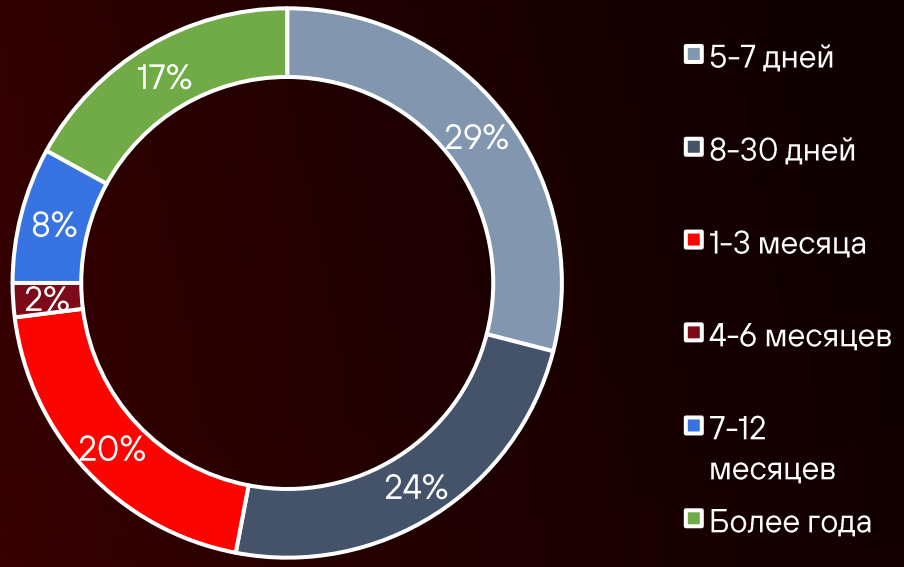
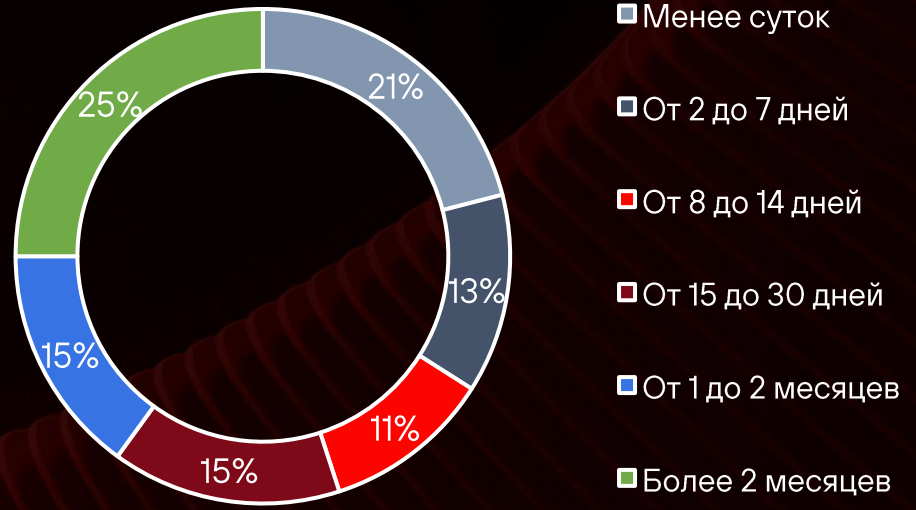

MaxPatrol SIEM
pt
MaxPatrol SIEM

Результаты расследований инцидентов

Длительность атаки

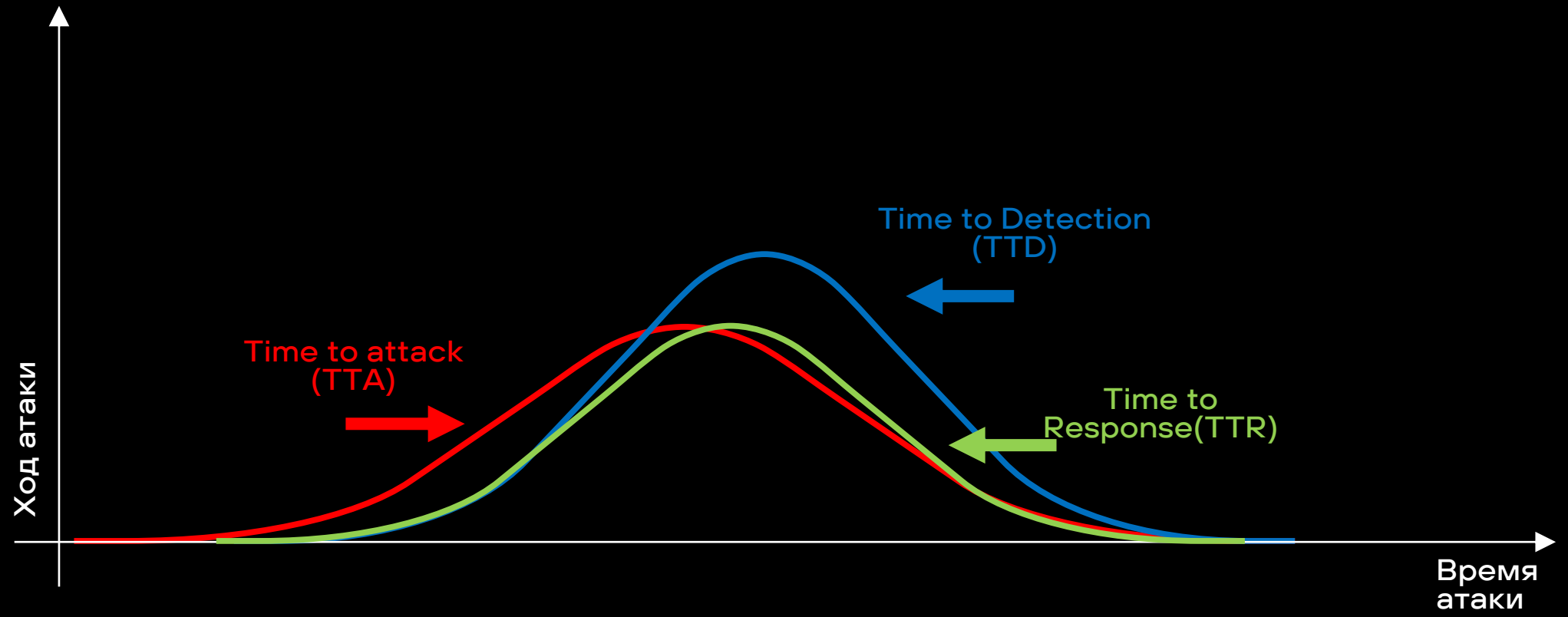


Время обнаружения с момента компрометации



Итоги проектов 2023-2024 по расследованию инцидентов и ретроспективному анализу

Как обеспечить защиту инфраструктуры?



Что предлагает MP SIEM

Полнота аудита инфраструктуры и контроля сбора событий

Качество обнаружения, в том числе целенаправленных атак

Полнота интеграций со смежными продуктами и «встройка» в процесс обеспечения ИБ

Знать, где искать

Знать, что искать

Знать, что делать дальше

Результат

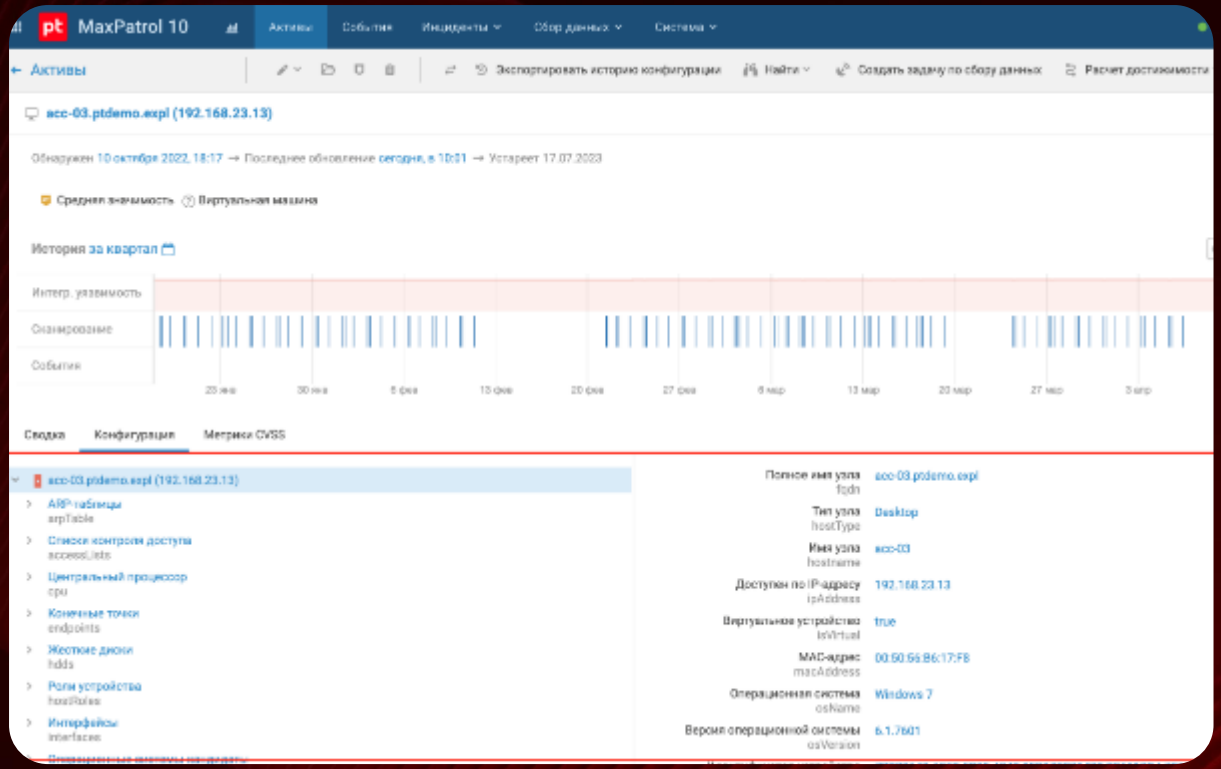
Почему активы в SIEM-системе обязательны?

- Определение контекста при обнаружении и работе с инцидентами
  критичность, роли узлов, принадлежность к периметру, пользовательские атрибуты актива
- Удобное управление доступом к событиям на базе групп активов
- Мониторинг источников – контроль полноты и качества сбора событий ИБ

Учитывает изменения в IT-инфраструктуре

- MaxPatrol SIEM идентифицирует активы не только по FQDN, MAC- и IP-адресам, но и по дополнительным параметрам, таким как тип ОС, имя сетевого узла, признаки виртуальности узла.

- Благодаря этому при изменении IP- или MAC-адреса актива он не дублируется, данные о его состоянии продолжают фиксироваться в изначально созданной карточке.



Экспертиза в MaxPatrol SIEM

Более 70 экспертов PT Expert Security Center работают над написанием контента для MaxPatrol SIEM

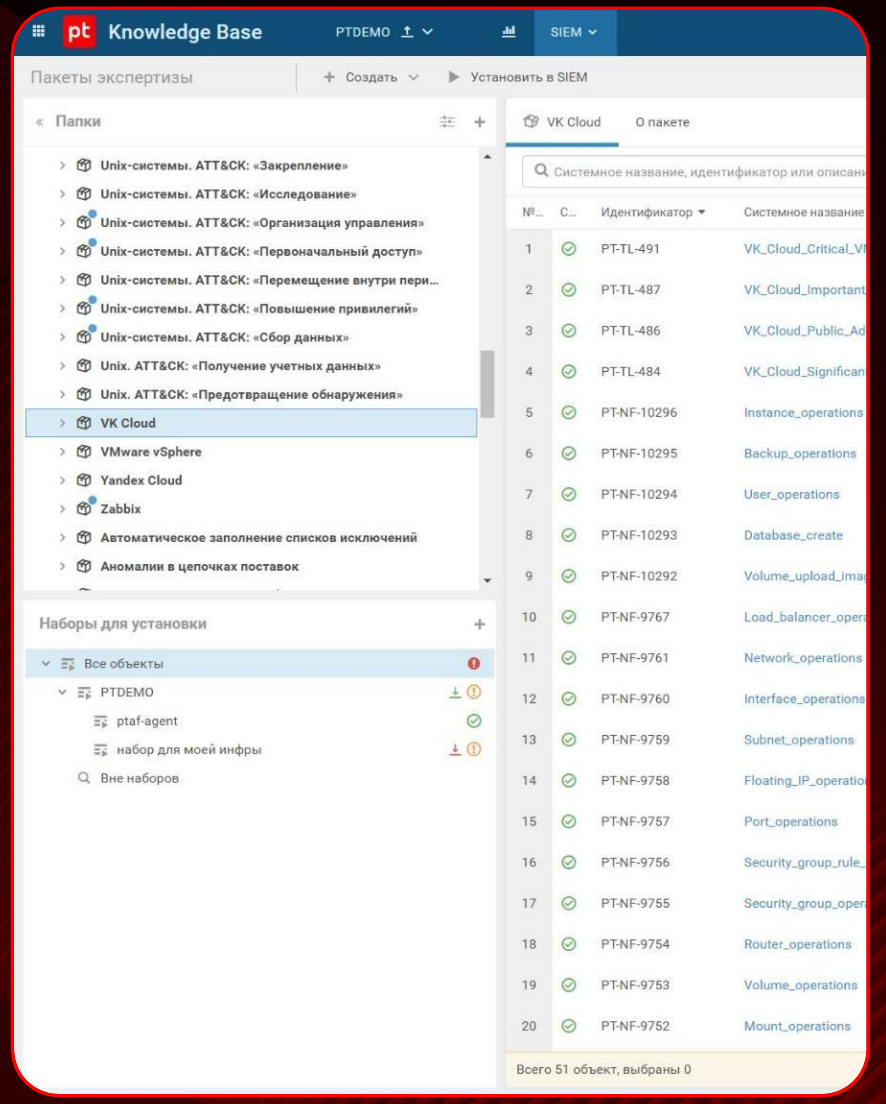
350	источников «из коробки»
126	правил обогащений
9732	правил нормализации
292	табличных списка
1769	правил корреляции
417	техник из матрицы MITRE ATT&CK покрывает экспертиза MaxPatrol SIEM «из коробки»

Данные актуальны на 10.04.2025

Новые пакеты экспертизы – два раза в месяц

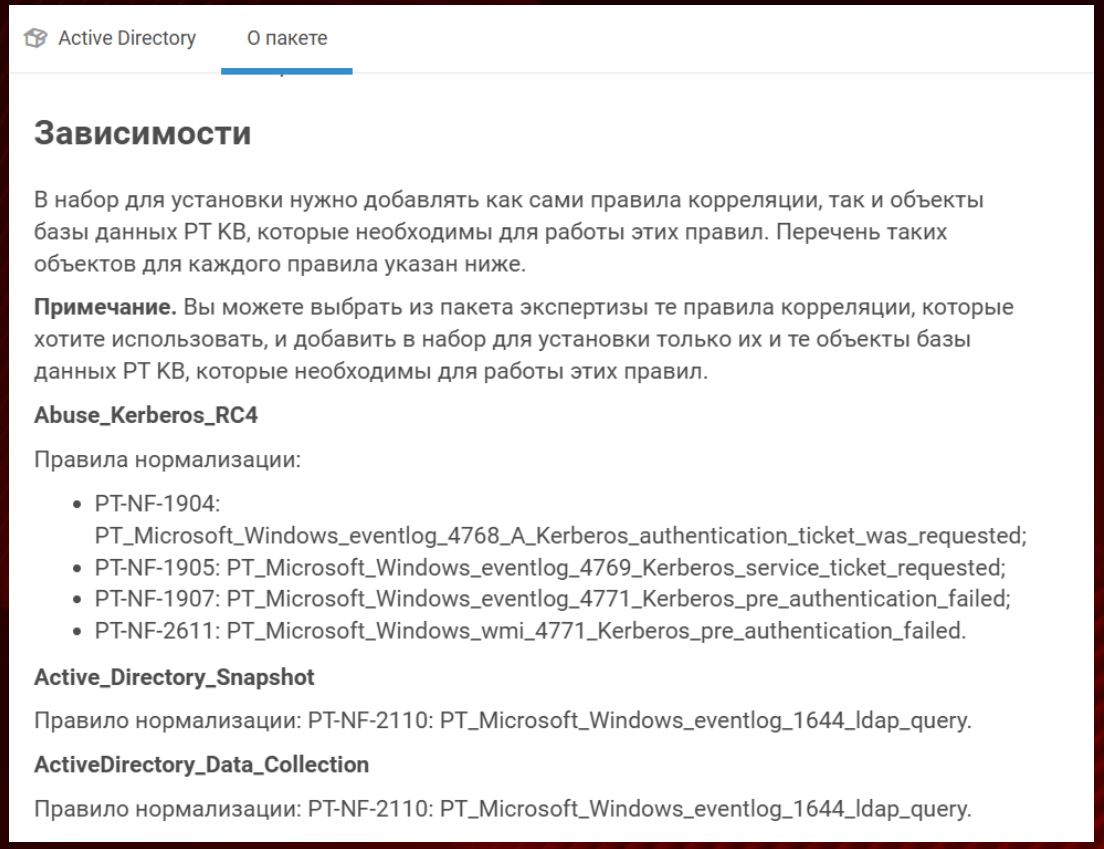
Готовые к работе правила корреляции

Правила корреляции в составе пакетов экспертизы легко настроить под особенности IT-инфраструктуры благодаря подробным инструкциям и табличным спискам исключений, часть из которых предзаполнена экспертами Positive Technologies.



Обновления в документации к пакету экспертизы

- Информация о взаимосвязях контента упрощает работу с правилами корреляции
- Категоризация активностей.
- Добавление единого гайда по настройке ОС Windows.
- Рекомендация в методологии какие пакеты экспертизы подключать в зависимости от инфраструктуры.



Пример экспертизы - Mimikatz

В пакет экспертизы входят:

- Правило корреляции
- Табличный список
- Правило нормализации
- Правило обогащение

correlation_rules | О пакете

Правило корреляции Mimikatz_Command

```
event Mimikatz_in_Commandline:
    key:
        event_src.host
    filter {
        filter::NotFromCorrelator()
        and filter::ProcessStart_Windows_any()
        and (
            regex(lower(object.process.cmdline), "\\b(privilege|crypto|sekurlsa|kerberos|lsadump|vault|token|misc|busylight|dpapi)::", 0) != null
            or regex(lower(object.process.cmdline), "\\biis::apphost\\b", 0) != null
            or regex(lower(object.process.cmdline), "\\bts::(multirdp|sessions|remote|logonpasswords)\\b", 0) != null
            or regex(lower(object.process.cmdline), "\\bnet::(alias|group|serverinfo|session|share|stats|tod|user|wsession)\\b", 0) != null
            or regex(lower(object.process.cmdline), "\\bprocess::(exports|imports|list|resume|run|start|stop|suspend)\\b", 0) != null
            or regex(lower(object.process.cmdline), "\\brpc::(close|connect|enum|server)\\b", 0) != null
            or regex(lower(object.process.cmdline), "\\bsid::(add|clear|lookup|modify|patch|query)\\b", 0) != null
            or regex(lower(object.process.cmdline), "-(dump-(credentials|hashes))\\b", 0) != null
            or regex(lower(object.process.cmdline), "(-wmimikatz|(\\blive\s+
(lsa|kerberos|smbapi|users|token|process|dpapi|smb|ldap|crypto|registry)))\\b", 0) != null
        )
        and filter::CheckWL_Process_Creation("Mimikatz_Command", lower(object.process.cmdline))
    }
```

tabular_lists | О пакете

Windows_Hacktools (справочник)

Известные утилиты для взлома ОС Windows

Идентификатор	PT-TL-200
Поставщик	Positive Technologies
Папка	Атаки с помощью специализированного ПО/tabular_lists
Наборы для установки	*не задано*
Статус валидации	
Статус установки	

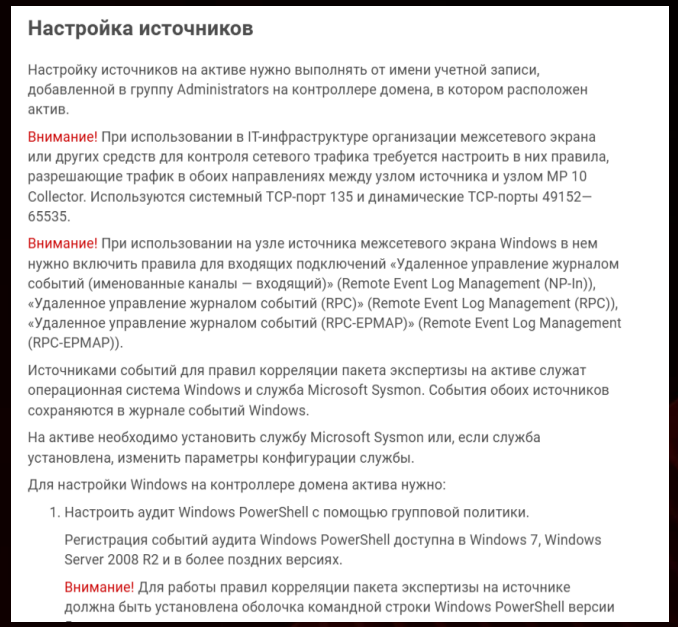
Добавить запись | Редактировать | Удалить | Активировать | Деактивировать | Импорт | Экспорт

binary_name	binary_description	commandline	hash	event_type	event_importance	event_description	Источник
gs-netcat.exe			1756b5d536035347ffb...	event	medium	Утилита для создания...	
rvb3v$v1.0.exe			79ac42b885de9e7bf59...	incident	high	Утилита для взаимоде...	
sharpefspotato.exe	\bsharpefspotato\b		239a78582fe7a8648ca...	incident	high	Утилита SharpEfsPotat...	
sweetpotato.exe	\bsharppotato\b		fdbaf19ed6f0a2d7a5da...	incident	high	Утилита SweetPotato д...	

Пример экспертизы - Mimikatz

В пакет экспертизы входят:

- Рекомендации по созданию задачи на сбор
- Как правильно установить пакет
- Как настроить источники/MP SIEM
- Помощь в расследовании



Настройка источников

Настройку источников на активе нужно выполнять от имени учетной записи, добавленной в группу Administrators на контроллере домена, в котором расположен актив.

Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом источника и узлом MP 10 Collector. Используются системный TCP-порт 135 и динамические TCP-порты 49152—65535.

Внимание! При использовании на узле источника межсетевого экрана Windows в нем нужно включить правила для входящих подключений «Удаленное управление журналом событий (именованные каналы — входящий)» (Remote Event Log Management (NP-In)), «Удаленное управление журналом событий (RPC)» (Remote Event Log Management (RPC)), «Удаленное управление журналом событий (RPC-EPMAP)» (Remote Event Log Management (RPC-EPMAP)).

Источниками событий для правил корреляции пакета экспертизы на активе служат операционная система Windows и служба Microsoft Sysmon. События обоих источников сохраняются в журнале событий Windows.

На активе необходимо установить службу Microsoft Sysmon или, если служба установлена, изменить параметры конфигурации службы.

Для настройки Windows на контроллере домена актива нужно:

1. Настроить аудит Windows PowerShell с помощью групповой политики.

   Регистрация событий аудита Windows PowerShell доступна в Windows 7, Windows Server 2008 R2 и в более поздних версиях.

   Внимание! Для работы правил корреляции пакета экспертизы на источнике должна быть установлена оболочка командной строки Windows PowerShell версии

Расследование инцидента

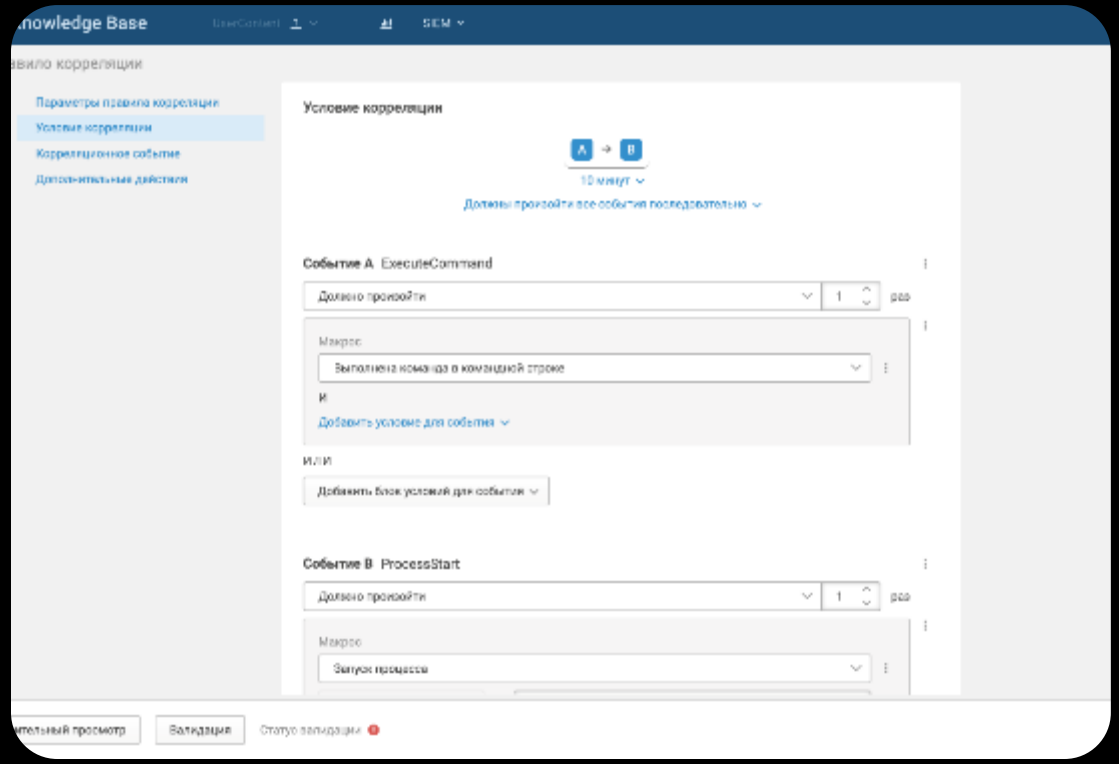
В расследовании инцидента помогает анализ связанного с ним события ИБ. По значениям полей события вы можете определить:

- `dst.ip`, `dst.fqdn` или `dst.host` — IP-адрес и полное доменное имя (FQDN) узла внутри контролируемого периметра, на который направлена атака, или узла во внешней сети, используемый злоумышленником для обмена данными (`dst.port` — порт подключения);
- `src.ip`, `src.fqdn` или `src.host` — IP-адрес и полное доменное имя (FQDN) узла, с которым связана подозрительная активность;
- `subject.account.id`, `subject.account.name`, `subject.account.domain` — идентификатор, логин и домен учетной записи, с которой связана подозрительная активность.

Помогает создавать правила корреляции

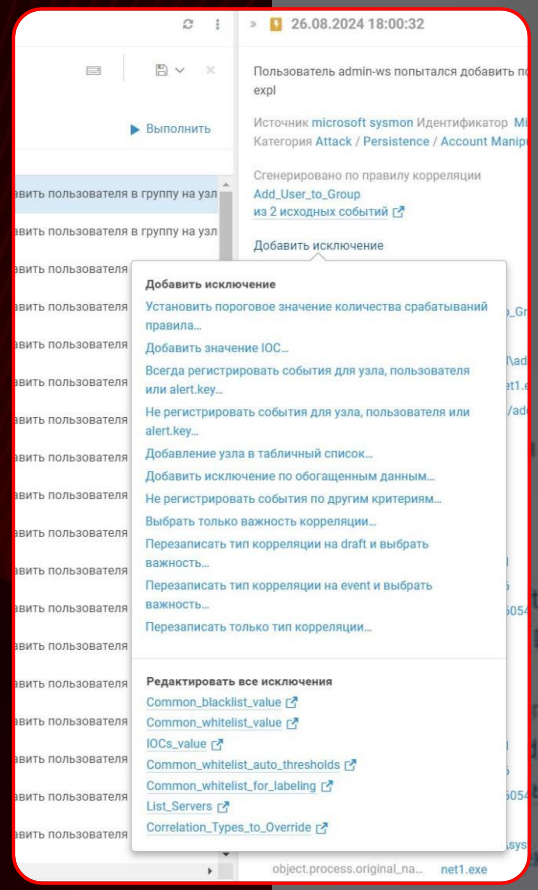
Чтобы создать собственные правила корреляции:

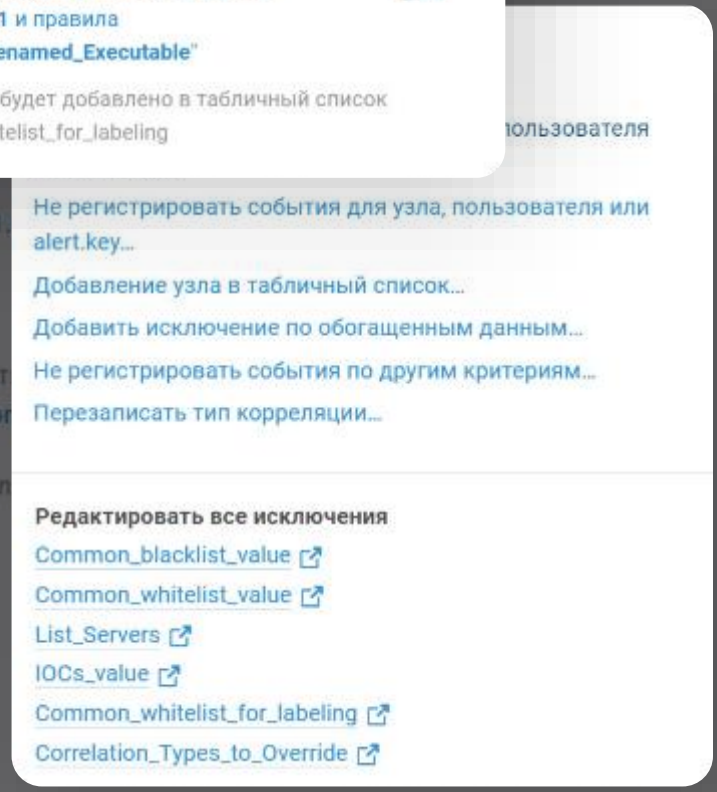
1. Выберите события, условия и подходящий макрос.
2. Настройте последовательность событий.
3. Задайте условия срабатывания.
4. Установите новые правила в MaxPatrol SIEM.



Вайтлистинг

- Пользователи MaxPatrol SIEM могут добавлять исключения для правил обнаружения угроз, чтобы предотвратить повторные ложные срабатывания.
- Достаточно отметить параметры событий, на которые правило не должно реагировать, например адрес сетевого узла или имя конкретного пользователя.
- Для создания исключений выполняется обогащение карточки события и используются данные обогащения



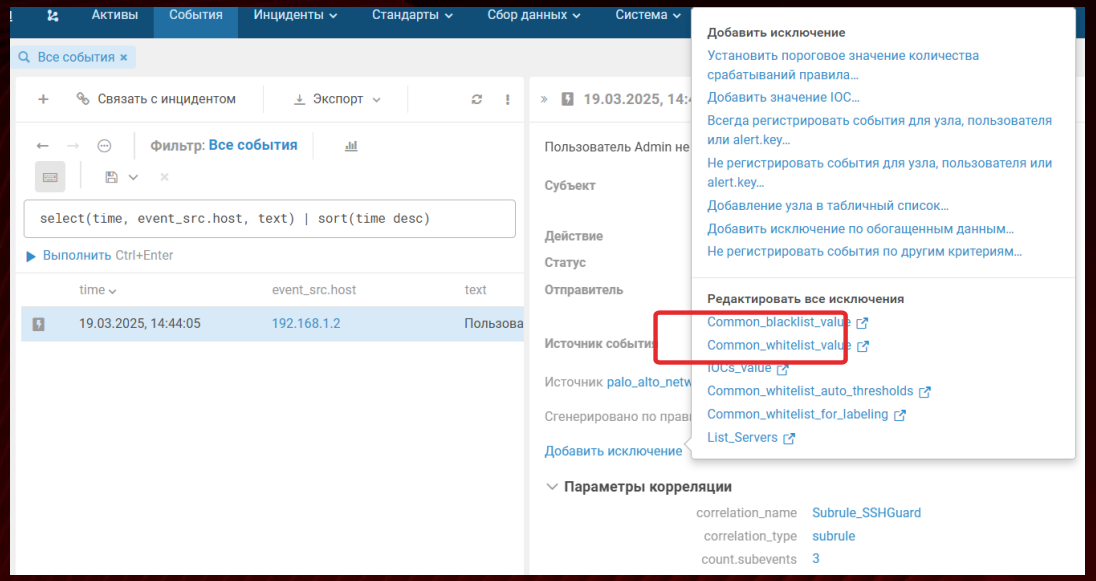


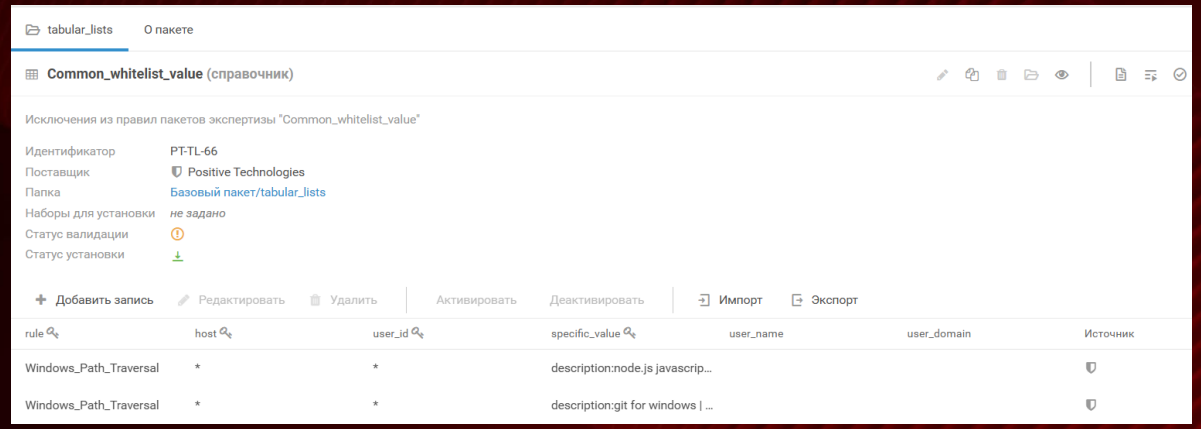
Механизмы вайтлистинга

Автоматическое заполнение белых (черных) списков исключений

Примеры таких активностей:

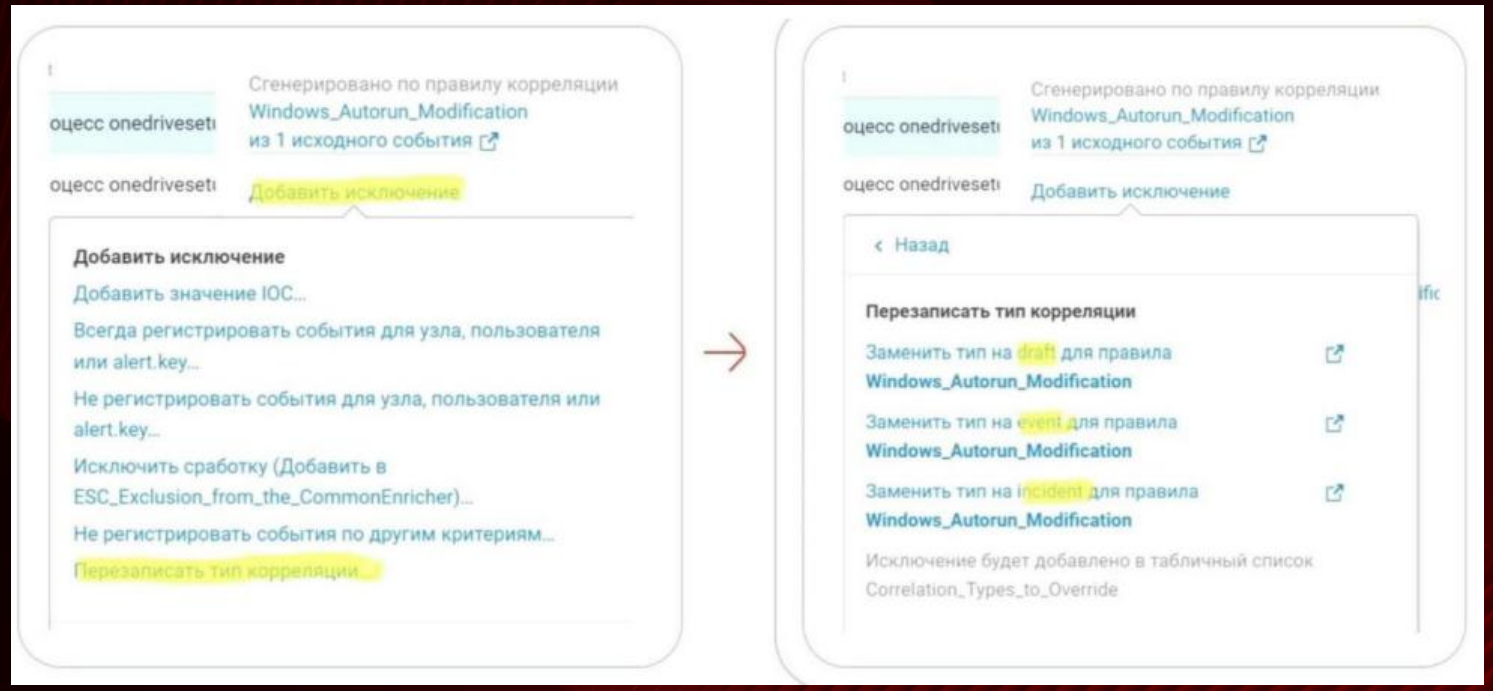
- Фоновая активность операционной системы
- Работа скриптов администрирования ИТ-инфраструктуры
- Регулярный запуск процессов (по расписанию)





Механизмы вайтлистинга

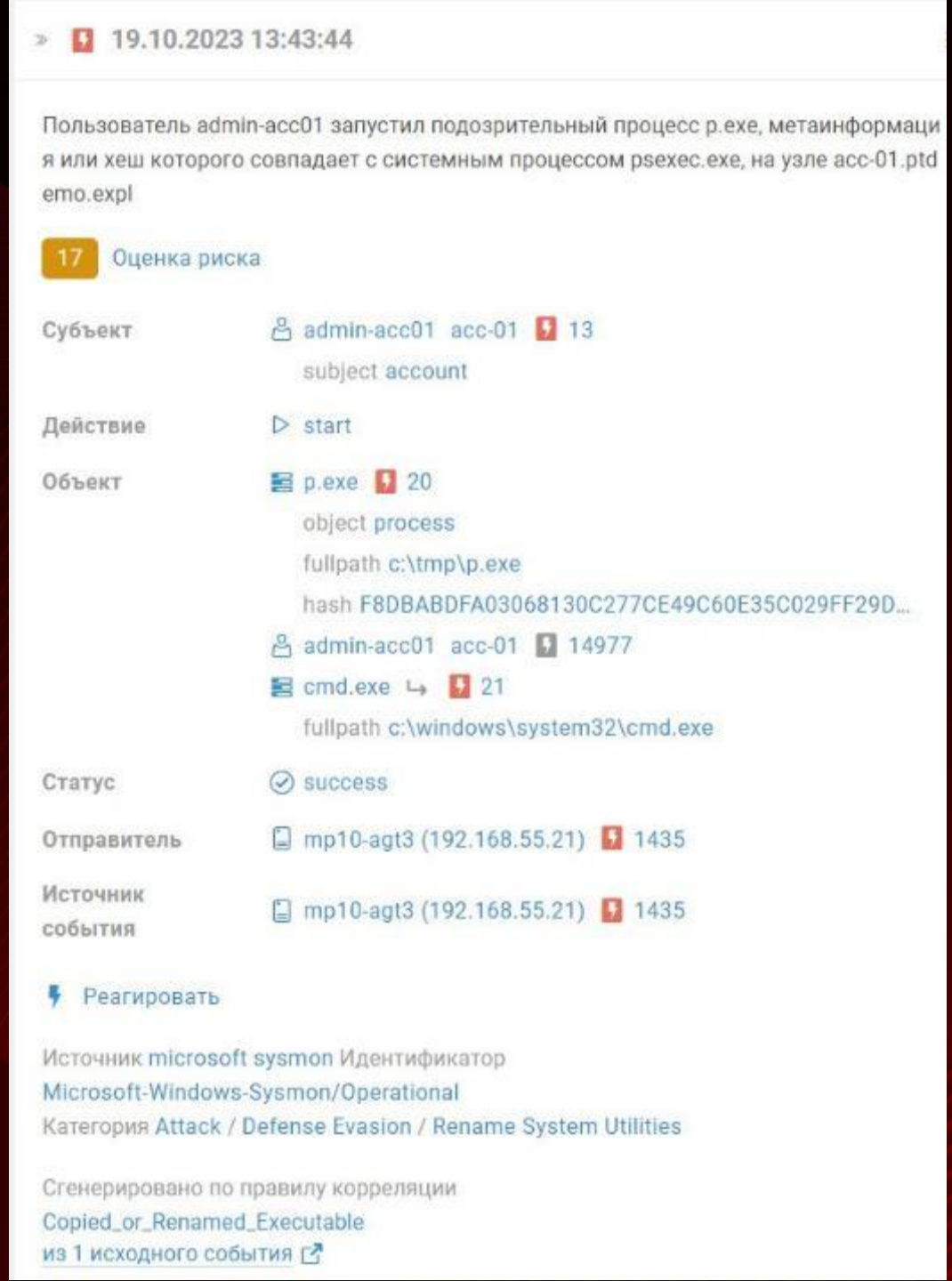
Изменение типа корреляции



Функционал расследования и реагирования

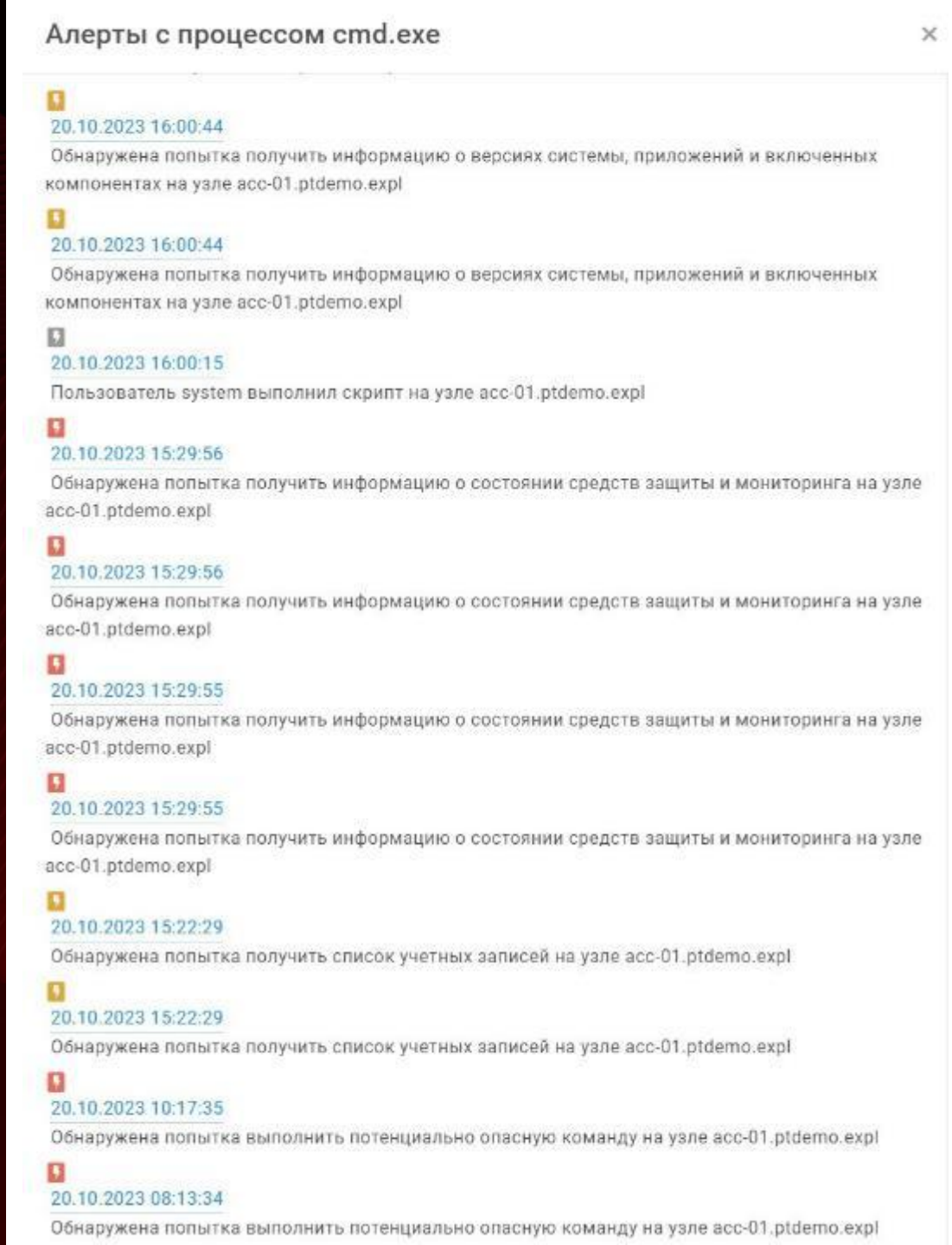
Карточка события

- Фокус на данных, обязательных для понимания контекста происходящего
- Возможность изменить карточки событий выбранных типов, чтобы сделать работу отдельных пользователей удобнее
- Контекстные экшены



Работа с деревом гипотез

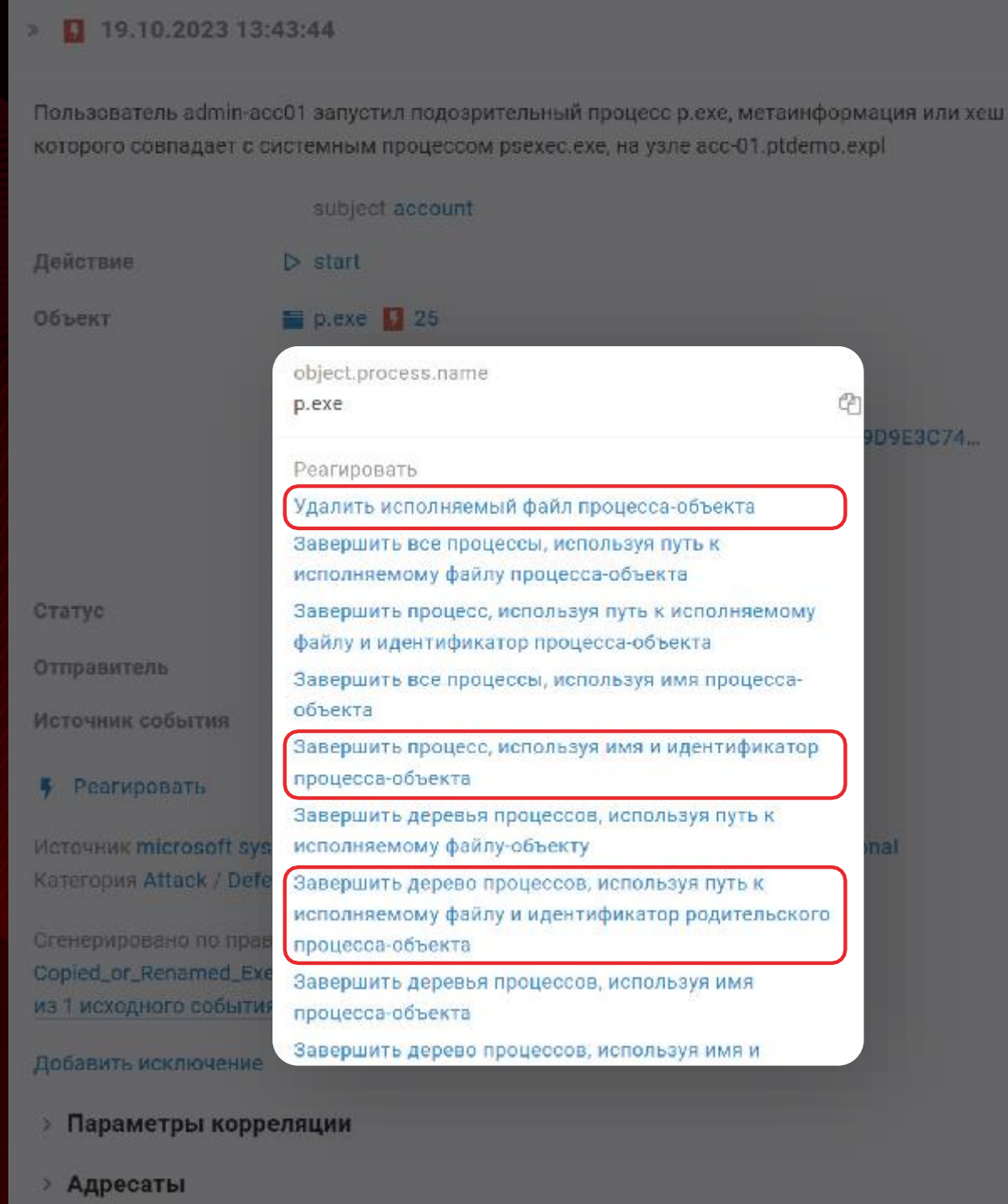
Алерты с узлами, файлами, процессами и учетными данными сгруппированы для быстрого анализа



Реагирование на инцидент

- Реагирование на инциденты на уровне узла*
- Процессы, файлы и узлы — под контролем

* С использованием агента MaxPatrol EDR и встроенной интеграции



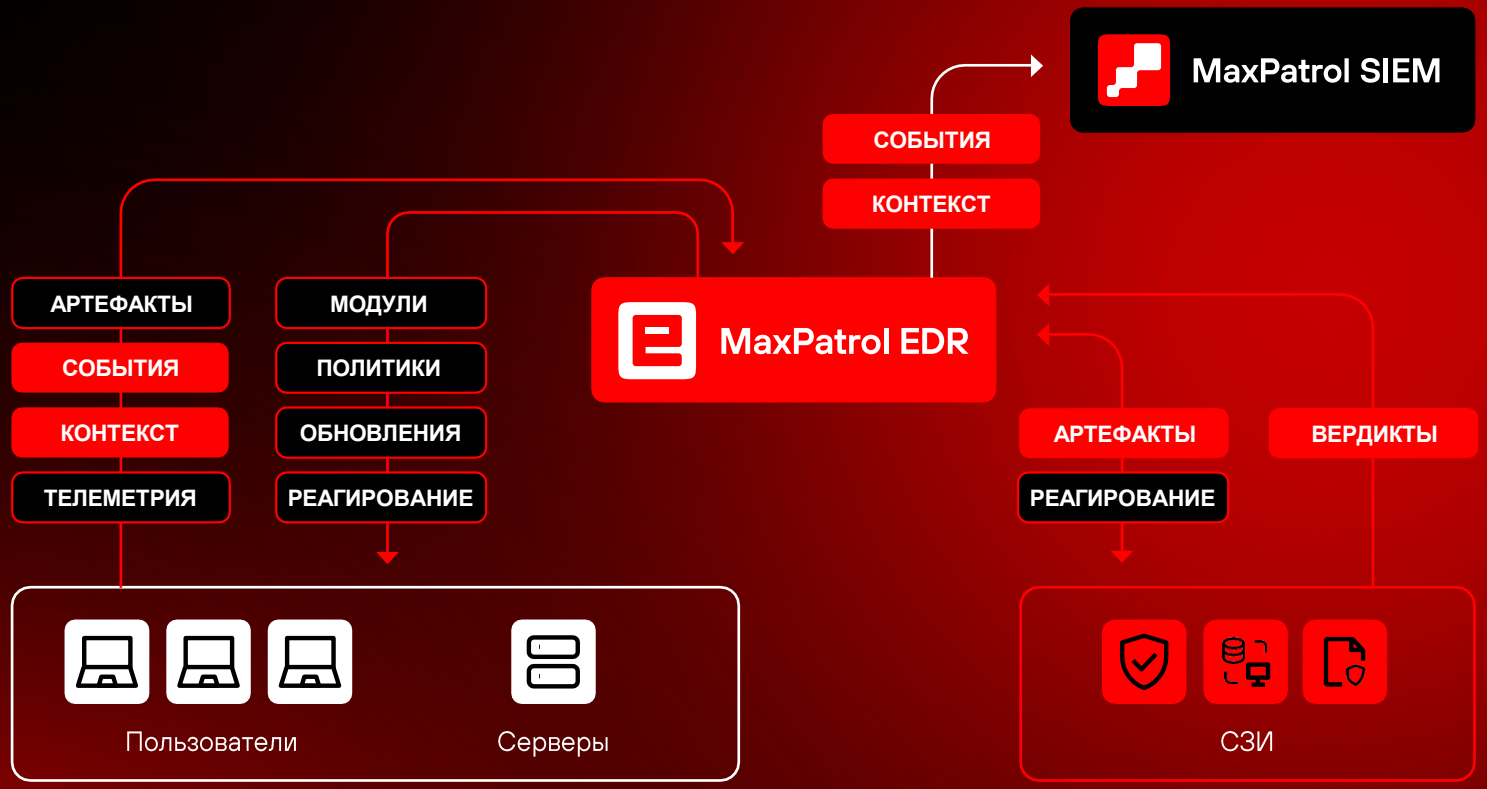
MaxPatrol EDR + MaxPatrol SIEM

Экосистема Positive Technologies

1. Дает дополнительный контекст — вне узла (для точного обнаружения)
2. Реагирование на угрозы в едином интерфейсе
3. Оптимизация архитектуры MaxPatrol SIEM

   (события собираются централизованно через серверы агентов)

- Сбор событий с устройств, не подключенных к корпоративной сети
- Возможность фильтровать события при чтении из журналов
- Управление в единой консоли



Мониторинг источников 2.0

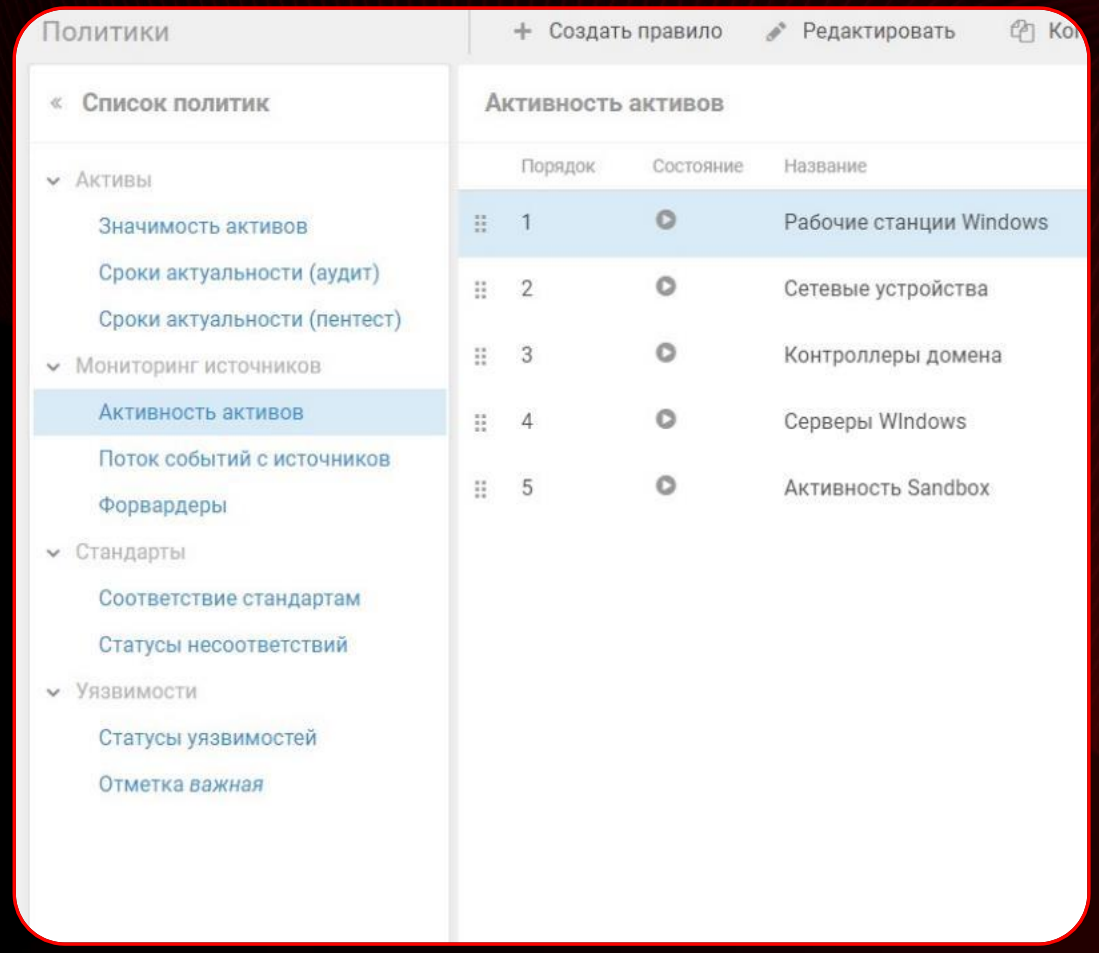
MaxPatrol SIEM не даст злоумышленнику использовать слепые зоны в мониторинге для обхода защиты

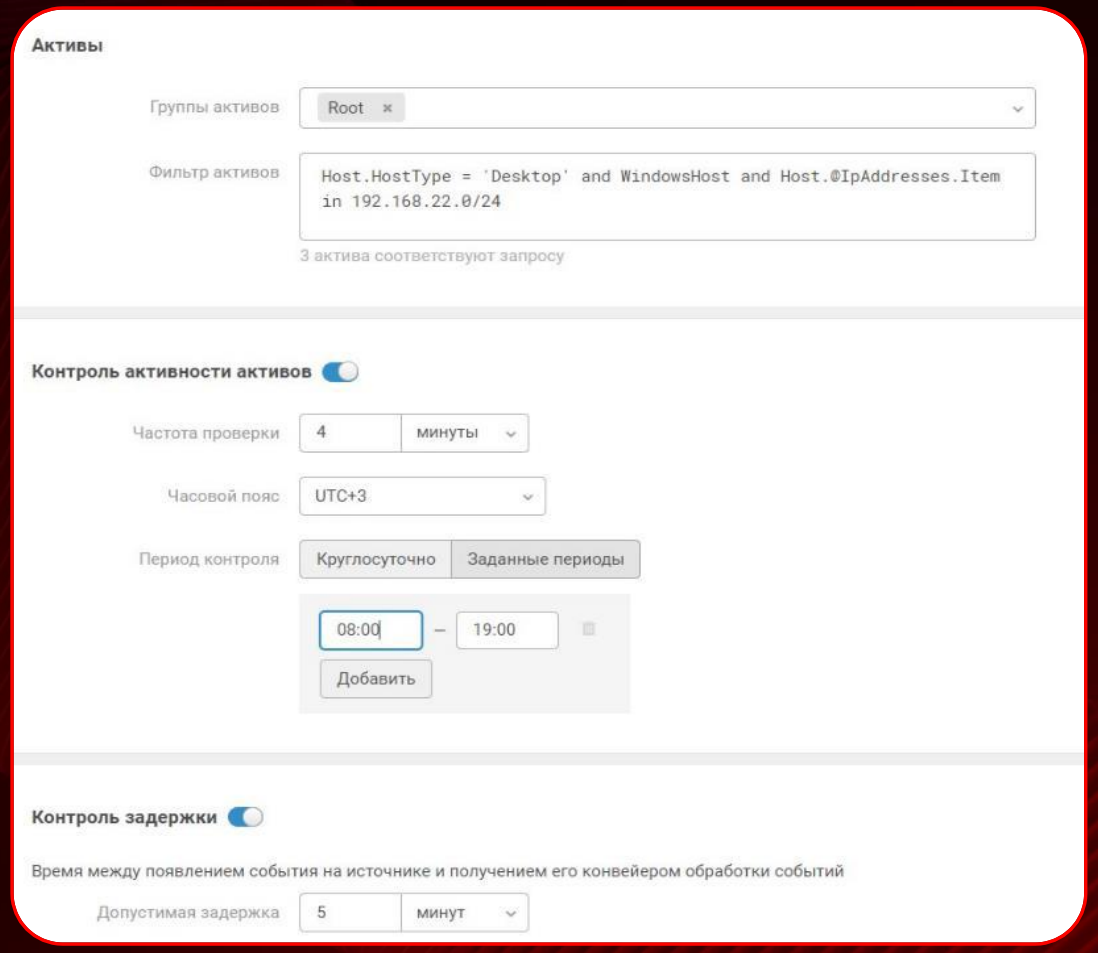
Рекомендации PT ESC

Какие источники необходимо мониторить и какие требования к контролю необходимы

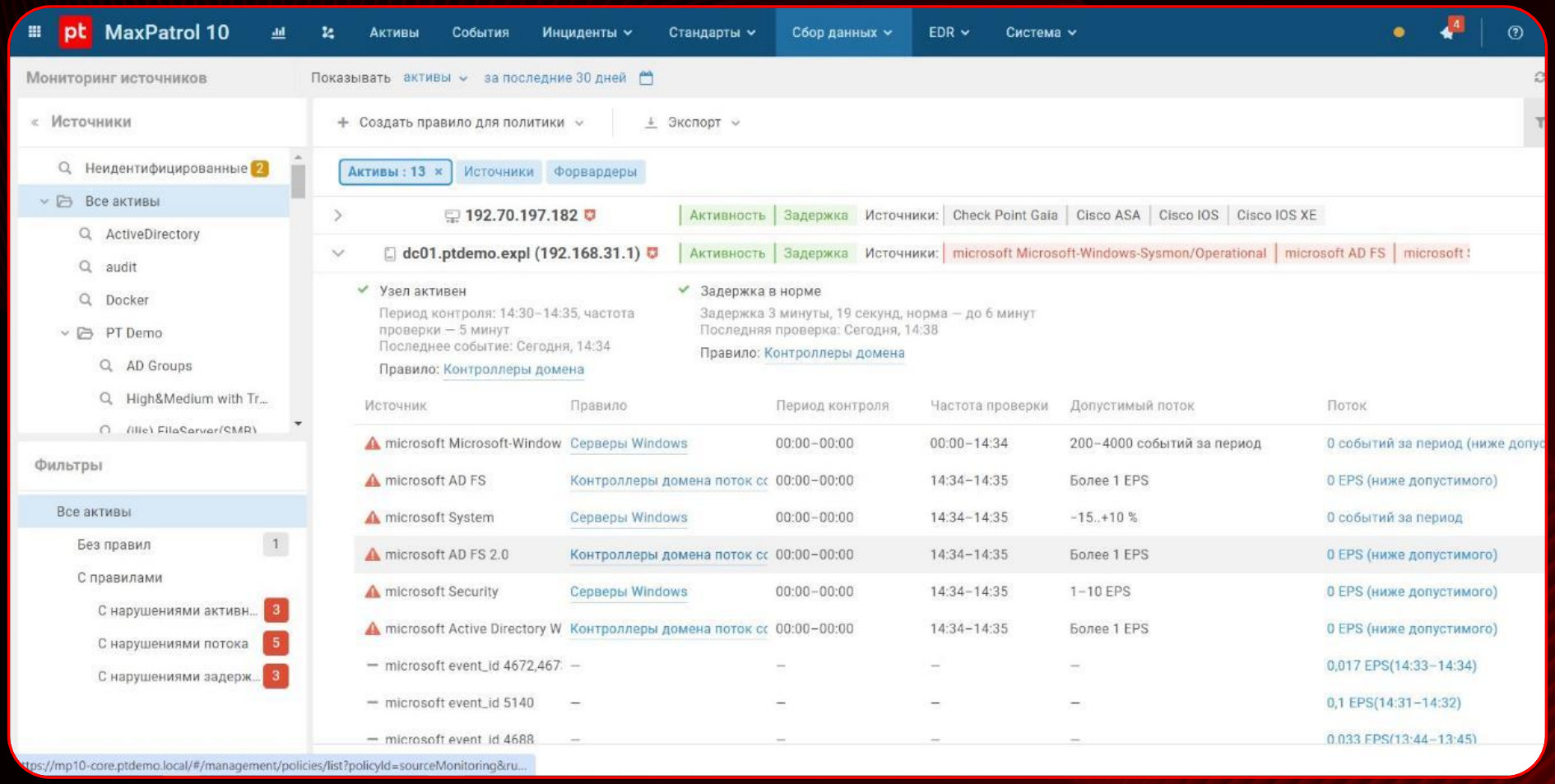
- Контроль активности источника
- Контроль потока событий (допустимый диапазон, отклонение от среднего)
- Контроль задержки
- Контроль необходимых идентификаторов в потоке событий
- Настройка автогенерации событий, связанных с нарушением проверок
- Настройка уведомлений при нарушении политики мониторинга источников

Мониторинг источников 2.0





Мониторинг источников 2.0

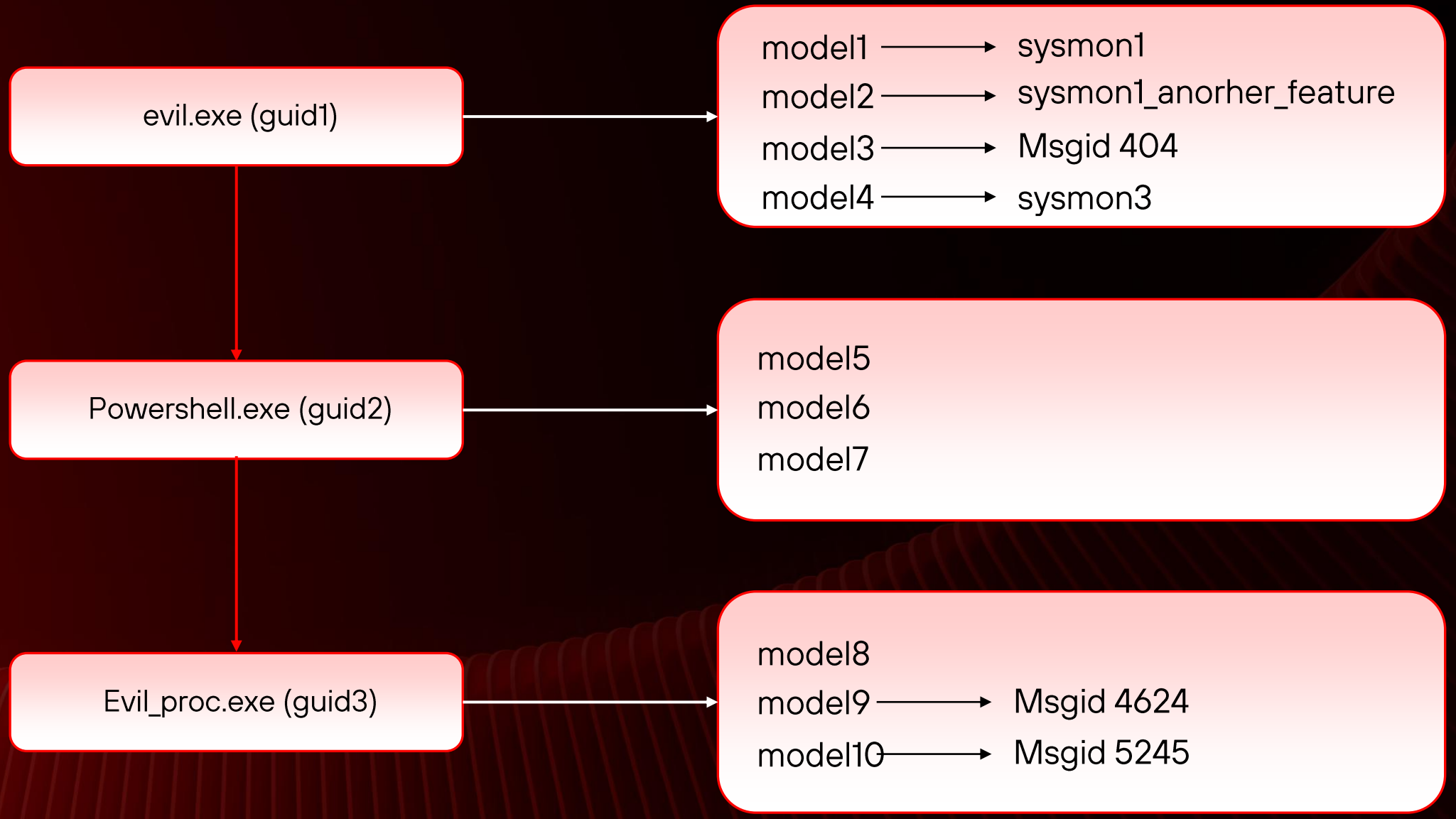


ML-модуль Behavioral Anomaly Detection (BAD) в MP SIEM

Область обнаружения угроз

Увеличиваем область обнаружения угроз

Пример работы



BAD сегодня

72

ML- модели

Выявление аномалий на базе событий из 14 типов систем

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

Данные актуальны для релиза MaxPatrol SIEM 27.3 (8.5)

ML-модуль BAD

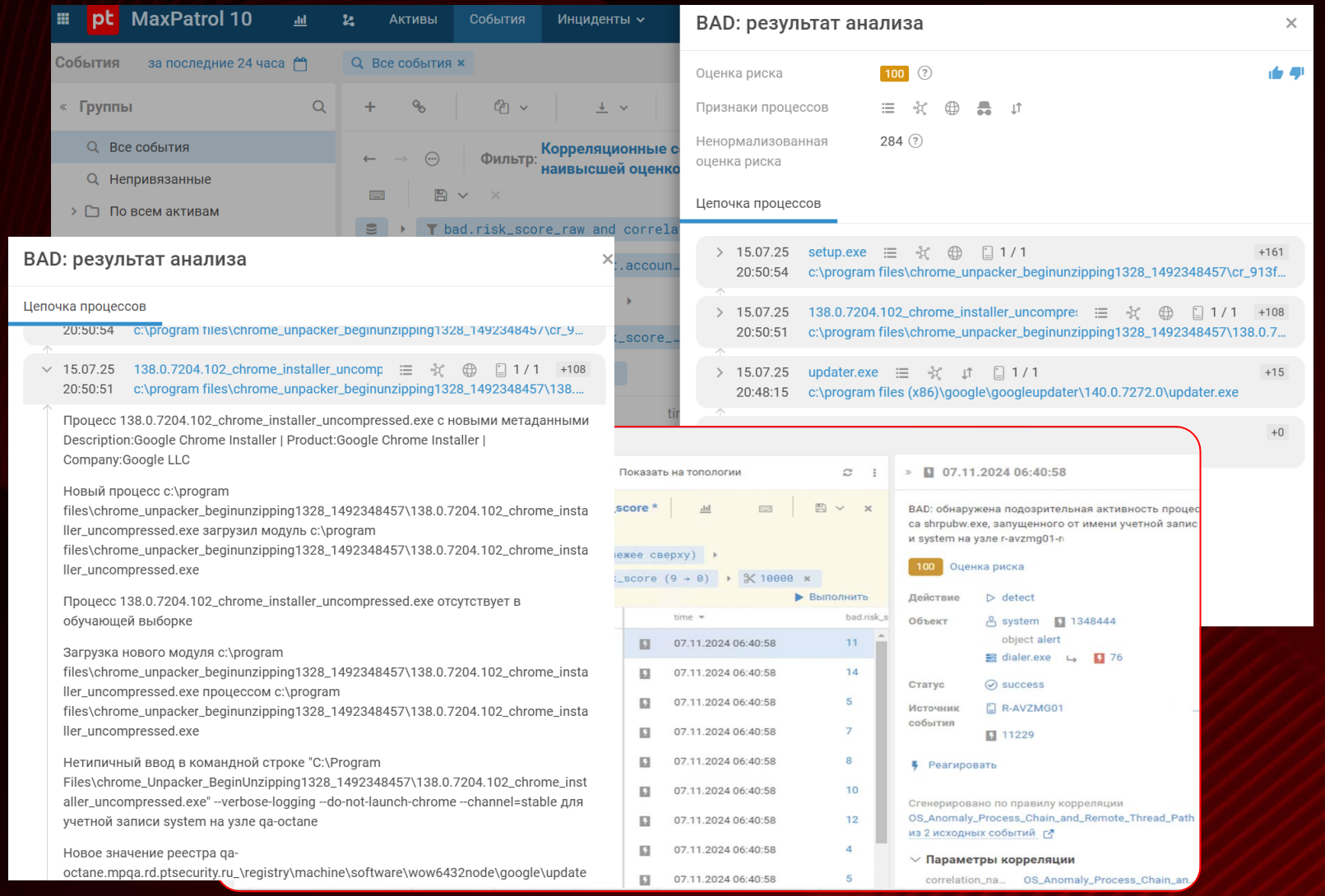
Behavioral Anomaly Detection (BAD) - высококвалифицированный помощник:

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**

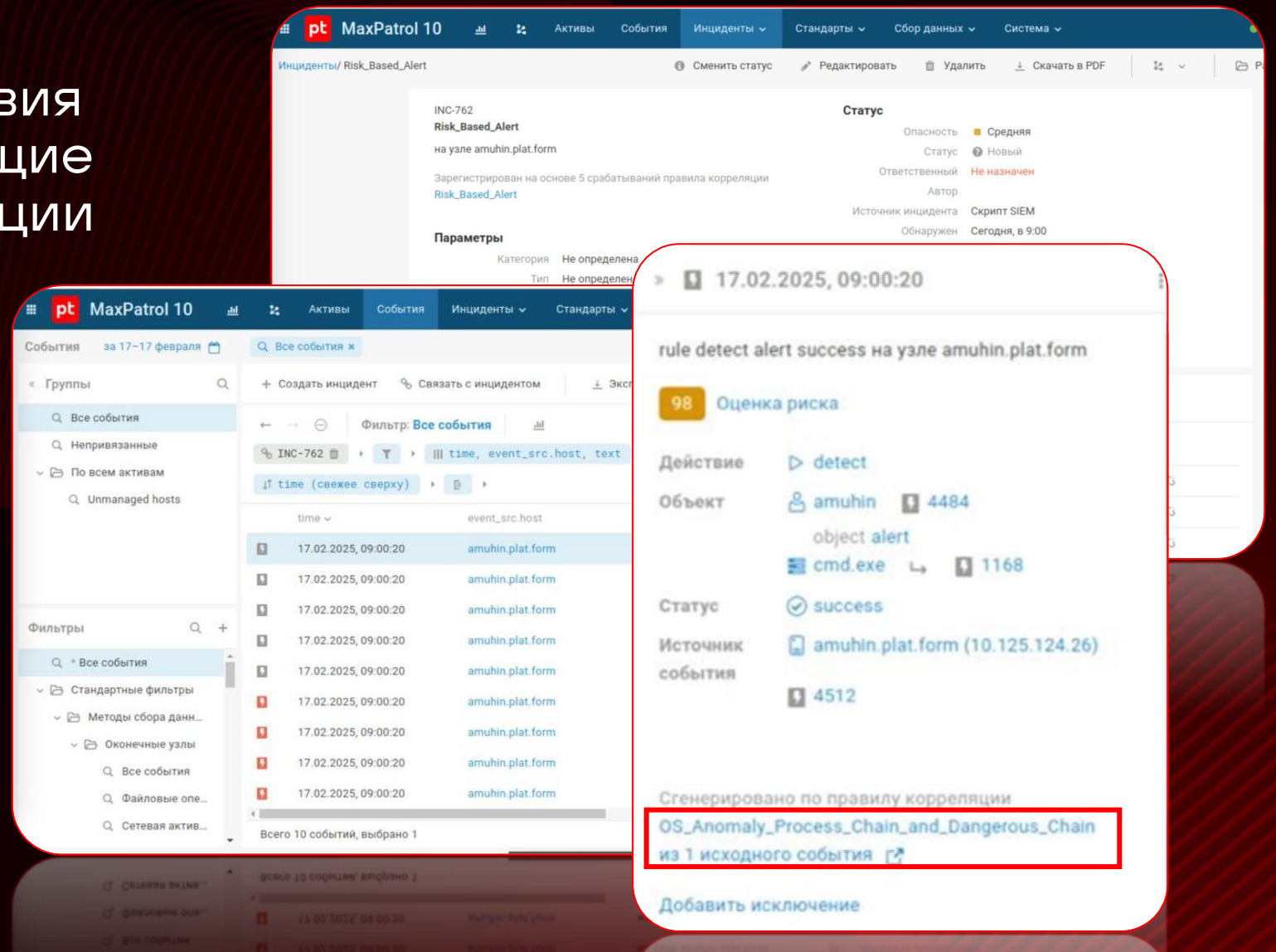
Приоритизация работы оператора

Подсвечивает приоритетные для обработки корреляционные события и дает дополнительный **контекст**



Второй эшелон защиты

Обнаруживает действия хакера, не подпадающие под правила корреляции



Преимущества

Фокус на критичных инцидентах

Снижает шум и позволяет сосредоточиться на действительно опасных событиях. Корреляция отсекает очевидное, BAD классифицирует сложное.

Видит то, что не ловит корреляция

Обнаруживает аномалии, которые невозможно поймать с помощью стандартных правил и сигнатур.
Выявляет нетипичное поведение в инфраструктуре, расширяя зону контроля за счёт поведенческого анализа.

Работает без ручной настройки

Не требует обновлений правил или постоянной ручной донастройки. автономные процессы обнаружения снижают необходимость ручного контроля. Первые релевантные результаты — через 1–2 недели (оптимально – 1 месяц)

Подстраивается под инфраструктуру

Система адаптирует логику детекта и переобучается на данных, снижая количество ложных срабатываний.

Алия Рахматуллина

Лидер продуктовой практики
MP SIEM, MP BAD, MP IM
Positive Technologies

arakhmatullina@ptsecurity.com

Спасибо!