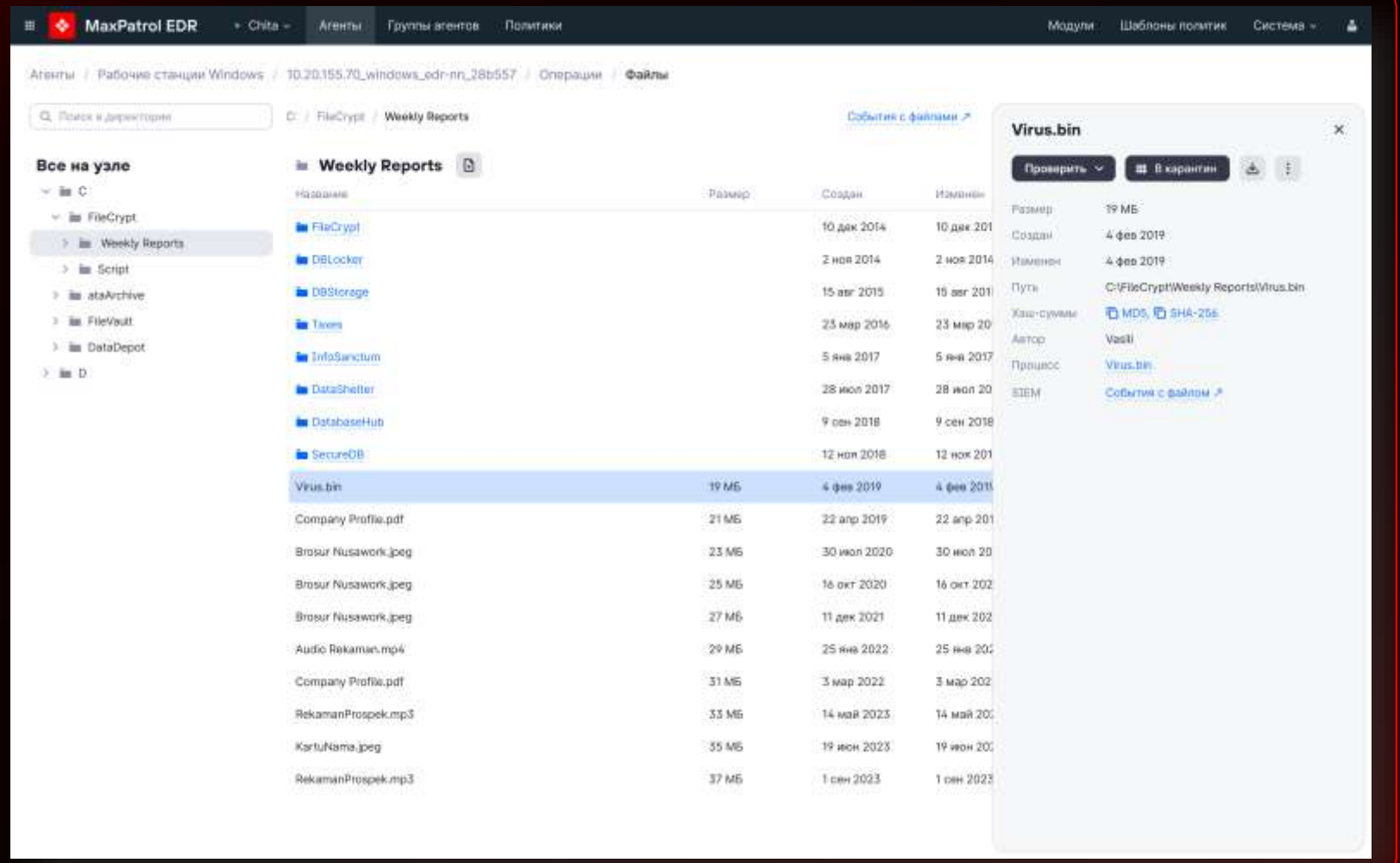
- Реагирование на устройствах вне корпоративного периметра

Полный перечень доступных модулей на операционных системах

Реагирование из интерактива модуля

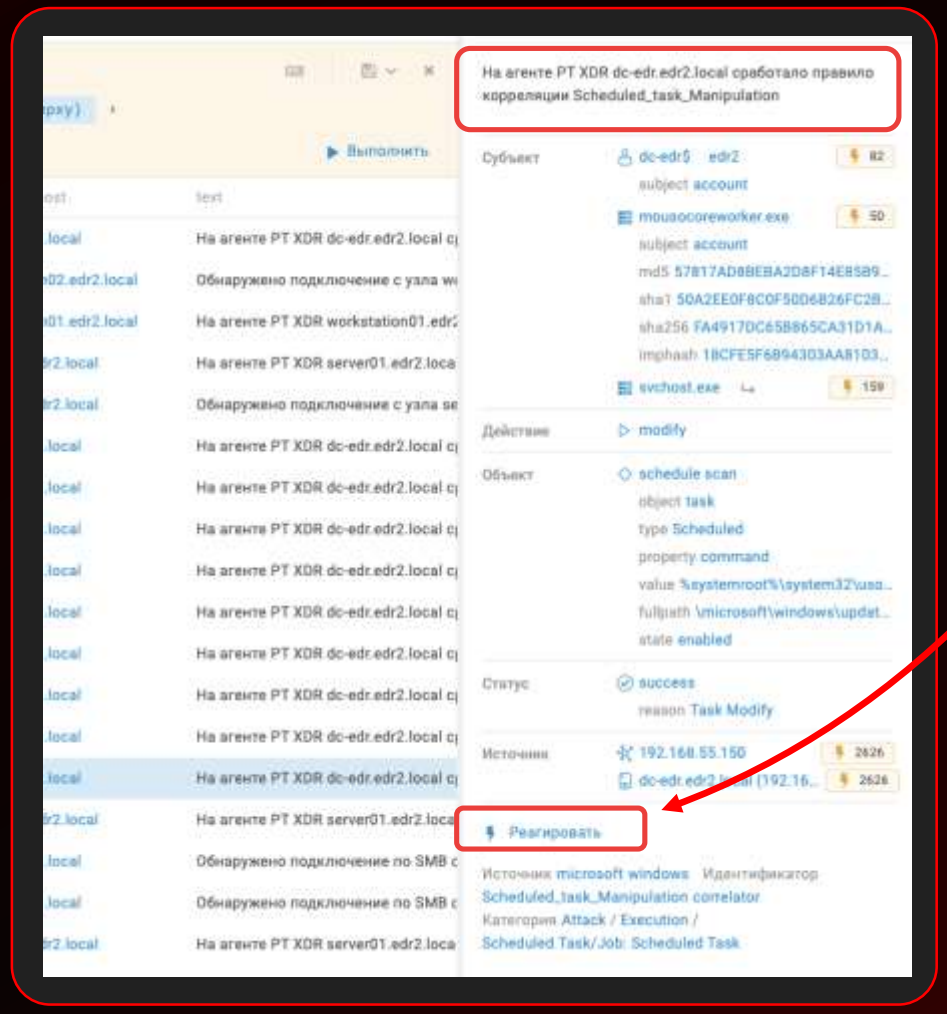


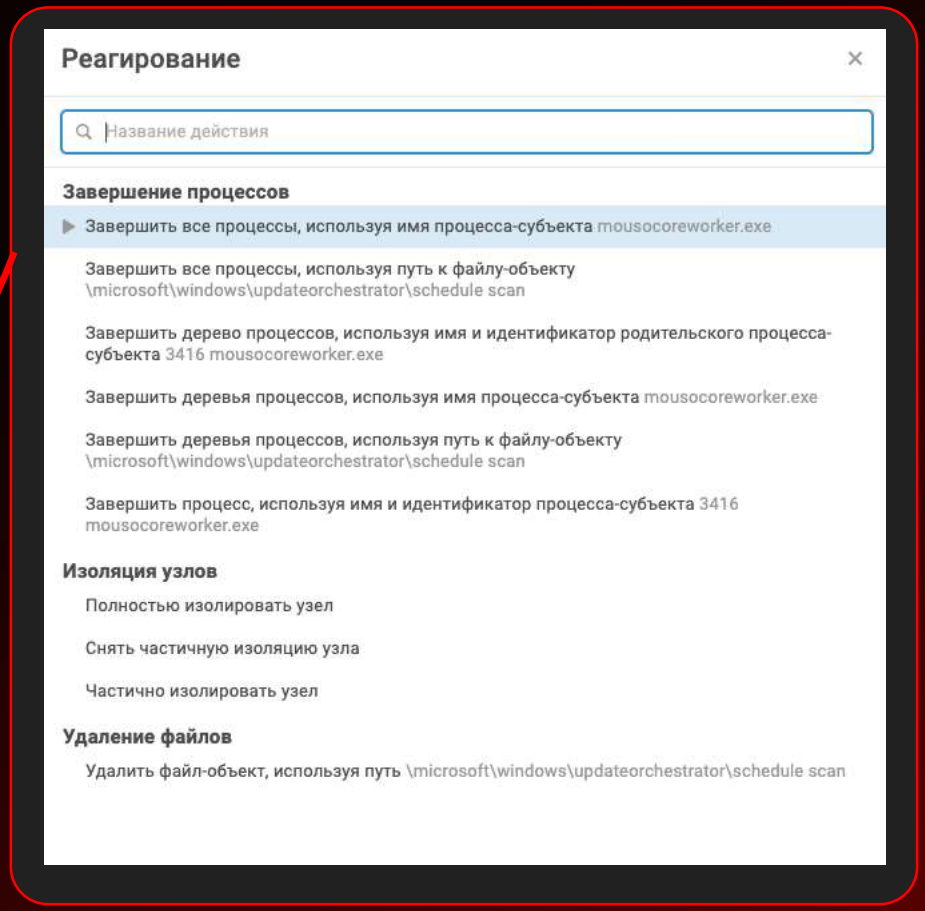
Обновления в следующих релизах



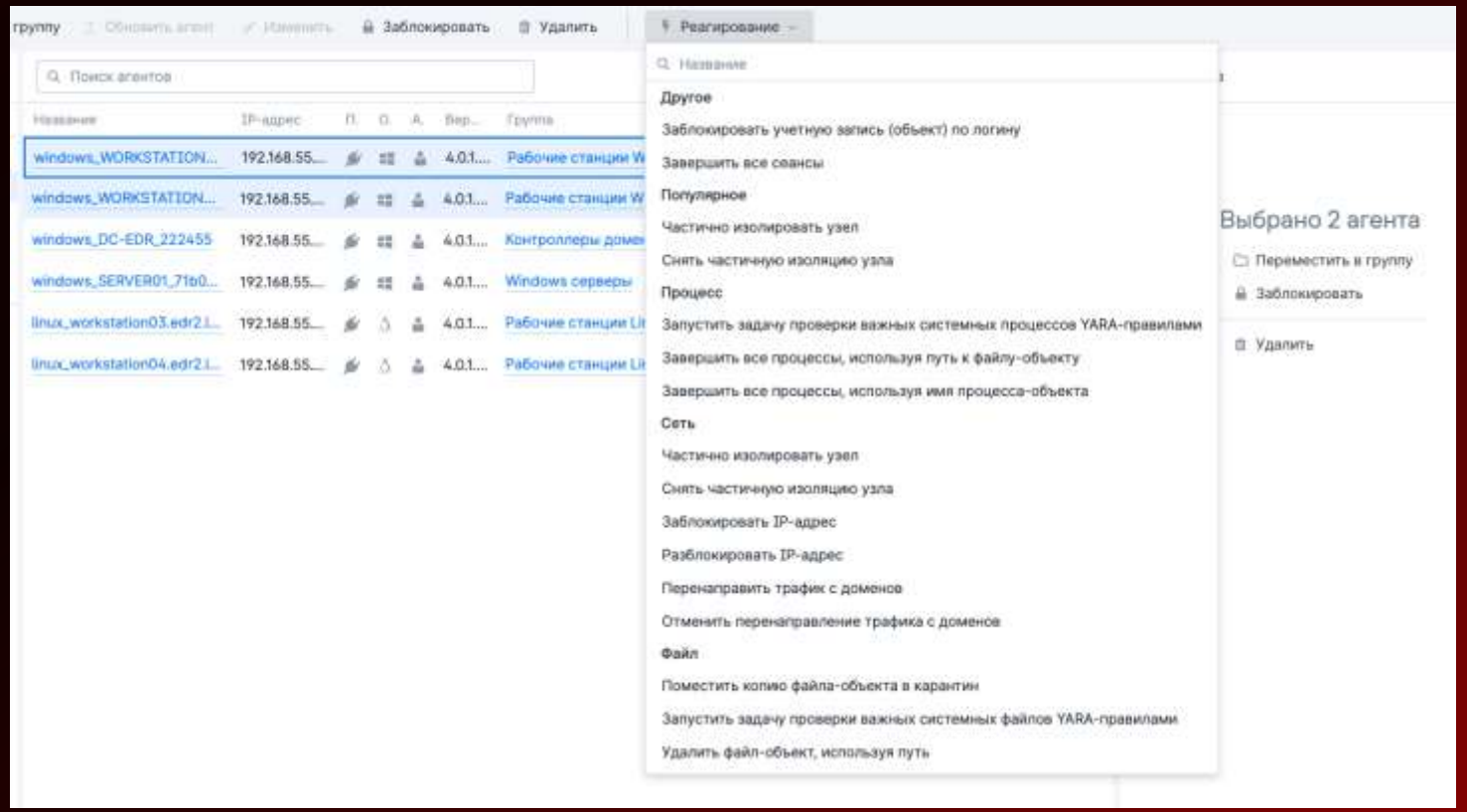
- Новый интерактив работы с файлами: выгрузка, загрузка, удаление, карантин, YARA и AV-сканы
- Новый интерактив для работы с процессами: завершить, просканировать, сделать дамп

Реагирование из карточки события
в 2 клика





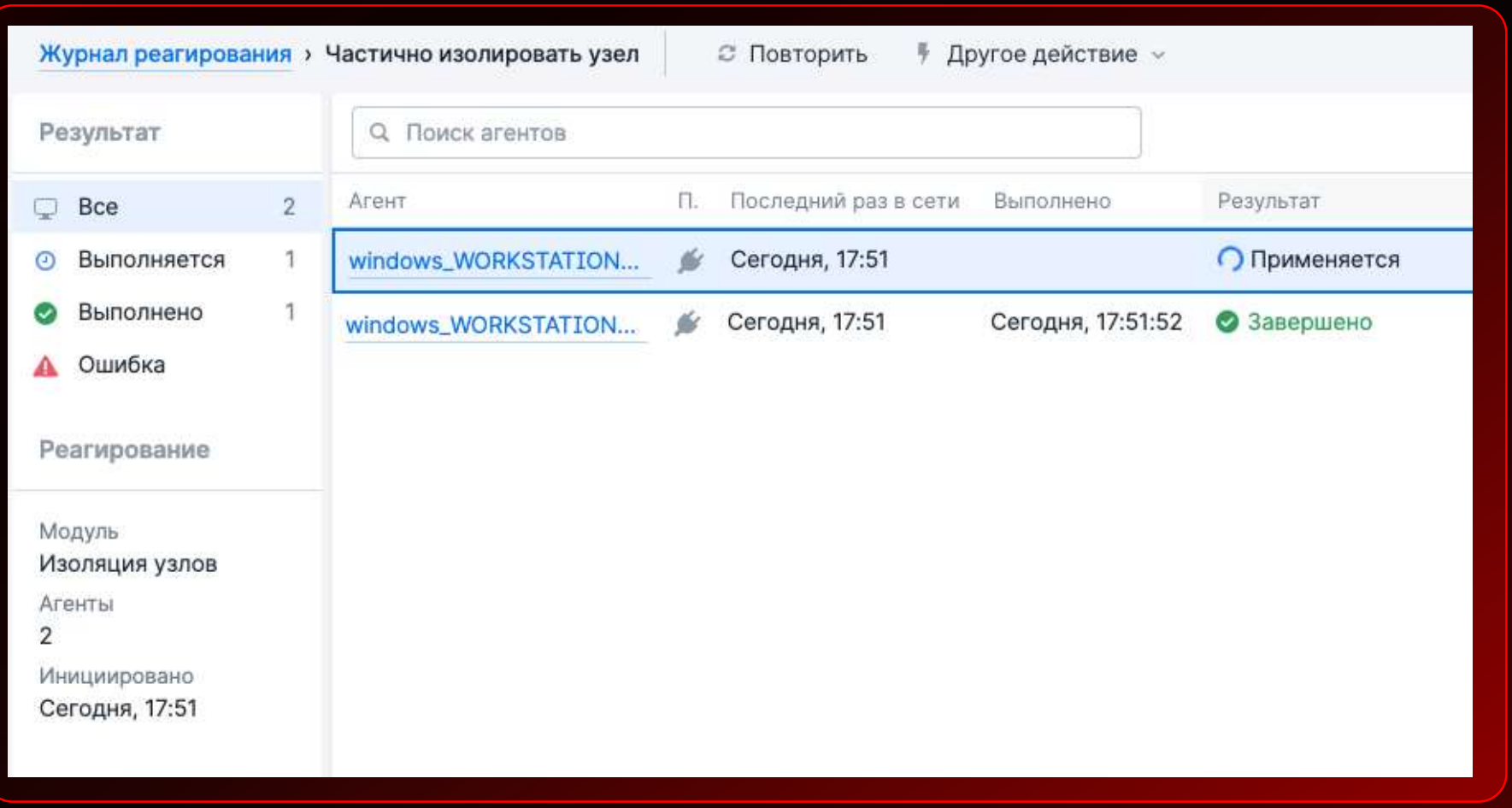
Реагирование на множестве агентов



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

Реагирование на множестве агентов



СЦЕНАРИЙ 3

EDR НА МАКСИМАЛКАХ. ПРОКАЧИВАЕМ ОБНАРУЖЕНИЕ

- Обнаружение на агенте
- Многоэтапные проверки
- Автоматизация реагирования

MaxPatrol EDR: обнаружение

- Поведенческий анализ прямо на устройствах с 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, PT Multiscanner)

ОБНАРУЖИВАЕТ ПОПУЛЯРНЫЕ ТЕХНИКИ ИЗ МАТРИЦЫ MITRE ATT&CK

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

ДАЕТ ВОЗМОЖНОСТЬ ГРАНУЛЯРНОЙ НАСТРОЙКИ СИСТЕМЫ

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

Корреляция на агенте

Sysmon, WEL

T1053 Scheduled Task/Job

Нормализатор	Коррелятор	Контекст
Создание исполняемого файла в TEMP	Создание экземпляра корреляции C2 Dropper	Путь до исполняемого файла Контрольная сумма файла
Запуск исполняемого файла из TEMP	Обогащение новой корреляции C2 Dropper	Информация о процессе Информация о пользователе и сессии
Копирование себя в home пользователя	Обогащение корреляции C2 Dropper	Новый путь до исполняемого файла
Создание задачи в планировщике	Обогащение корреляции C2 Dropper	Имя задачи в планировщике Путь до исполняемого файла в задаче
Запуск задачи из планировщика	Обогащение корреляции C2 Dropper	Информация о процессе Путь до исполняемого файла
Установка сетевого соединения вовне	Обогащение корреляции C2 Dropper	Информация о внешнем узле Информация о сетевом соединении
Создание исполняемого файла в системе	Финализация корреляции C2 Dropper	Путь до нового исполняемого файла Контрольная сумма файла

Пользовательская экспертиза

- Пользователи могут создавать в PT Knowledge Base (PT KB) свои наборы экспертизы для установки в MaxPatrol EDR
- Наборы экспертизы включают правила корреляции и нормализации, а также табличные списки
- Можно использовать отдельные наборы для разных политик

MaxPatrol EDR использует корреляционный движок, который работает на агентах.

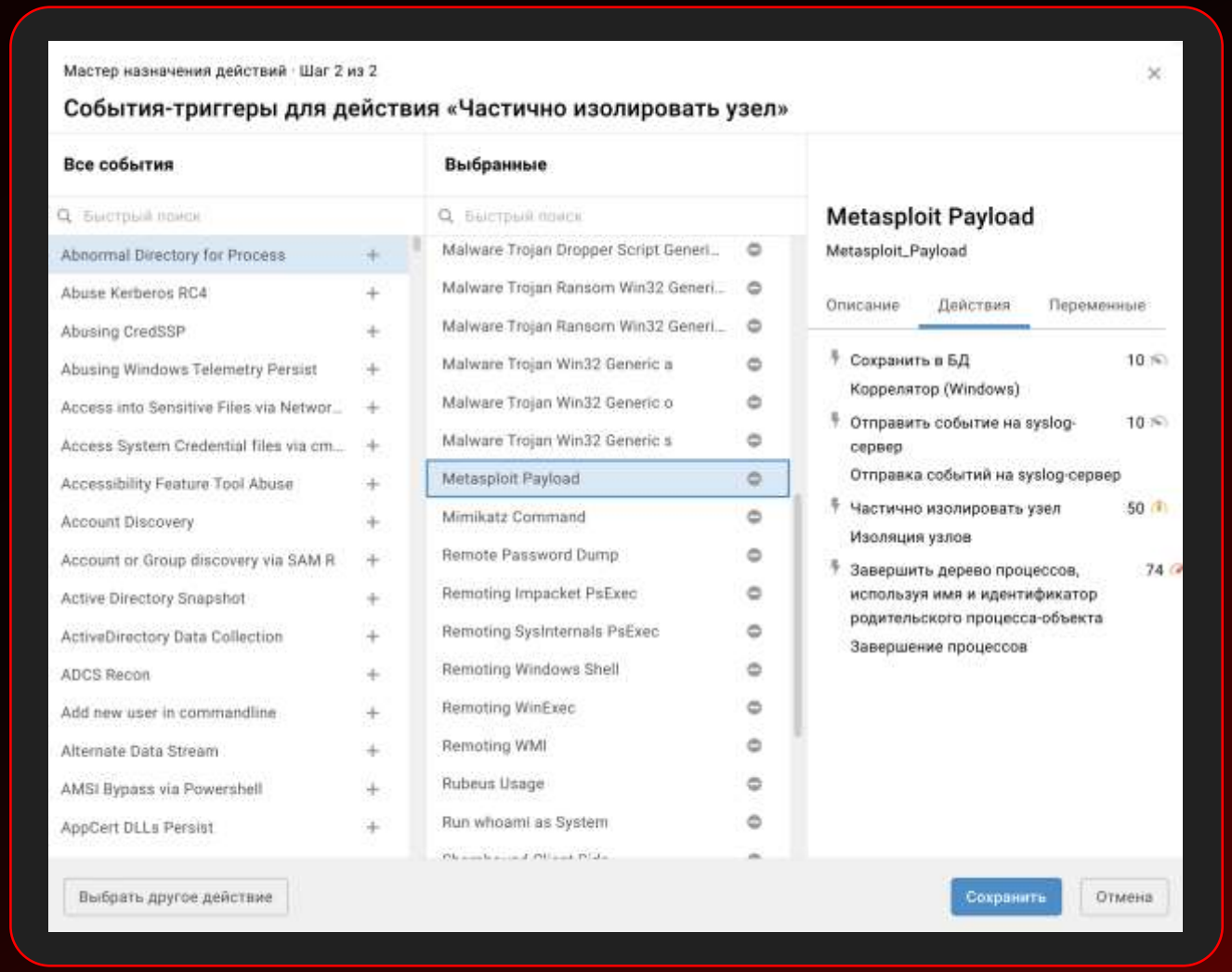
Это позволяет выявлять техники злоумышленников локально. Даже тогда, когда агент не подключен к серверу управления.

Срабатывания коррелятора можно использовать как триггеры для автоматизации действий реагирования

Автоматизация действий

ЭКОНОМИЯ ВРЕМЕНИ И РЕСУРСОВ

- Можно назначить разные сценарии для разных групп агентов
- Действия выполнятся даже в автономном режиме*

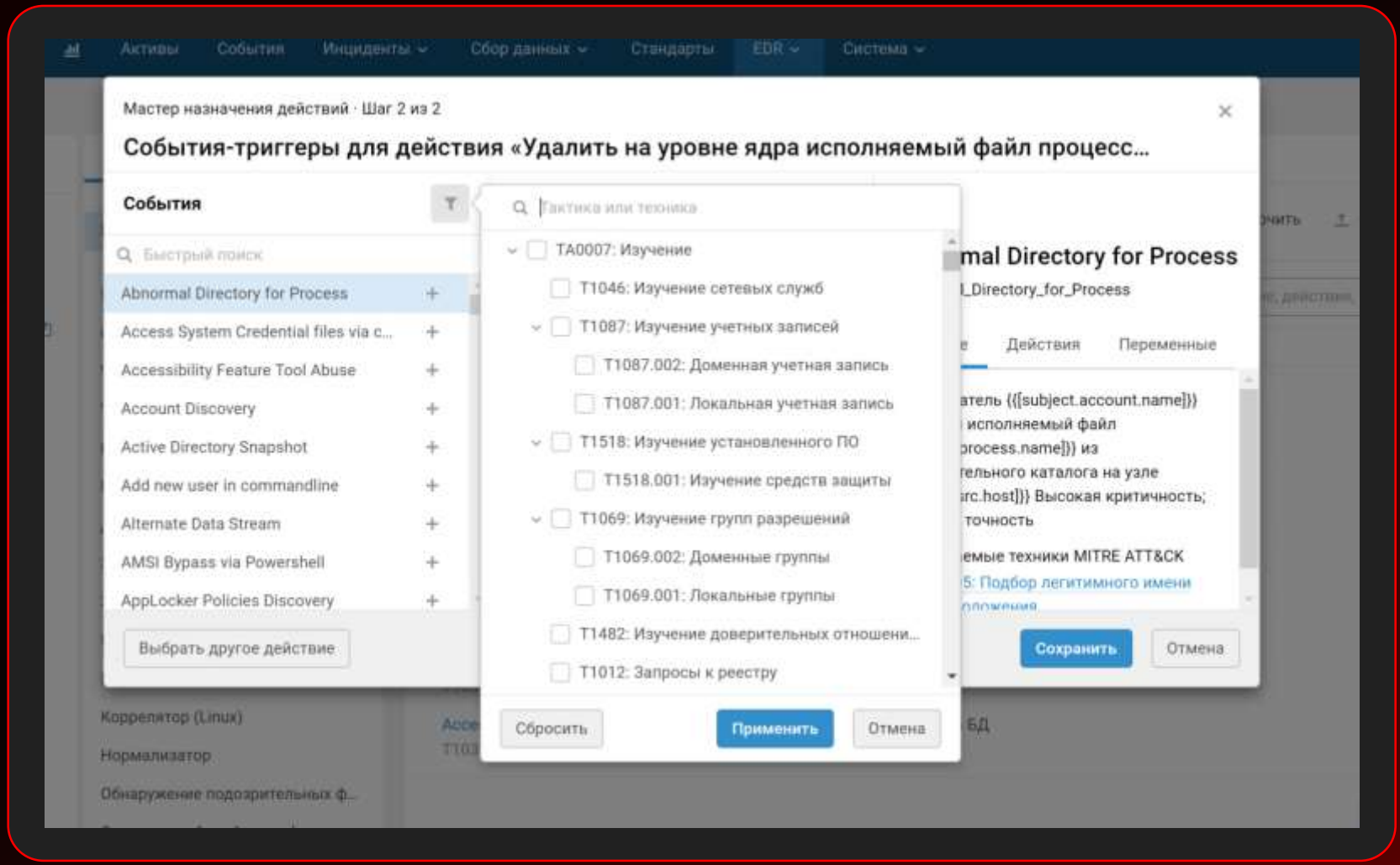


* Если не подразумевают взаимодействия с внешними системами

Автоматизация действий

ФИЛЬТРАЦИЯ ПО ТЕХНИКАМ MITRE

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



MaxPatrol EDR + PT Sandbox для сложных случаев

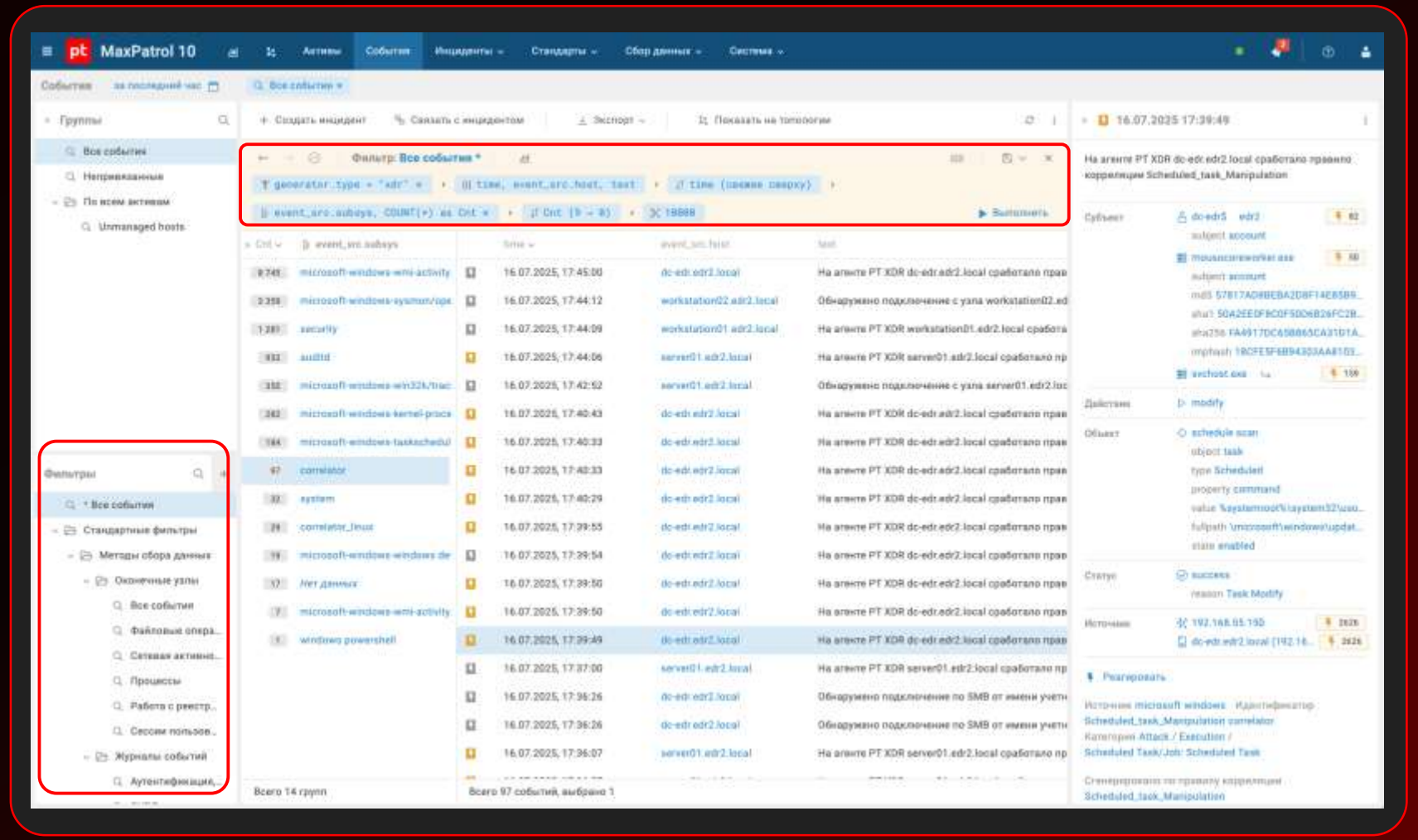
1. Обнаруживаются файлы, скачиваемые, например, через Telegram, браузеры, P2P
2. Проводится подробный статический и поведенческий анализ
3. Реагирование выполняется автоматически в соответствии с параметрами политики

«Работодатель года». Атака Lazarus Group

Объединенная консоль для работы с событиями

ИНСТРУМЕНТЫ ДЛЯ РАССЛЕДОВАНИЯ И THREAT HUNTING

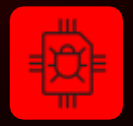
- Группировка событий по активам и типам, преднастроенные фильтры
- Настройка представления: фильтрация, выбор колонок, группировка и агрегация
- Интерактивное добавление условий в фильтры по клику
- Единый интерфейс для MaxPatrol EDR, MaxPatrol SIEM и MaxPatrol VM



Предотвращение известных угроз
на устройствах компании и сотрудников

MaxPatrol EPP

Модули MaxPatrol EPP



В разработке

Антивирусный движок

Молниеносное обнаружение и блокировка угроз на основе эмуляции поведения ВПО.

В разработке

Защита от шифровальщиков

Проактивная защита от шифровальщиков: мгновенная блокировка и восстановление.

В разработке

Контроль устройств

Ограничение доступа и предотвращение несанкционированного использования подключаемых устройств.

2026

Контроль приложений

Разрешение запуска только доверенных приложений.

2027

Защита от веб-угроз

Автоматическая блокировка доступа к опасным сайтам и предотвращение попыток заражения через интернет.

2027

Защита от сетевых угроз

Защита узла от сетевых атак: блокировка вредоносного трафика и подозрительной активности.

План развития в 2025 году

MaxPatrol EDR

MaxPatrol EDR 7.2 → 8.0 → 8.1
Улучшаем UX, управление агентами, выявление угроз, сбор событий
20 РКБ-проектов
Bug Bounty

Q1

Анонс M&A
Расширение команды
Стратегия развития

Q2

PHDays

22–24 мая

Демонстрация антивирусной технологии

Q3

Антивирусный модуль (prevent) в MaxPatrol EDR

Выпуск модуля в коммерческое пользование

Q4

PSD

Новый продукт для защиты устройств класса EPP

Сертификат ФСТЭК по требованиям САВЗ

MaxPatrol EPP

Дорожная карта EDR & EPP

	Q3 2025 – Следующий релиз	**Q3–Q4 2025 – Бэклог со сквозным приоритетом (приоритет может меняться)**
Версия	8.1	8.2–9.0
Product & agent management	• Улучшение UX в части работы с агентами • Темная тема интерфейса • Браузер файлов и процессов с возможностью реагирования • Расширение возможностей интеграции по протоколу Syslog • Перенастройка политик безопасности в зависимости от принадлежности к сети	• Улучшение UX в части настройки политик и основной функциональности • Оптимизация компонентов управляющего сервера: снижение требований к техническим характеристикам серверов, рост эффективности, работа с собственным хранилищем событий • Повышение прозрачности состояния агентов (Health Check), расширение функций аналитики • Развитие методов интеграции для обеспечения реагирования (в частности в PT NAD) • Поддержка новых версий ОС на базе Linux
Detect & Response	• Улучшение интеграции с PT Sandbox (поддержка нового контракта API) • Стабилизация пользовательской экспертизы	• Расширение возможностей сбора событий с помощью eBPF-программ и различных файловых журналов • Расширение возможностей сбора данных для расследования инцидентов • Модернизация поведенческого обнаружения на конечном устройстве • Передача файлов на конечное устройство • Работа с пользовательскими списками IoC на хосте
EPP Endpoint Protection Platform NEW **PT AV**	• Антивирусный модуль с защитой в реальном времени, сканирование по запросу или по расписанию • Списки исключений (whitelists) • Поддержка Windows, Astra Linux и РЕД ОС • Обновленная антивирусная экспертиза от антивирусной лаборатории Positive Technologies	• Новый модуль Anti-Ransomware с автоматическим восстановлением поврежденных объектов (Alpha ver) • Контроль устройств и приложений (Alpha ver) • Развитие технологии превентивного обнаружения на базе антивируса
Цели	Улучшение интеграционных сценариев Улучшение сценариев реагирования Поставка модуля антивирусной защиты в едином агенте	Развитие функций Endpoint Protection Platform Сертификация ФСТЭК по требованиям САВЗ Улучшение опыта управления агентами, улучшенное развертывание и мониторинг Усиление функций сбора событий Качественный рост детектирующих механик за счет новых технологий
События	PSD	GISEC, GITEX

Данный документ не является официальным обязательством и описывает планы развития продукта на июнь 2025 года

Кирилл Черкинский

Руководитель практики
защиты конечных устройств,
Positive Technologies

kcherkinskiy@ptsecurity.com

Спасибо!