Владимир Яцюк
Positive Technologies

MaxPatrol SIEM:

новые функции и методика результативного внедрения

01

Что такое SIEM

Что предлагает MaxPatrol SIEM

+ Полнота аудита инфраструктуры и контроля сбора событий

+ Качество обнаружения атак, в том числе целенаправленных

+ Полнота интеграции со смежными продуктами и встройка в процесс обеспечения ИБ

Знать, где искать → Знать, что искать → Знать, что делать дальше → **Результат**

Главное в последних релизах

27.1
июнь 2024

27.2
сентябрь 2024

27.3
апрель 2025

27.4
июль 2025

27.5+
ноябрь 2025

MaxPatrol SIEM 27.3

- Поддержка Astra Linux 1.7.6
- FlowControl 2.0
- Расширение ролевой модели
- Улучшение UI/UX

MaxPatrol SIEM 27.4

- Оптимизация производительности
- Дашборды Grafana
- Улучшение UI/UX
- Значительные улучшения в MaxPatrol BAD

Релиз 27.3

FlowControl 2.0

Сглаживание потока на стороне receiver

- Health monitor регулярно проверяет состояние очередей
- Для сигнализации используются три уровня: зеленый, желтый и красный
- На желтом уровне система сглаживает поток (троттлинг)
- На красном уровне прием событий временно прекращается
- После нормализации состояния работа конвейера возобновляется

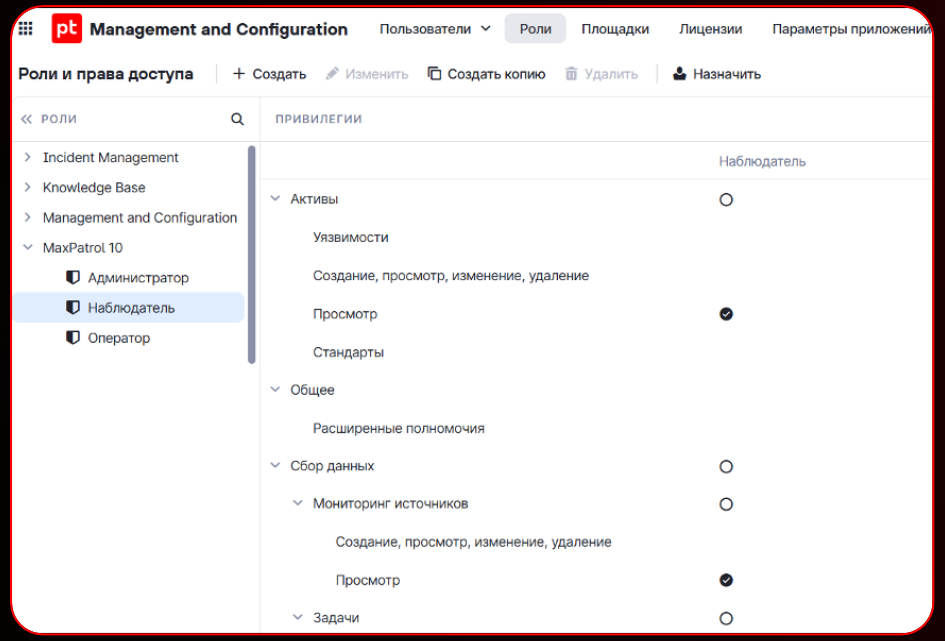
* Можно использовать старый алгоритм (инструкция приведена в документации)

Релиз 27.3

Расширение ролевой модели

Возможность назначения пользователю роли «Наблюдатель»

Read-only-роль
с ограничениями на запуск, остановку, редактирование, создание и удаление задач сбора, правил SIEM, табличных списков и активов. Доступен только просмотр.



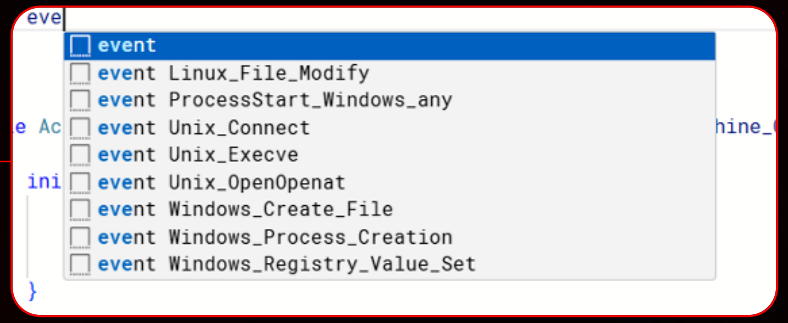
Релиз 27.3

Улучшение UI/UX

Подсветка синтаксиса в PT KB

```
event Remove_Machine_Or_Backup_Plan:
    key:
        event_src.host
    filter {
        filter::NotFromCorrelator()
        and event_src.vendor == "acronis"
        and event_src.title == "backup"
        and action == "remove"
        and in_list(["task", "host"], object)
        and filter::CheckWL_Specific_Only("Acronis_Mass_Drop_Machine_Or_Backup_Plan", lower
        (join([event_src.host, object.type, object.name], "|")))
```

Сниппеты в PT KB




```
event :
    key:
        event_src.host
    filter {
        filter::NotFromCorrelator()
        and
    }
```

Описание правила рядом с названием корреляции

Сгенерировано по правилу корреляции
Abnormal_Directory_For_Process
из 1 исходного события
Исполняемый файл запущен из подозрительного каталога

Релиз 27.4

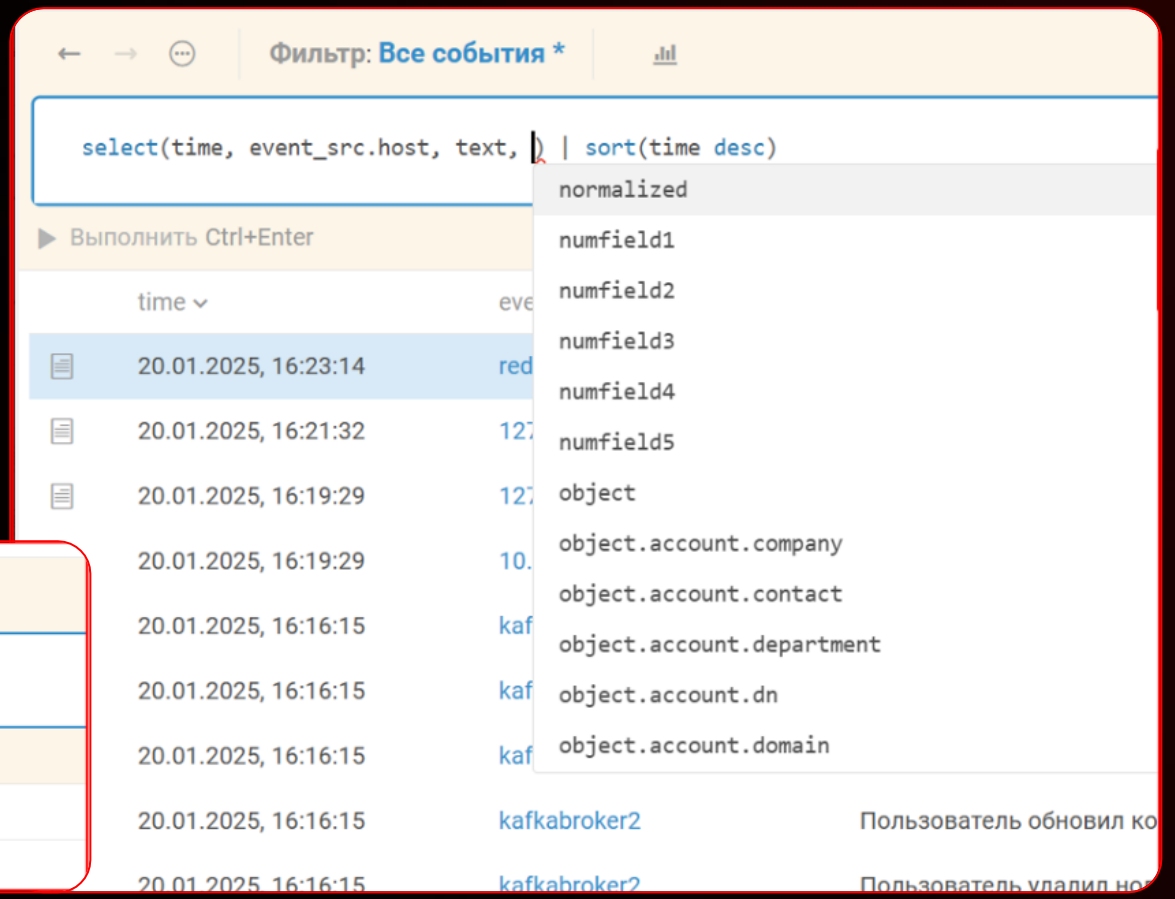
Оптимизация производительности

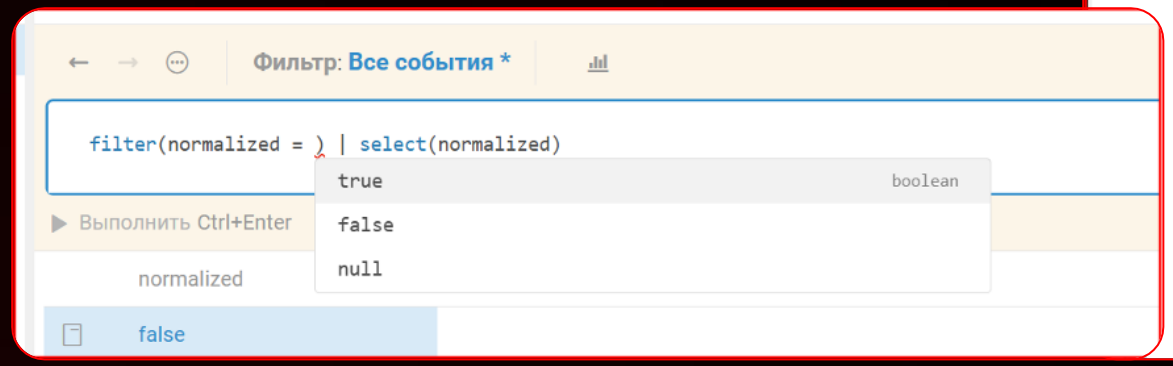
- Объем оперативной памяти, потребляемый коррелятором, снижен **на 20%**
- Ускорена работа страницы **«События»**
- Увеличена производительность модуля SysLog MP 10 Collector
- Очистка фильтров от избыточных скобок
- Автоподстройка потоков в конвейере обработки событий
- Автоматическое развертывание средне- и высоконагруженных систем с помощью манифеста
- Одновременное обновление однотипных ролей (с помощью манифеста)

Релиз 27.4

Автокомплит в PDQL- запросах

- подсказки по синтаксису PDQL
- подсказки по полям таксономии
- автоматическое открытие и закрытие скобок и кавычек
- подсветка синтаксиса
- real-time-валидация синтаксиса запроса

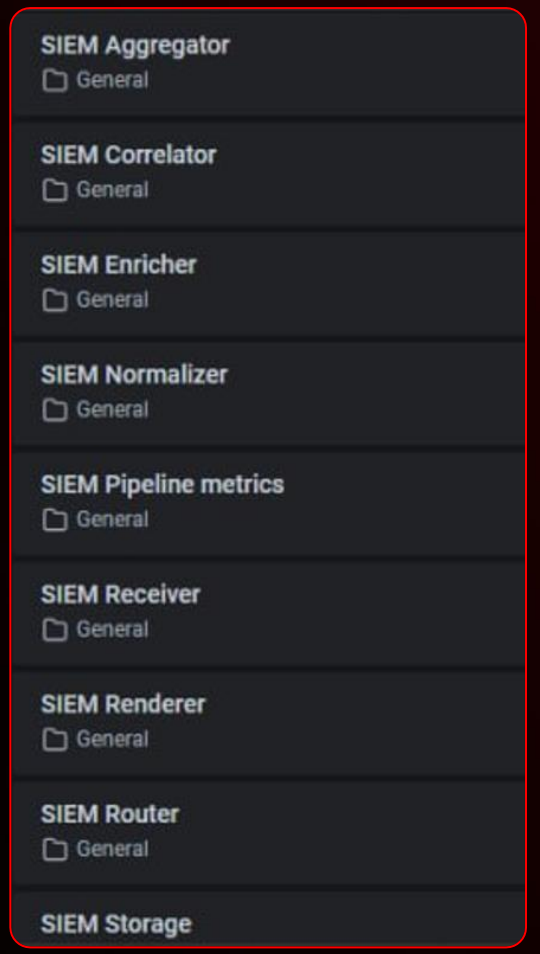




Релиз 27.4

Дашборды Grafana

- Время работы сервиса
- Количество воркеров для каждого сервиса
- Количество медленных событий за минуту
- Метрики fpta
- Количество входящих пакетов на receiver
- Время обработки пакета
- Количество нормализованных и ненормализованных событий (в том числе по источнику)
- Количество событий с ошибками при записи в БД
- И так далее...



Следующий релиз 27.6

R27.6 — осень (ноябрь)

- Умная кластеризация (группировка) событий
- Развитие PT KB: тестирование в WebUI
- HA-кластер и обновление без простоя
- Multitenancy 2.0 — оркестрация тенантов
- Кластер LogSpace
- Развитие BAD

Повышение отзывчивости UI и оптимизация аппаратных ресурсов

Повышение стабильности. Self-healing

Следующий релиз 27.6

Умная кластеризация (группировка) событий

Объединение событий в кластеры по степени похожести

Критерии кластеризации:

- поля события (не более трех)
- процент схожести для каждого поля
- лимит (max число событий, которые можно кластеризовать)

Развитие PT KB: тестирование в WebUI

Возможность тестирования правил внутри PT KB

HA-кластер и обновление без простоя

- Изоляция сервисов
- Обновление плеча кластера поочередно, без остановки сервисов
- Кластеризация коллектора
- Следующий шаг (осень 2025) — deployer для кластерной инсталляции

Без привязки к релизам MaxPatrol SIEM

Central Management Console

Roadmap

Q2 2025
MVP

Q4 2025
Инциденты
и тенант-локатор

2026
Мультиплексирование
для MaxPatrol SIEM (MVP)

Июль 2025

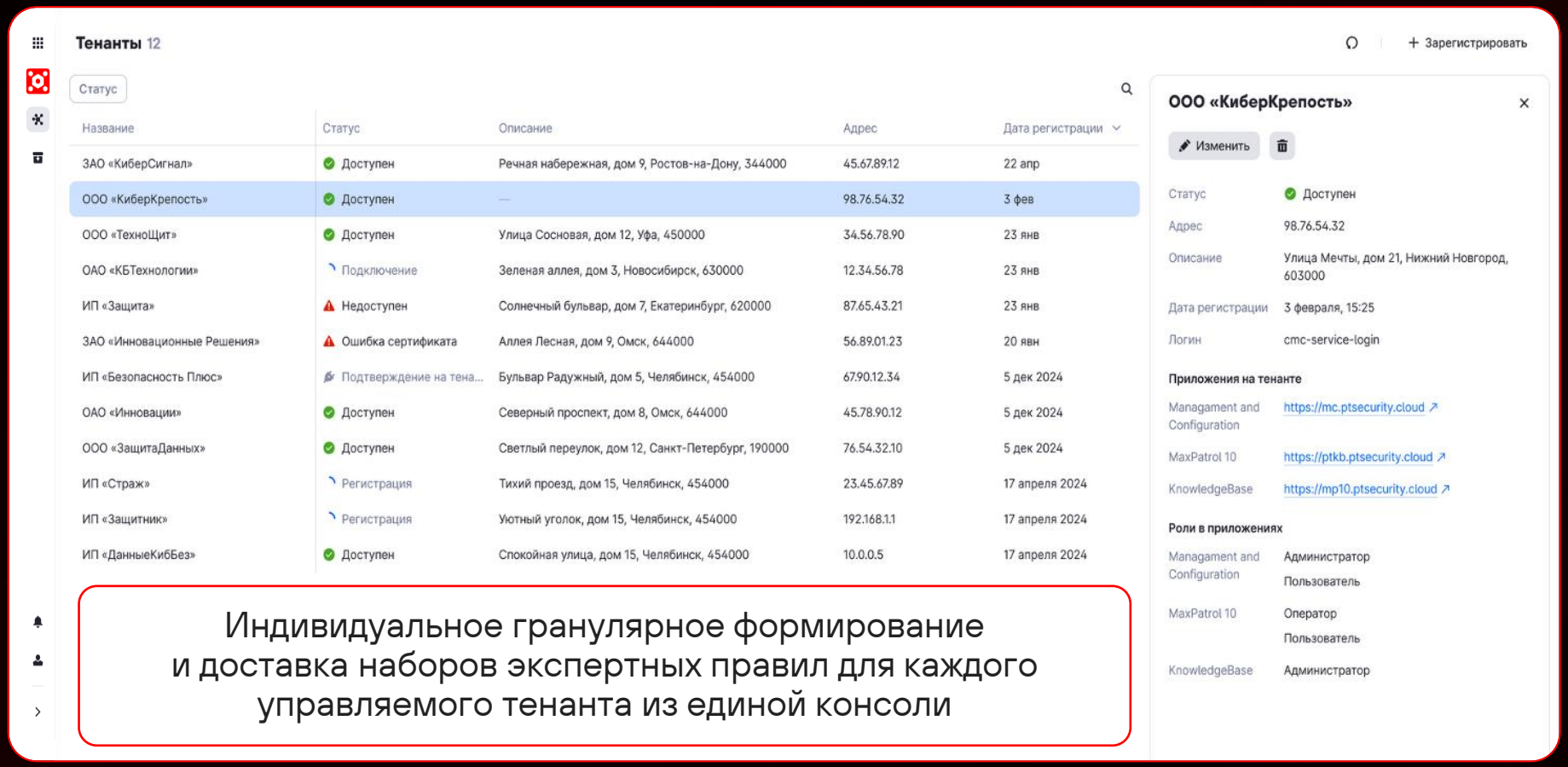
- Central Management Console как инструмент управления тенантами
- Централизованное распространение экспертизы

Осень 2025

- Мультитенантный Incident Management и дашборды
- Централизованная установка в конвейеры
- Переход по тенантам в режиме SPoG

Central Management Console

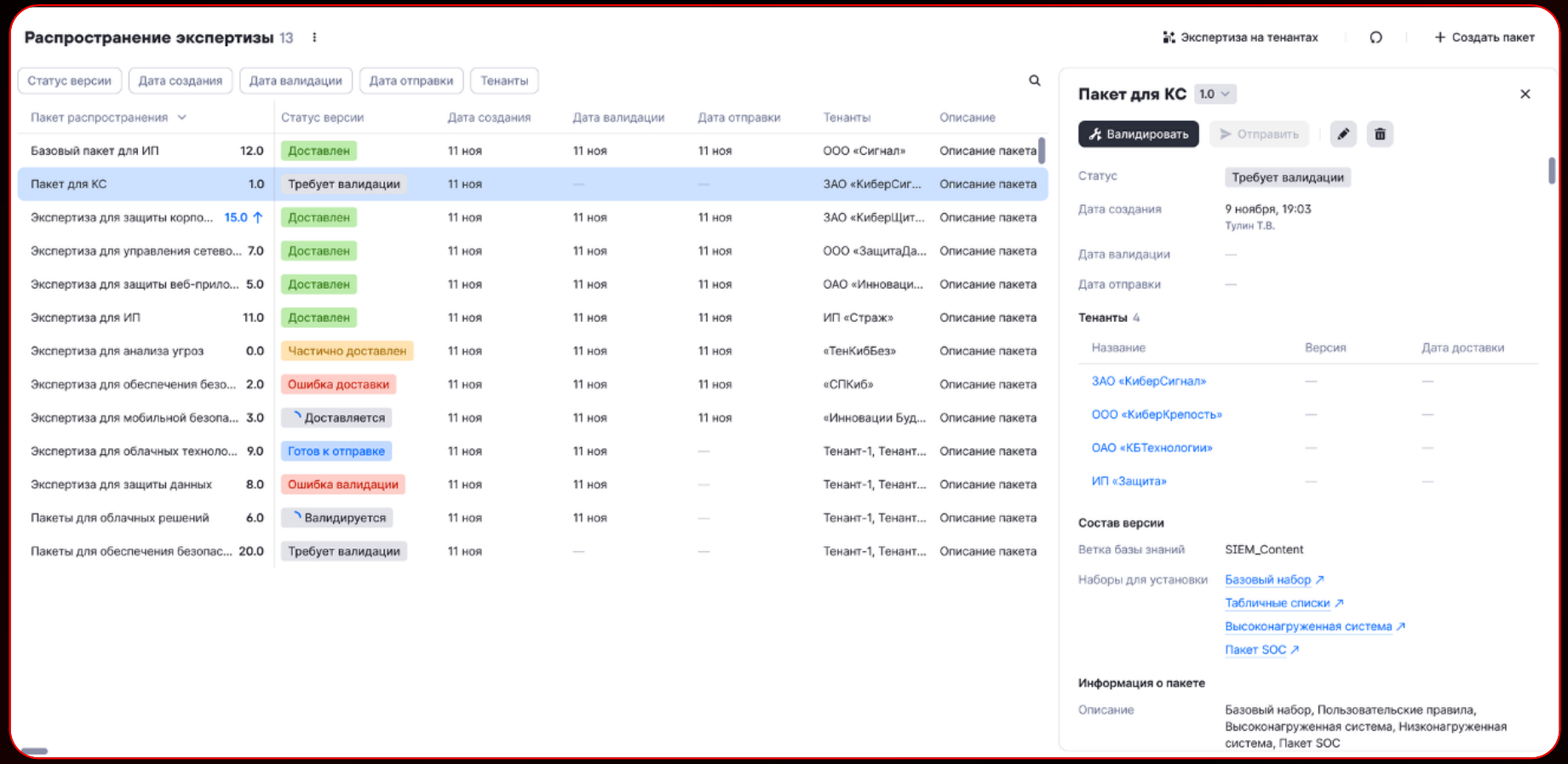
Централизованное распространение экспертизы



Индивидуальное гранулярное формирование
и доставка наборов экспертных правил для каждого
управляемого тенанта из единой консоли

Central Management Console

Централизованное распространение экспертизы



02

MaxPatrol BAD

ML-модуль MaxPatrol BAD

Behavioral Anomaly Detection (BAD) — высококвалифицированный помощник

Приоритизирует работу оператора — акцентирует внимание на событиях MaxPatrol SIEM с наиболее высоким уровнем риска, опираясь на вердикт ML-моделей

Расширяет возможности MaxPatrol SIEM — работает как второй эшелон защиты, самостоятельно обнаруживает скрытые и целенаправленные атаки

Для чего нужен MaxPatrol BAD

1. Самостоятельно обнаруживает целенаправленные атаки и создает алерты, выступая вторым эшелоном защиты

2. Снижает TTR, фокусируя внимание оператора на самых опасных событиях и на расширенной аналитике по ним

MaxPatrol BAD
AI/ML-помощник для оператора SOC

Ключевые преимущества

Дает фокус на самые опасные инциденты

Корреляция отсекает очевидное, BAD классифицирует сложное: оператор видит 3 инцидента с высоким приоритетом, а не разбирает 100 «серых» алертов.

Видит то, что скрыто

Выявляет нетипичное поведение в инфра-структуре, расширяя зону контроля за счет поведенческого анализа.
Обнаруживает аномалии, которые невозможно поймать с помощью стандартных правил и сигнатур.

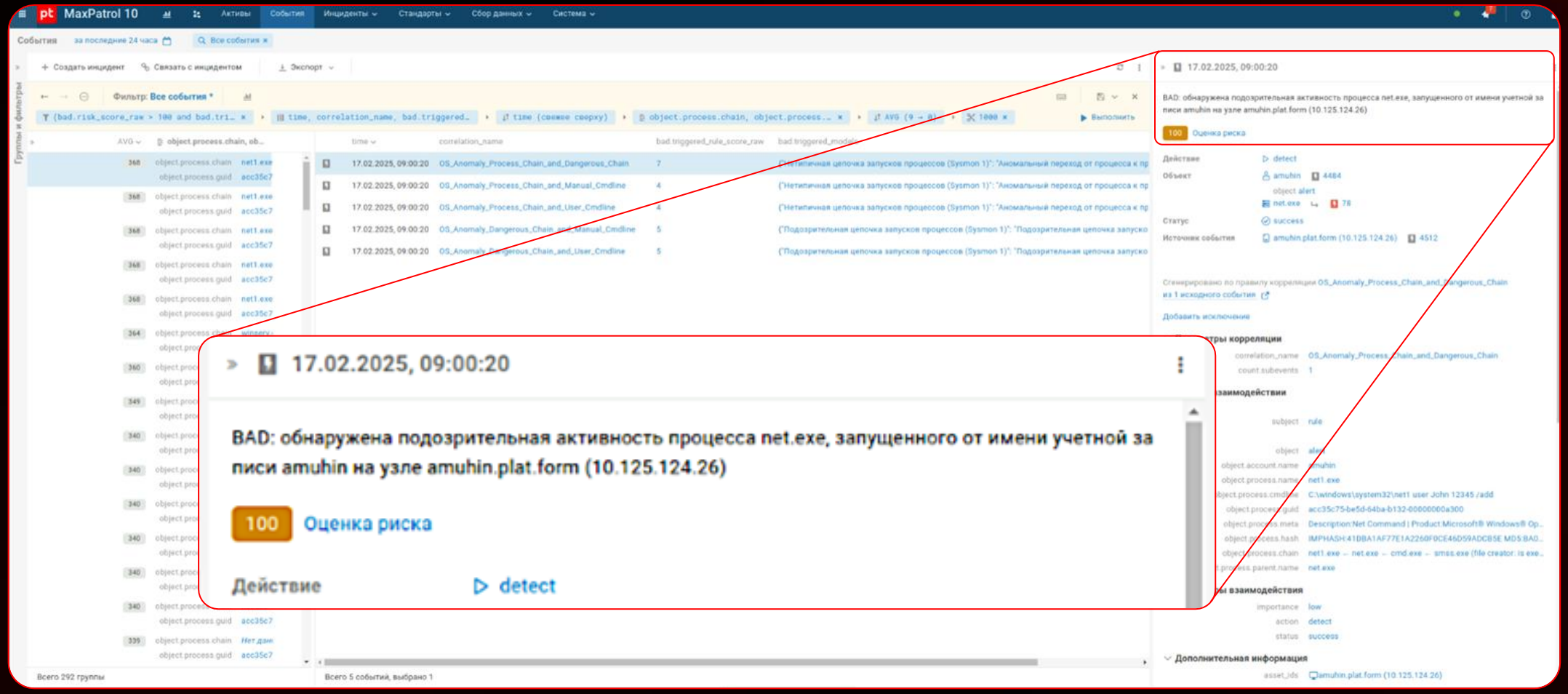
Работает без ручной настройки

Не требует обновления правил или постоянной донастройки.
Автономные механизмы обучения начинают работать сразу, первые релевантные результаты — через 1–2 недели.

Подстраивается под инфраструктуру

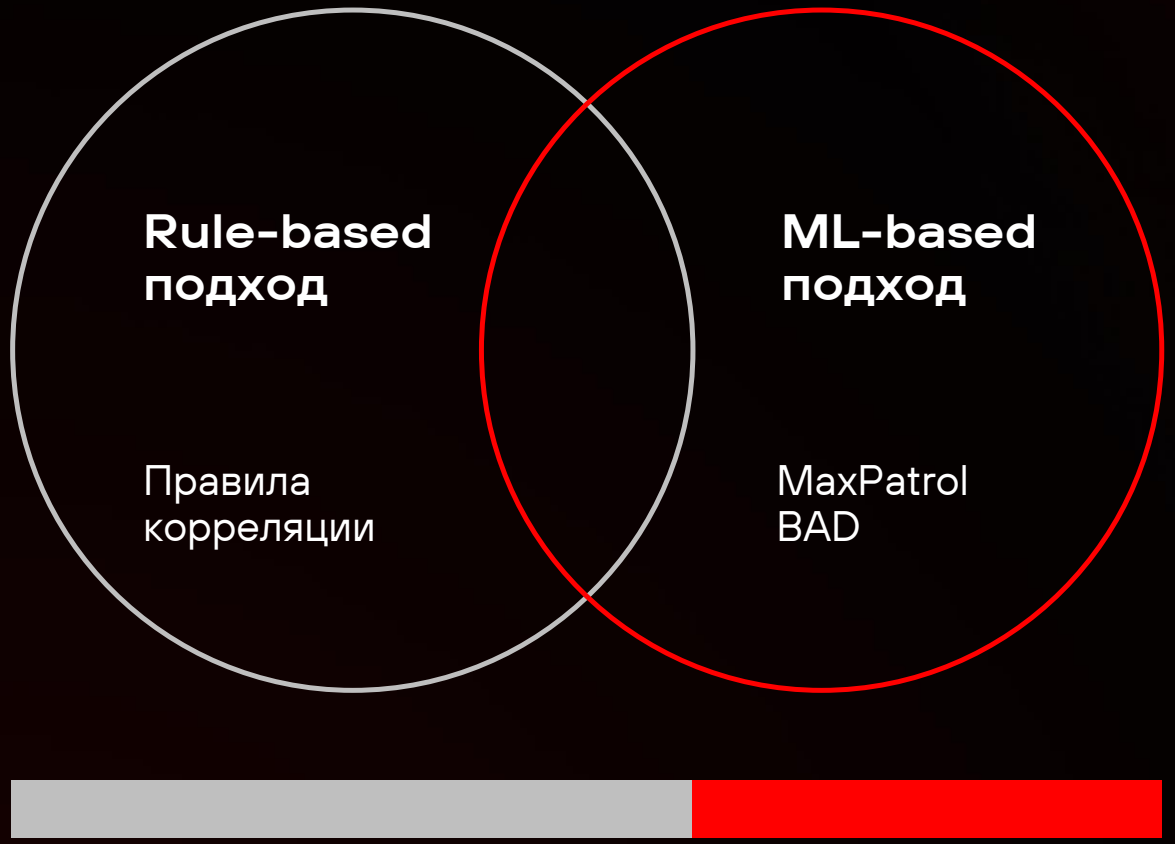
Система адаптирует логику детекта и переобучается на данных инфраструктуры, снижая количество ложных срабатываний.
Минимум false positive, максимум пользы — без участия человека.

Видит то, что скрыто



Собственные события от MaxPatrol BAD — увеличение полноты покрытия обнаружения угроз

Практические результаты



С MaxPatrol BAD видно больше угроз

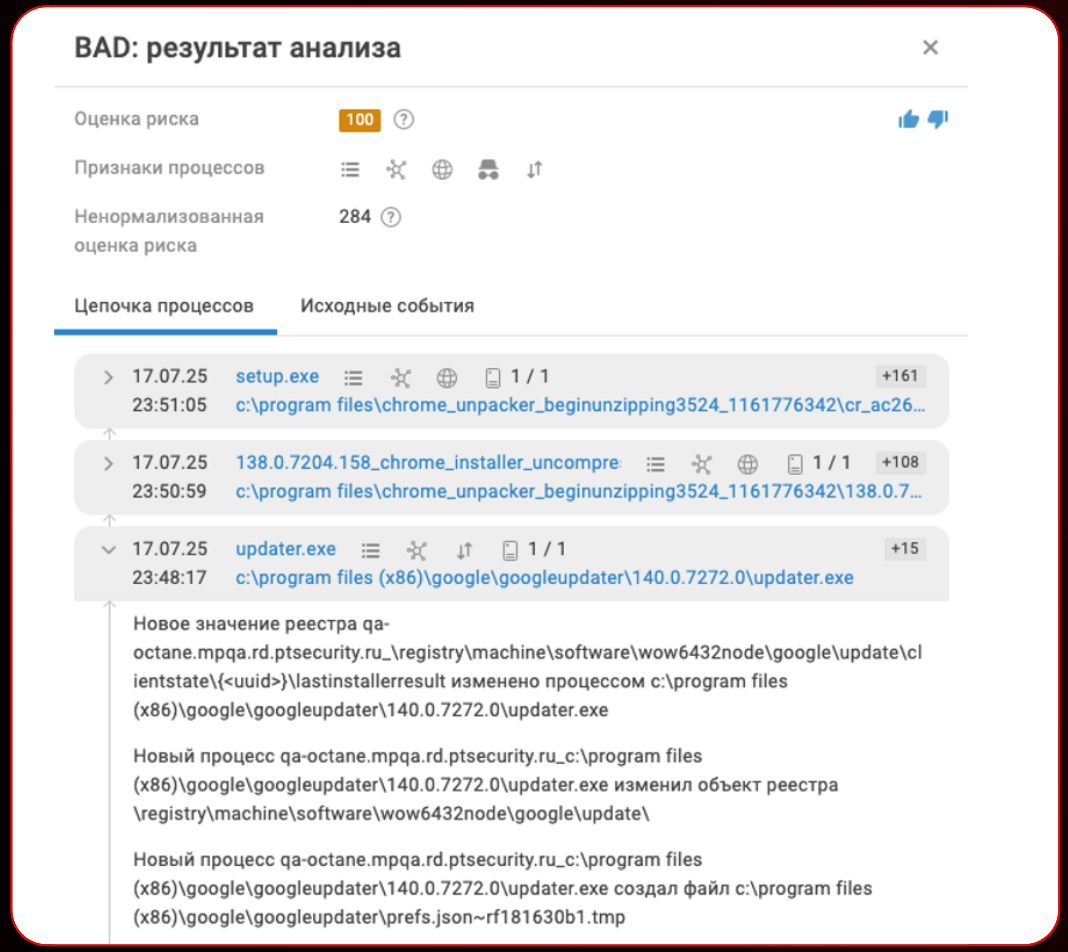
+7 уникальных подтвержденных инцидентов
за 2 месяца
в инфраструктуре
Positive Technologies

360° видимость:
где не хватает корреляций —
действует MaxPatrol BAD

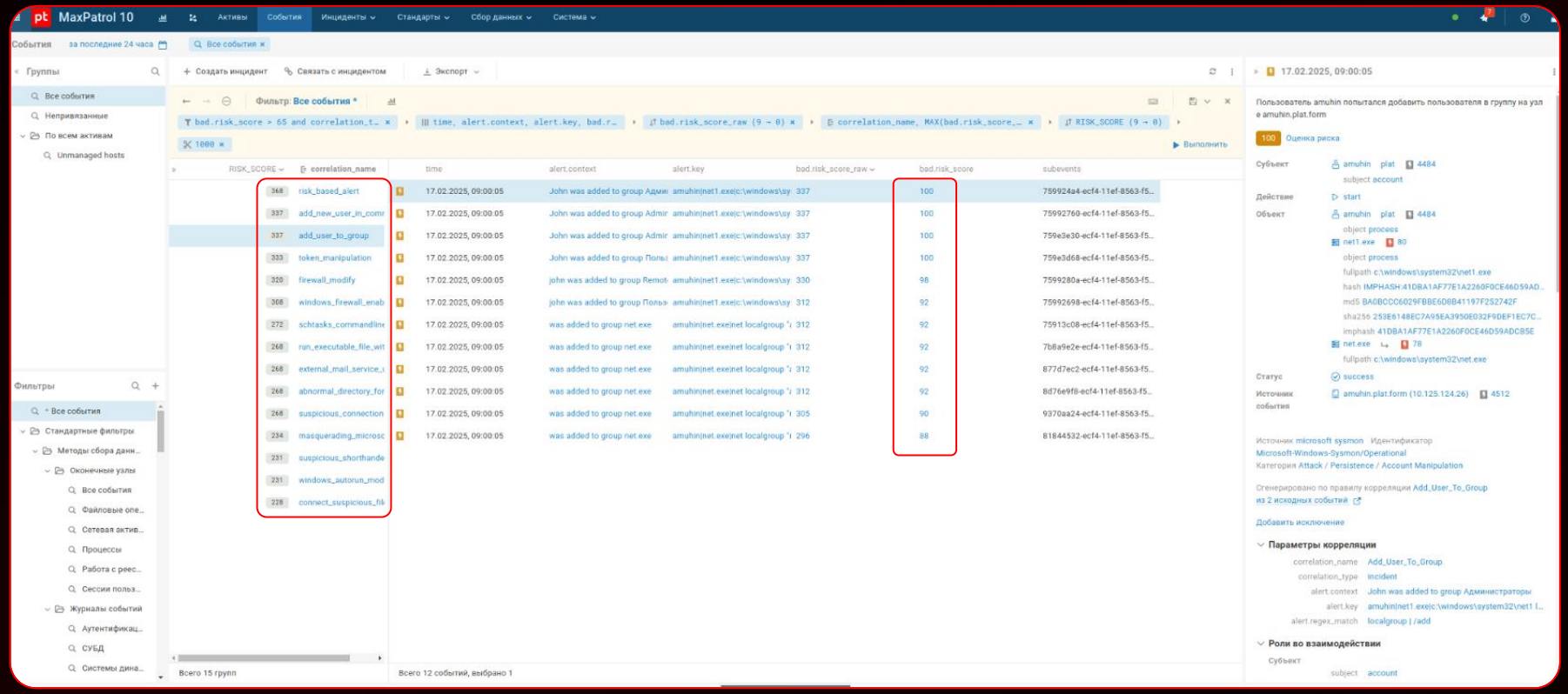
Расширяет контекст

Второе мнение внутри карточки события — FN

- Расширенная аналитика внутри карточки события в удобном виде помогает оператору в расследовании
- MaxPatrol BAD самостоятельно собирает контекст события и проверяет его легитимность без участия аналитика MaxPatrol SIEM



Подсвечивает то, что действительно важно



MaxPatrol BAD приоритизирует события по оценке риска, а аналитик сразу реагирует на самое опасное

Практические результаты

90%

алертов

MaxPatrol SIEM на потоке событий от атакуемой инфраструктуры были классифицированы MaxPatrol BAD как реальные атаки. Модуль ранжировал их по убыванию риска.

Результаты подтверждены оператором SOC Positive Technologies в рамках анализа событий.

Основные показатели

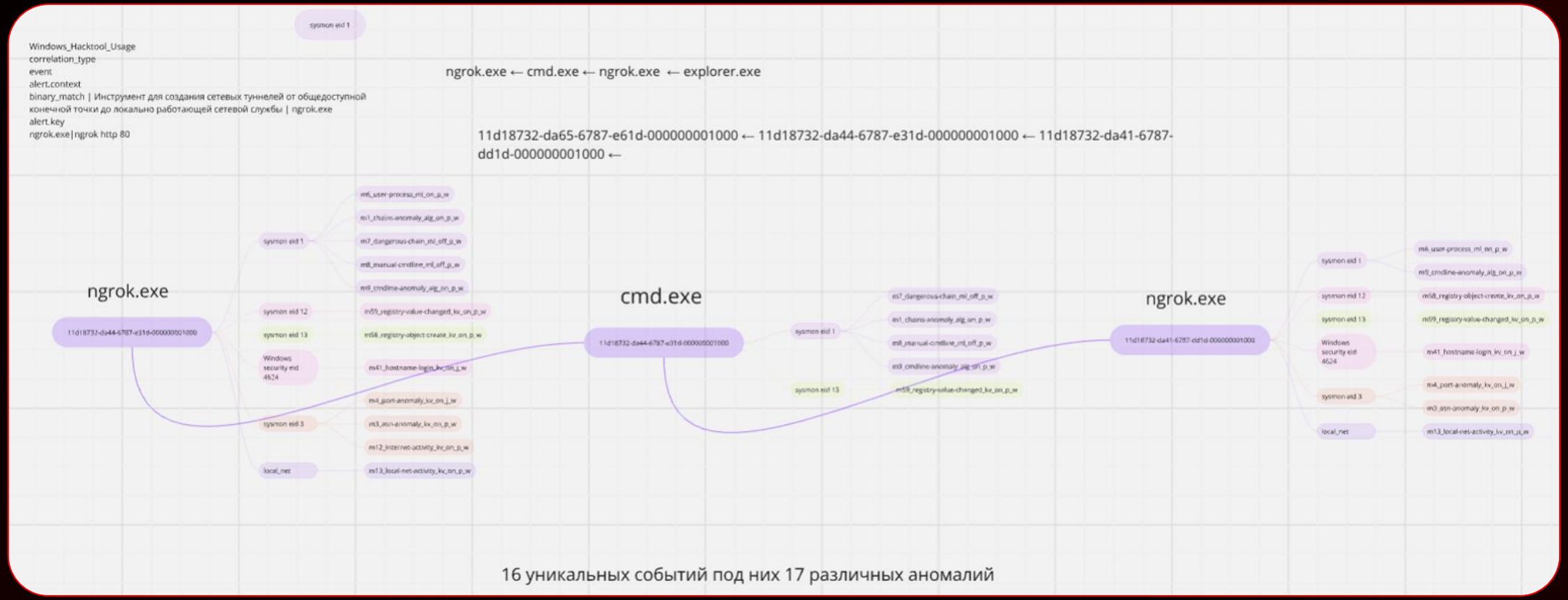
72

ML-модели

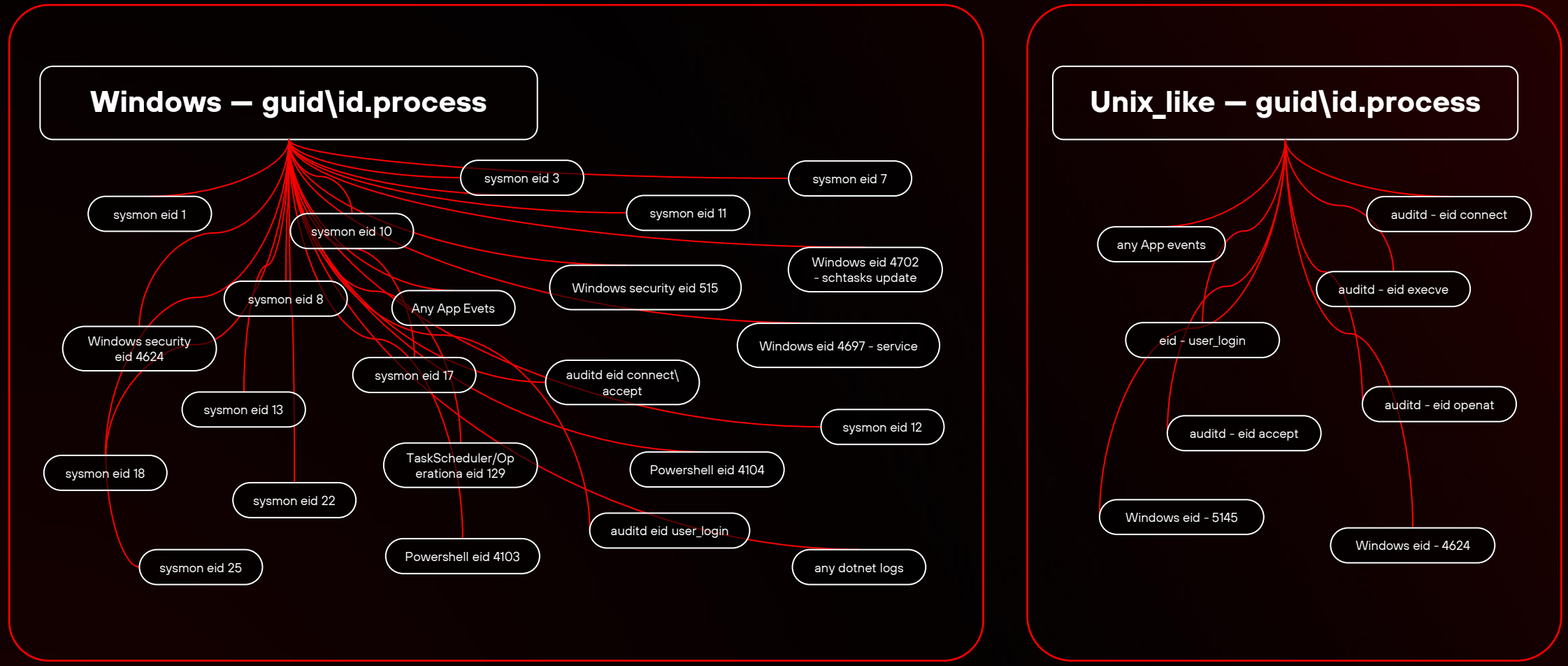
Выявление аномалий на базе событий из 14

- Windows + Sysmon
- KSC
- SQL Server
- TeamCity
- 1C Enterprise
- Keycloak
- Passwork
- AuditD
- vSphere (ESXi)
- Check Point Gaia
- Cisco (IOS, ASA, FWSM, PIX)
- FortiGate
- OpenVPN
- Artifactory

Как работает BAD



Целевая модель данных



Аппаратные требования

Аппаратные требования к серверу ядра MaxPatrol BAD

Компонент сервера	Минимальные требования
Количество логических ядер в системе виртуализации	2
Память (ОЗУ)	4 ГБ
Жесткий диск (HDD)	100 ГБ

Аппаратные требования к серверу анализатора поведения MaxPatrol BAD в конфигурации для средненагруженных систем

Компонент сервера	Минимальные требования
Количество логических ядер в системе виртуализации	16
Память (ОЗУ)	64 ГБ
Твердотельный накопитель (SSD)	5000 ГБ

Аппаратные требования к серверу анализатора поведения MaxPatrol BAD в конфигурации для высоконагруженных систем

Компонент сервера	Минимальные требования
Количество логических ядер в системе виртуализации	24
Память (ОЗУ)	128 ГБ
Твердотельный накопитель (SSD)	8000 ГБ

> BAD 27.4:

- 1 × ВМ под bad-core
- k × ВМ под bad-analyzer
  (k — количество конвейеров)

> BAD 27.3 и ниже:

- 1 × ВМ под bad-analyzer,
  только на главный конвейер

https://doc.ptsecurity.com/ru-RU/projects/bad/27.4/help/9226133899

Технические требования

Совместимость версий MaxPatrol SIEM — MaxPatrol BAD

- MaxPatrol SIEM 27.3 и ниже — MaxPAtrol BAD 27.3 (установка MaxPatrol BAD только на главный конвейер)
- MaxPatrol SIEM 27.4 — MaxPatrol BAD 27.4 (установка MaxPatrol BAD на любое количество конвейеров)

Поток на анализатор MaxPatrol BAD не более 15к EPS (до 40к EPS на конвейер)

Наличие событий Microsoft Sysmon, Windows Event Log и auditd

Roadmap BAD

R27.4

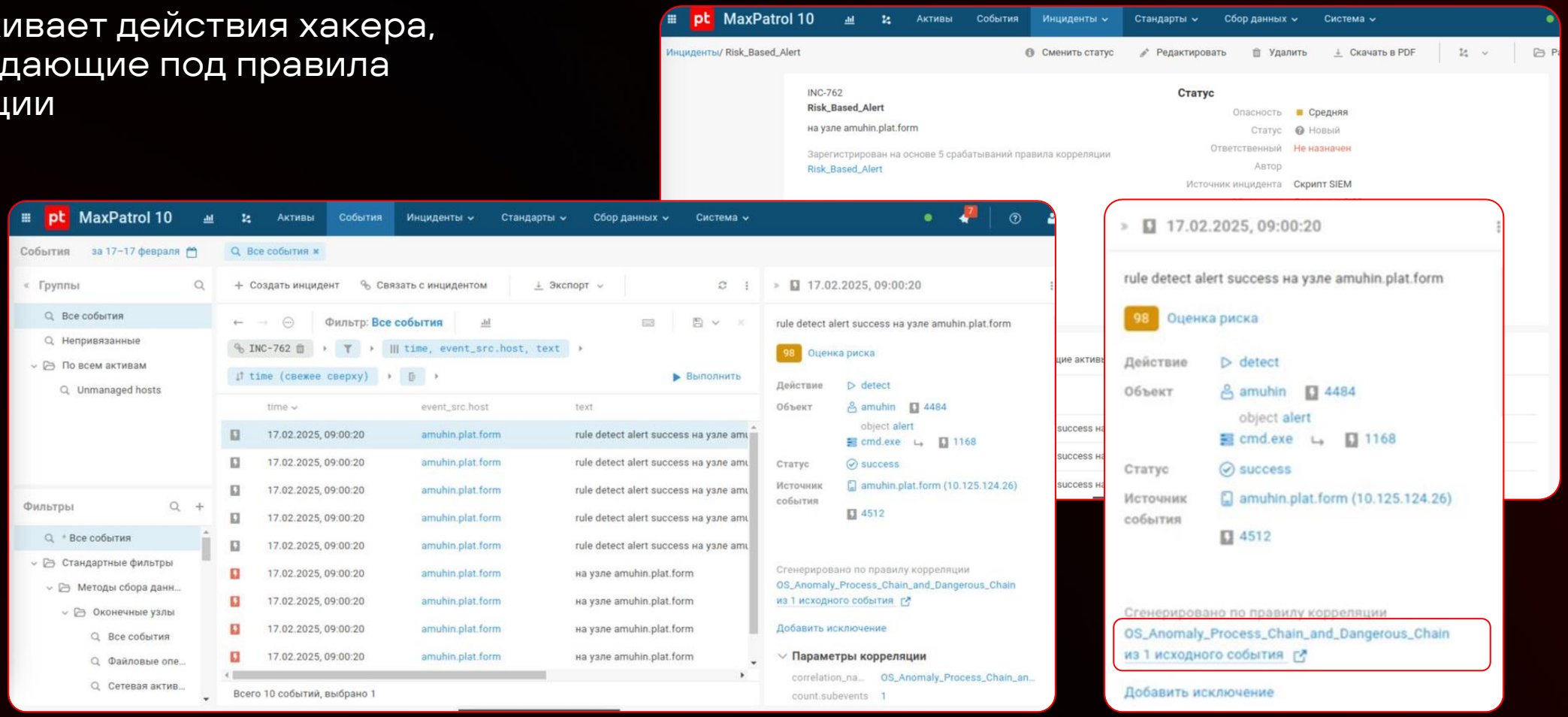
- Лицензирование BAD
- Работа BAD с множеством конвейеров 1 к 1
- Бесшовная интеграция — без правил брокера
- Обновленный UI BAD в карточке события
- Дашборды Threat Detection и Health Monitor
- Стандартные фильтры для работы с BAD

R27.5+

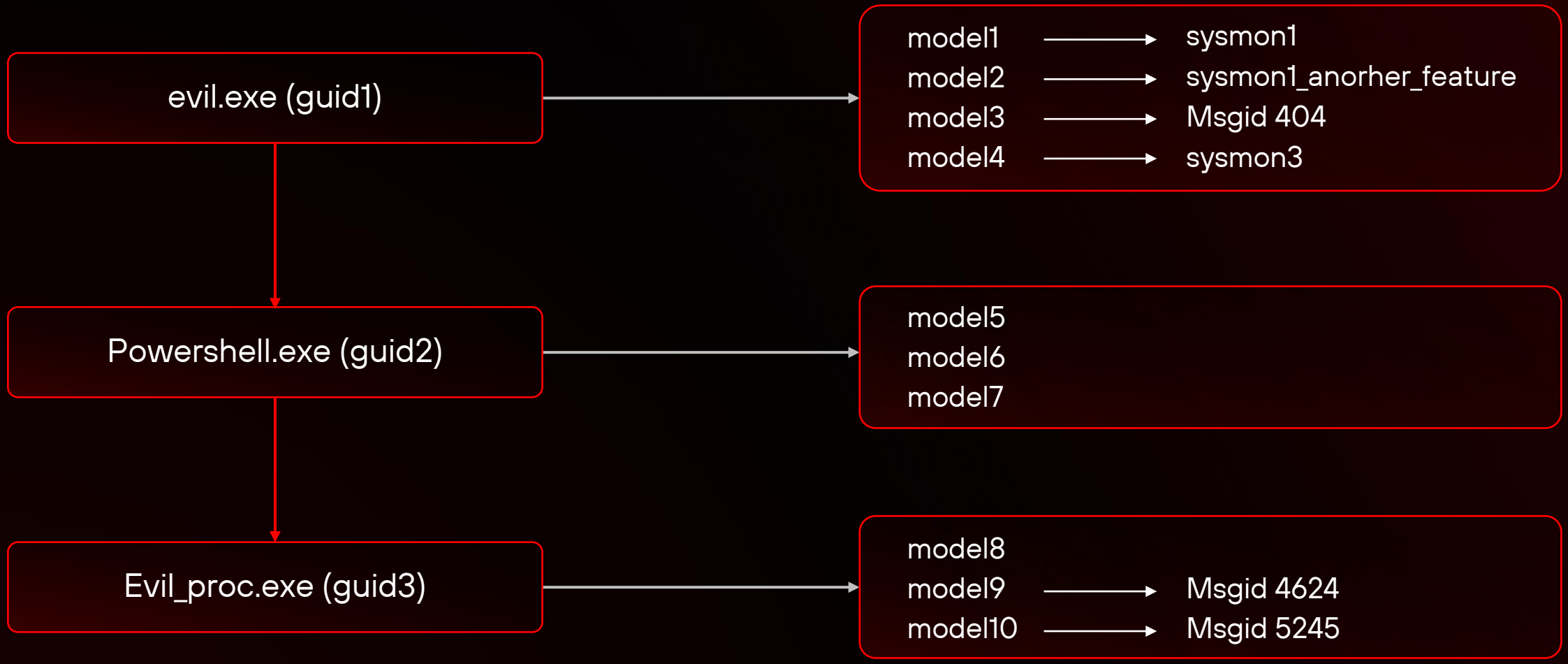
- Расширение моделей для Unix-like ОС
- Работа BAD с множеством конвейеров 1 ко многим
- Кластеризация похожих сработок внутри BAD — снижение FP

Второй эшелон защиты

Обнаруживает действия хакера,
не подпадающие под правила
корреляции



Пример работы

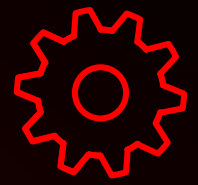


03

Мониторинг источников

Мониторинг источников 2.0

MaxPatrol SIEM не даст злоумышленнику обойти систему,
используя слепые зоны в мониторинге

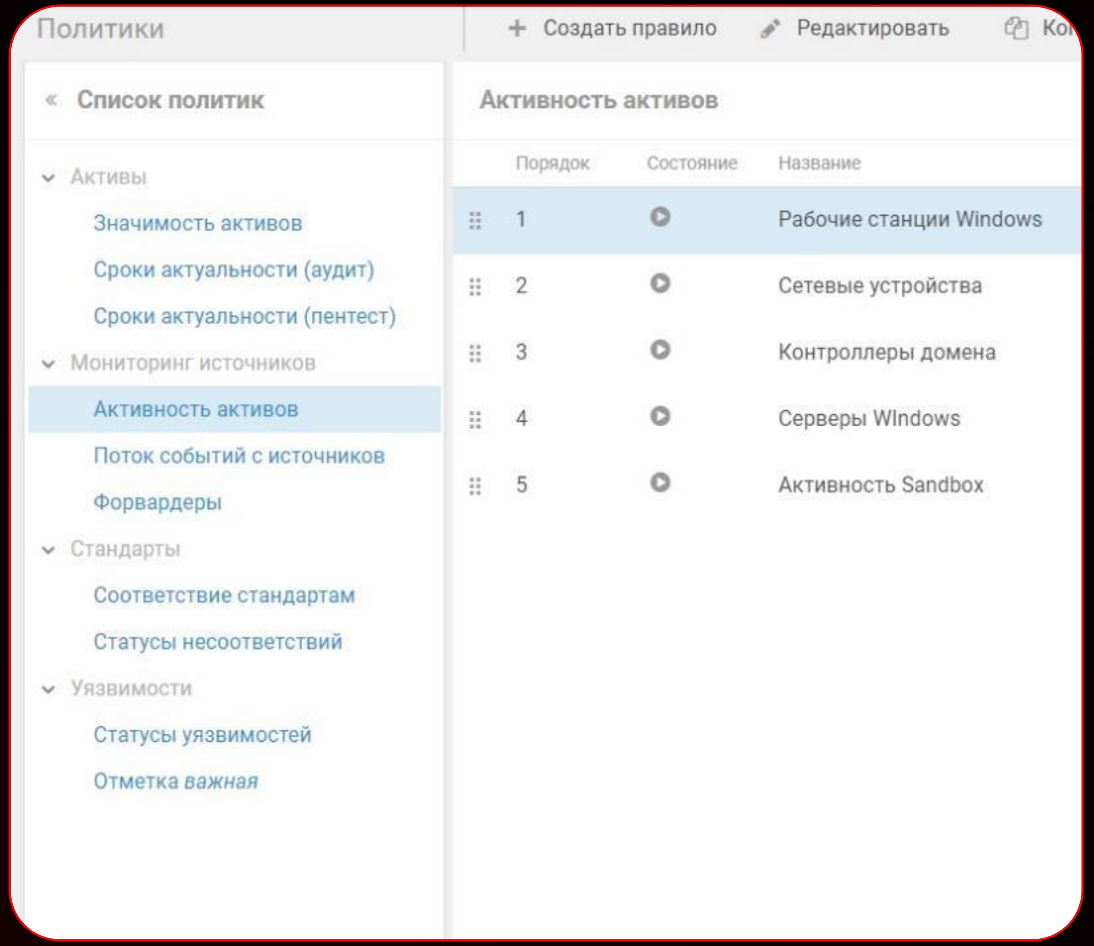


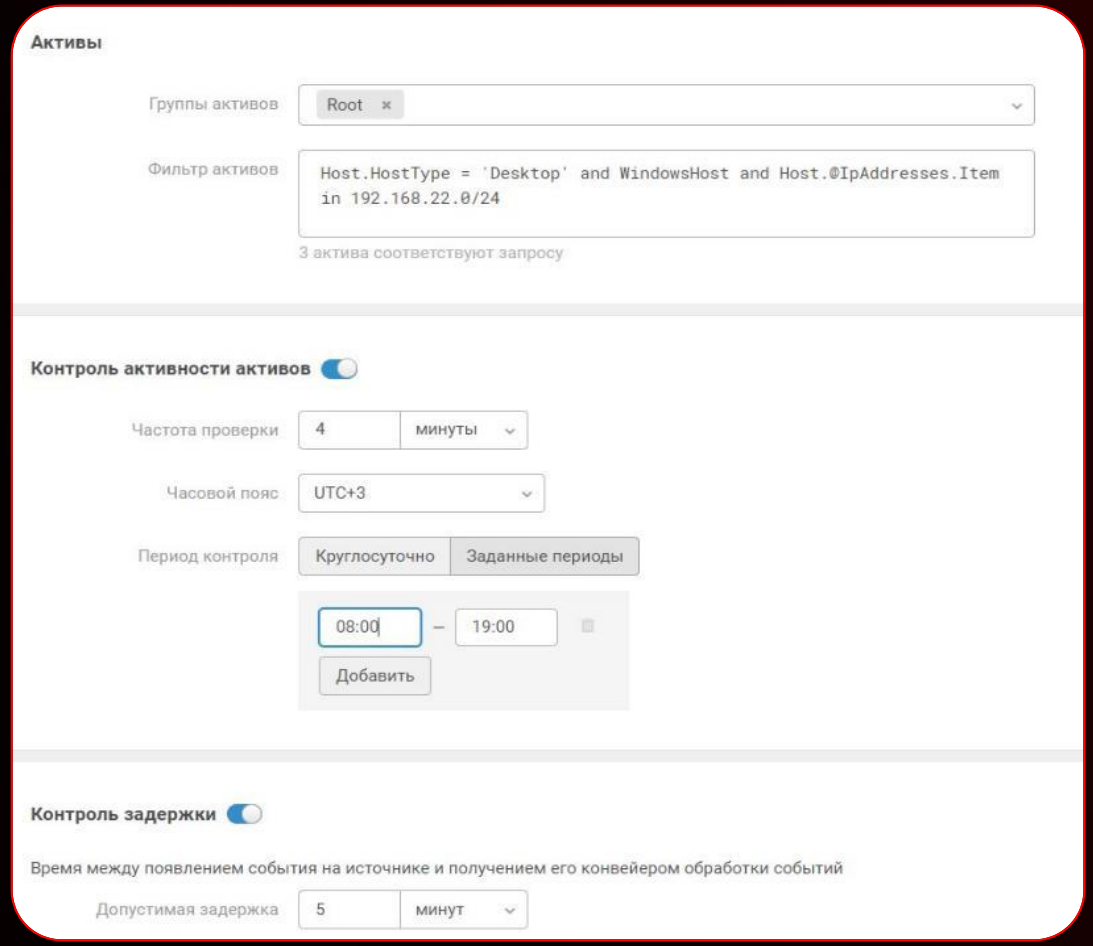
Рекомендации от PT ESC

о том, какие источники необходимо мониторить и какие требования к контролю необходимы

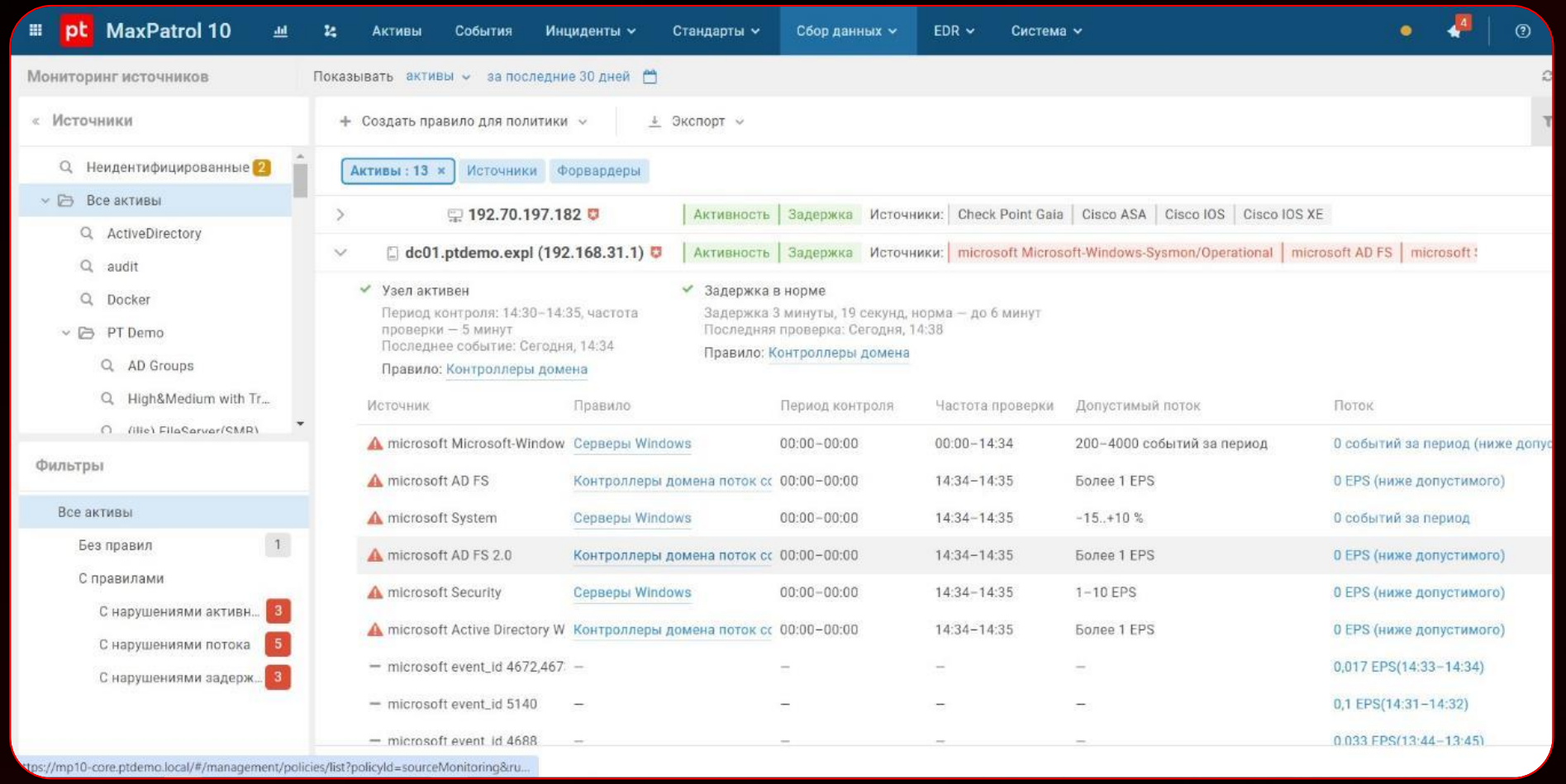
- Контроль активности источника
- Контроль потока событий (допустимый диапазон, отклонение от среднего)
- Контроль задержки
- Контроль необходимых идентификаторов в потоке событий
- Настройки уведомлений при нарушении правил политики мониторинга источников

Мониторинг источников 2.0





Мониторинг источников 2.0



04

Результативный SIEM

Что такое результативный SIEM

Цели:

1. повысить эффективность защиты от угроз с помощью MP SIEM
2. пошаговое повышение уровня зрелости SIEM
3. Видимый (ощутимый) результат работы SIEM

Критерии достижения результативного SIEM

Задать вопрос по теме выступления

habrahabr.ru/company/pt

pt@ptsecurity.com

ptsecurity.com

Спасибо