Скоринг активов

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

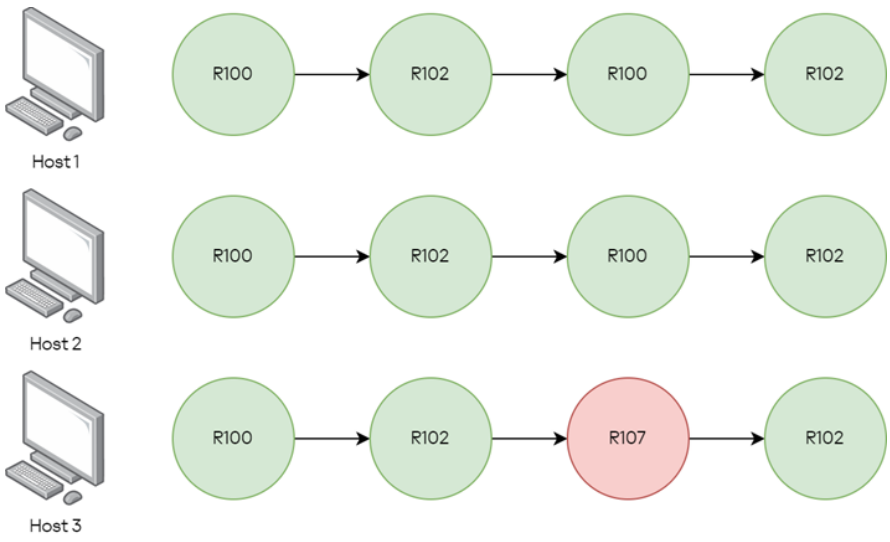
> Официальная документация по данному разделу приведена в онлайн-справке на продукт:
>
> https://support.kaspersky.ru/kuma/4.0/292782

Описание

Скоринг активов – это локальный сервис на базе машинного обучения, который обучается на сработавших правилах корреляции, анализирует типичные цепочки срабатываний в инфраструктуре и отслеживает отклонения.

Если на активе происходит нетипичная для инфраструктуры последовательность срабатываний, его рейтинг и статус повышаются, что перемещает его в более критичную категорию активов.

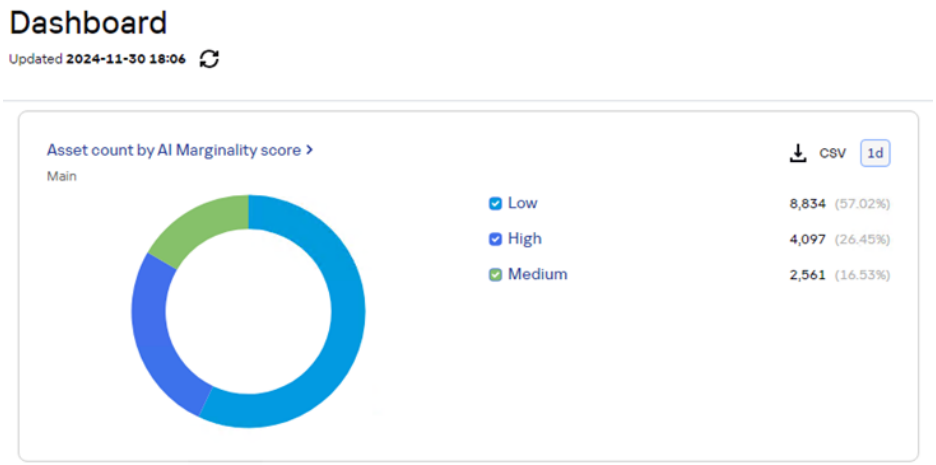
Таким образом, сервис помогает приоретизировать уже создаваемые алерты за счет анализа поведения хостов, вокруг которых эти алерты происходят. Кроме того, аналитик можно самостоятельно выбрать активы с высоким статусом аномальной активности и проанализировать события для поиска потенциальных угроз.



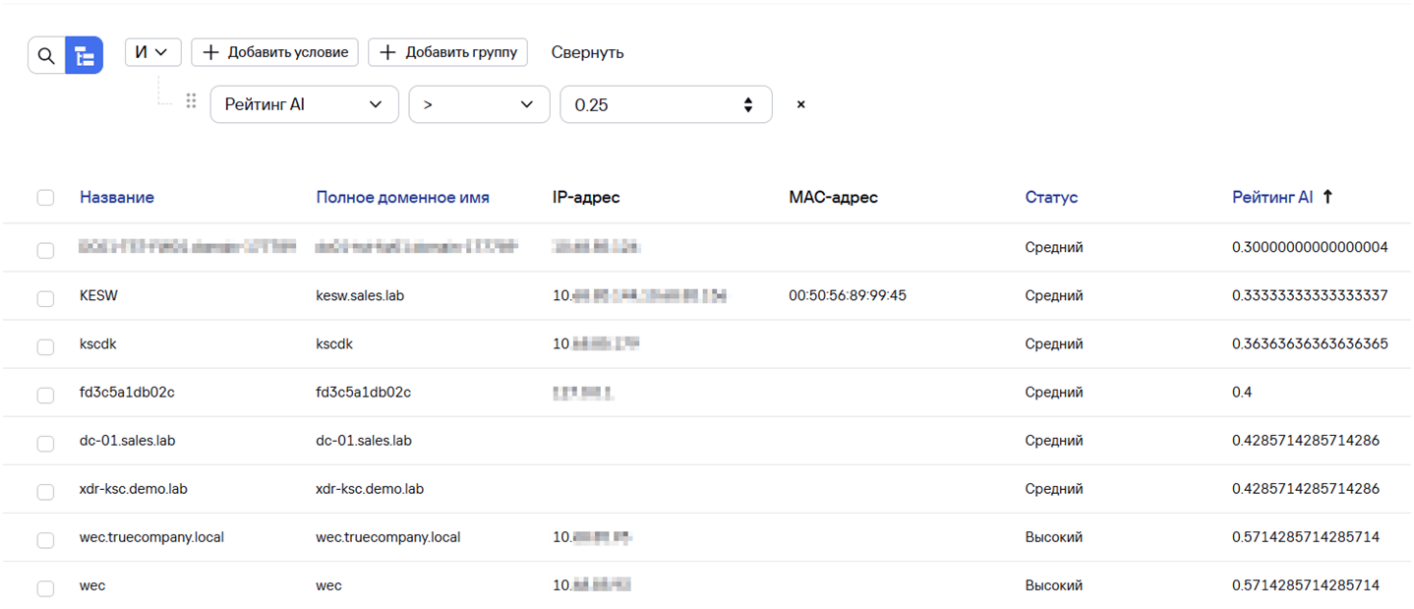
Сервис **Скоринг активов** получает из доступных кластеров хранения корреляционные

события, содержащие непустое поле Affected assets, выстраивает ожидаемую последовательность событий и обучает модель AI. На основании цепочки срабатываний корреляционных правил AI-сервис высчитывает, является ли такая последовательность срабатываний характерной в этой инфраструктуре. Нехарактерные паттерны повышают рейтинг актива.

По результатам расчетов сервиса **Скоринг активов** в карточке активов становится доступным для просмотра поле **AI-рейтинг** и **AI-Статус**. Рейтинг – это число, которое отражает степень нетипичной активности на активе, на которую стоит обратить внимание. Доступные значения поля **AI-Статус**: Low, Medium, High, Critical.



После каждого перезапуска сервиса **Скоринг активов**, сервис заново обучает модель и выполняет переоценку рейтинга активов, указанных в событиях за сегодня. Активы со скорингом выглядят следующим образом:



Название	Полное доменное имя	IP-адрес	MAC-адрес	Статус	Рейтинг AI
[redacted]	[redacted]	[redacted]		Средний	0.30000000000000004
KESW	kesw.sales.lab	10.[redacted]	00:50:56:89:99:45	Средний	0.33333333333333337
kscdk	kscdk	10.[redacted]		Средний	0.36363636363636365
fd3c5a1db02c	fd3c5a1db02c	[redacted]		Средний	0.4
dc-01.sales.lab	dc-01.sales.lab			Средний	0.4285714285714286
xdr-ksc.demo.lab	xdr-ksc.demo.lab			Средний	0.4285714285714286
wec.truecompany.local	wec.truecompany.local	10.[redacted]		Высокий	0.5714285714285714
wec	wec	10.[redacted]		Высокий	0.5714285714285714

В директории, указанной в конфигурационном файле, хранятся события, которые сервиса **Скоринг активов** получил из кластеров хранения KUMA за указанное количество дней. Например, если в конфигурационном файле указано 12 дней (period_for_train_days), сервис будет получать события за последние 12 дней. Самые давние события удаляются из

директории. В этой же директории будет храниться обученная модель.

Переобучение модели происходит в полночь по UTC. Переоценка рейтинга активов происходит раз в час для всех активов, которые были в событиях за сегодня по UTC.

Если лицензию удалить, поля **AI-рейтинг** и **AI-Статус** будут скрыты из карточки актива. Если лицензию снова добавить, значения полей **AI-рейтинг** и **AI-Статус** снова будут отображаться.

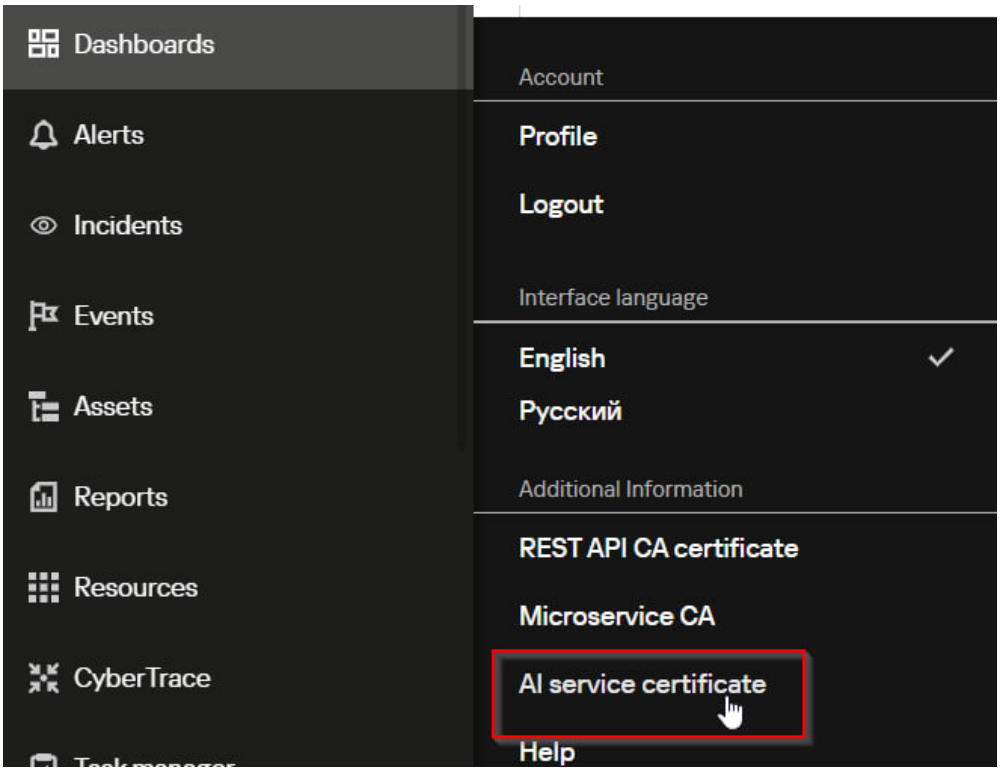
Журналы сервиса хранятся в `/var/log/syslog.`

Требуемые аппаратные ресурсы

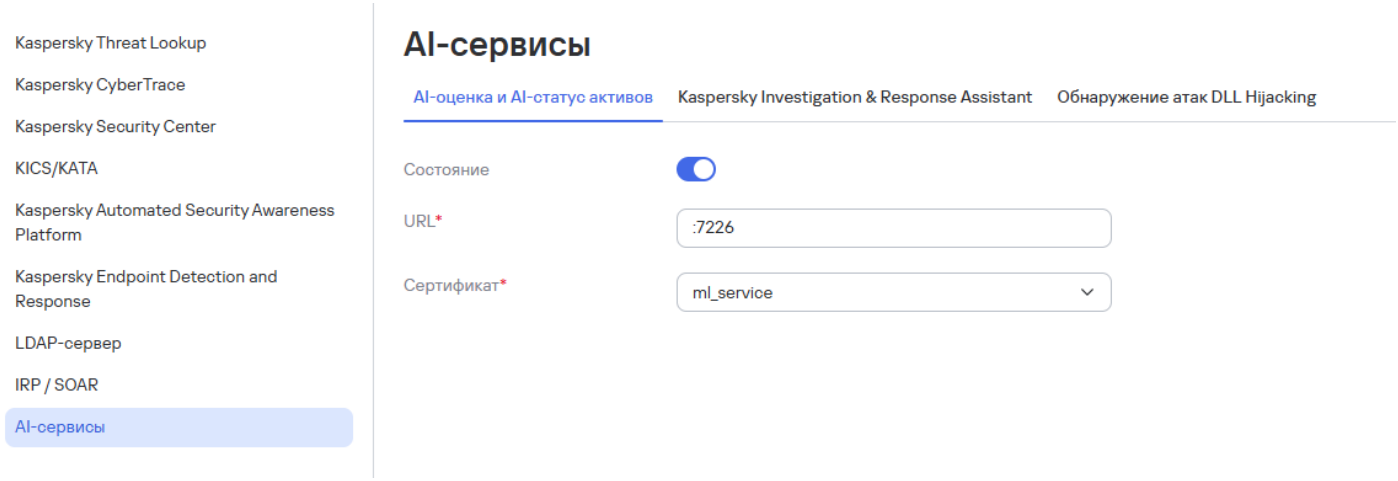
4 vCPU, 12 GB RAM, 100 GB HDD

Шаги по установке

- Скачайте архив: **ссылка**. Архив содержит скрипты для установки и удаления сервиса, а также конфигурационный файл `config.yaml`.
- В конфигурационном файле `config.yaml` укажите порт, по которому сервис Ядра будет ожидать подключения от сервиса Скоринг активов. Например, в установке в отказоустойчивой конфигурации должен быть указан порт 7226. Для остальных параметров можно оставить значения по умолчанию.
- В веб-интерфейсе KUMA скачайте **AI service certificate** (в меню пользователя) и поместите его в `roles/mlservice/files`.



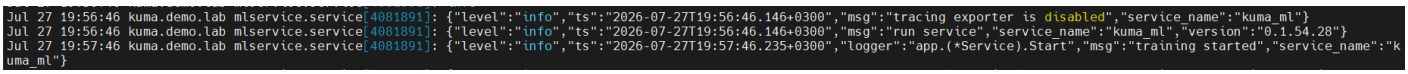
- Перейдите в директорию с файлами сервиса и из этой папки выполните команду: `bash ./install <путь к ИНВЕНТОРИ.yaml>`
- По умолчанию сервис устанавливается на хост с Ядром. Если вы хотите установить сервис на другой хост, укажите в конфигурационном файле `<hostname>:<port>` ядра KUMA в `kuma_address` и убедитесь в наличии сетевого доступа.
- Установщик генерирует необходимые сертификат и ключ в процессе установки и помещает их в директории, указанные в конфигурационном файле, по умолчанию: `/opt/kaspersky/mlservice/`. Сертификат необходимо загрузить в KUMA. В веб-интерфейсе KUMA в разделе (появляется при наличии лицензии AI) **Параметры – Интеграции → AI-сервис** во вкладке **AI рейтинг и статус активов** заполните следующие поля:
  - В поле **URL** укажите **адрес и номер порта**, по которому Ядро будет ожидать подключения от AI-сервиса. Например, **:7226** (означает поднять порт на ядре 0.0.0.0:7226). Номер порта должен соответствовать указанному в конфигурационном файле.
  - В поле **Сертификат** в раскрывающемся списке выберите Создать и в открывшемся окне Создание сертификата укажите тип сертификата Certificate и загрузите сертификат из директории, указанной в конфигурационном файле, по умолчанию `/opt/kaspersky/mlservice/service.crt`.



Сразу после установки сервис будет пытаться в течение 15 минут подключиться к KUMA с интервалом в 1 минуту. Если сертификат не добавлен в веб-интерфейсе KUMA, подключение не будет выполнено и сервис остановится. В таком случае можно добавить сертификат и перезапустить сервис (`systemctl restart mlservice.service`), сервис Скоринг активов опять попробует подключиться к Ядру KUMA.

Сервис Скоринг активов установлен.

Для проверки, что Скоринг активов успешно запущен выполните команду `systemctl status mlservice` и проверьте наличие строки старта обучения модели (msg: "training started").



Use Case 1. Приоритизация алертов

В KUMA можно настроить проактивную категоризацию активов на основании значений полей «**AI-рейтинг**» и «**AI-статус**». Как только **ИИ-сервис «Скоринг активов»** присвоит активу рейтинг и статус, актив будет перемещен в категорию, соответствующую данному уровню нетипичной активности.

Уровень важности категории актива влияет на уровень важности алерта, с которым связан этот актив. Таким образом, итоговый уровень важности алерта будет выше, если на активе фиксируется аномально высокий уровень нетипичной активности и актив помещен в соответствующую категорию.

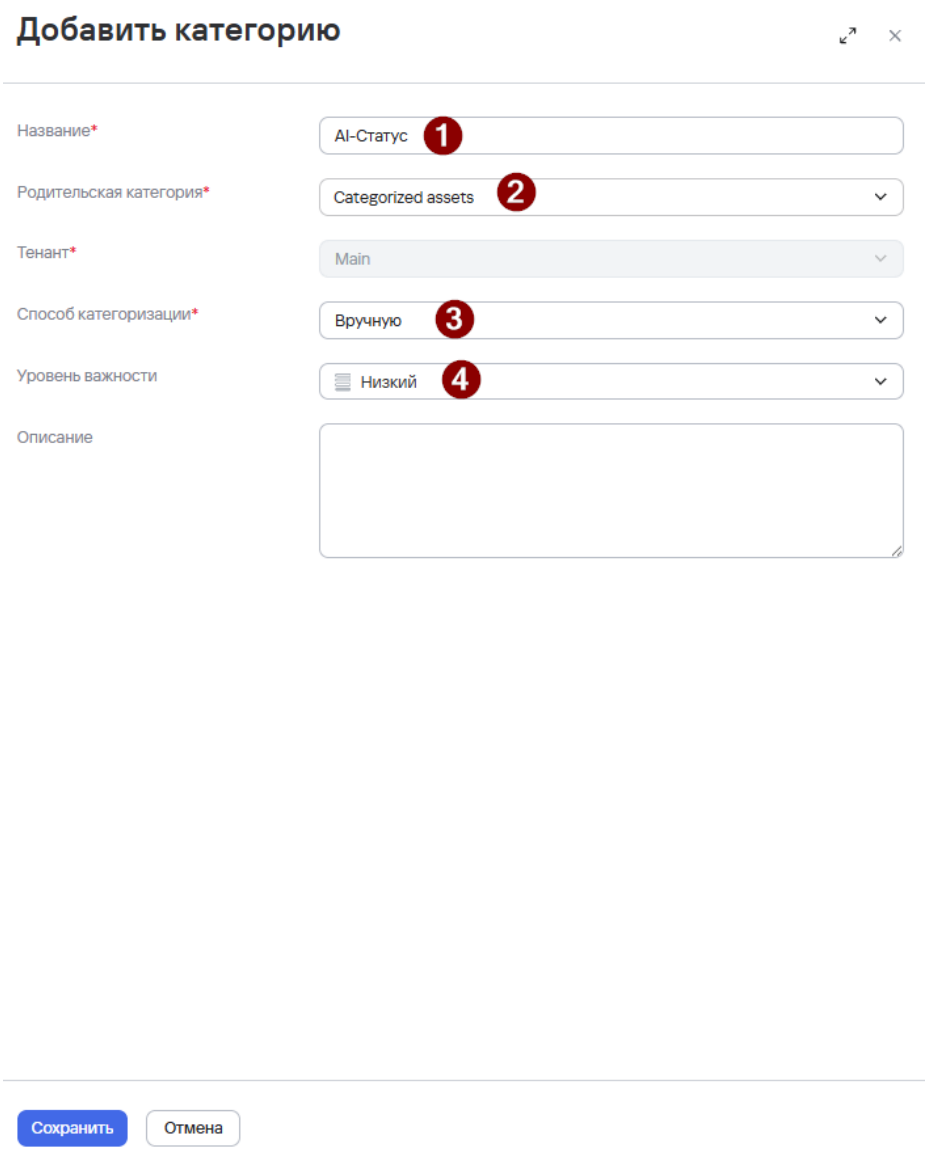
> По умолчанию уровень важности алерта определяется сработавшим правилом корреляции.

Благодаря скорингу активов выполняется автоматическая приоритизация: алерты, связанные с активами с повышенным уровнем нетипичной активности, получают более высокий уровень важности и должны обрабатываться аналитиками в приоритетном

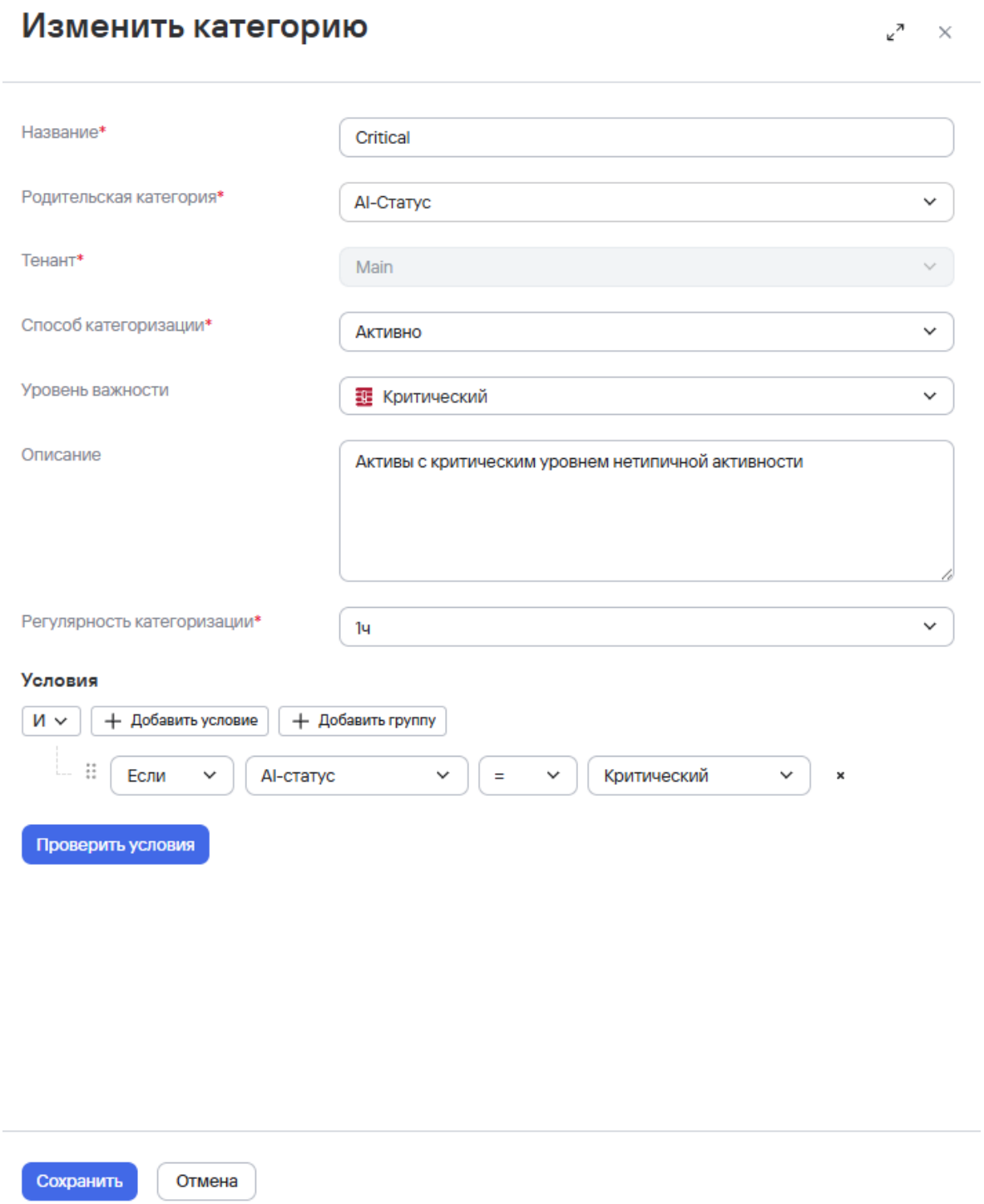
порядке. Помимо этого аналитики получают дополнительный контекст при расследовании алерта/инцидента, принимая во внимание текущий уровень нетипичной активности на активе.

Чтобы настроить проактивную категоризацию:

- Перейдите в раздел **Активы** веб-интерфейса KUMA.
- Выберите категорию **Main**/**Categorized assets** и нажмите **Добавить подкатегорию**.
- В окне **Добавить категорию** укажите:
  - В поле **Название** введите название категории - **AI-Статус**.
  - В поле **Родительская категория** укажите место категории в дереве категорий - **Categorized assets**.
  - В поле **Тенант** отображается тенант, в структуре которого вы выбрали родительскую категорию.
  - В раскрывающемся списке **Способ категоризации** выберите **Вручную**.
  - Назначьте уровень важности категории в раскрывающемся списке **Уровень важности** выберите **Низкий**.
- Нажмите **Сохранить**.



- Далее выберите созданную категорию выберите категорию **AI-Статус** и нажмите **Добавить подкатегорию**.
- Создайте подкатегорию Critical с параметрами, как на скриншоте ниже.



- Повторите операцию для подкатегорий High, Medium и Low.

Изменить категорию

Название*: High

Родительская категория*: AI-Статус

Тенант*: Main

Способ категоризации*: Активно

Уровень важности: Высокий

Описание: Активы с высоким уровнем нетипичной активности

Регулярность категоризации*: 1ч

Условия

И | + Добавить условие | + Добавить группу

Если | AI-статус | = | Высокий

Проверить условия

Сохранить | Отмена

Изменить категорию

Название*: Medium

Родительская категория*: AI-Статус

Тенант*: Main

Способ категоризации*: Активно

Уровень важности: Средний

Описание: Активы со средним уровнем нетипичной активности

Регулярность категоризации*: 1ч

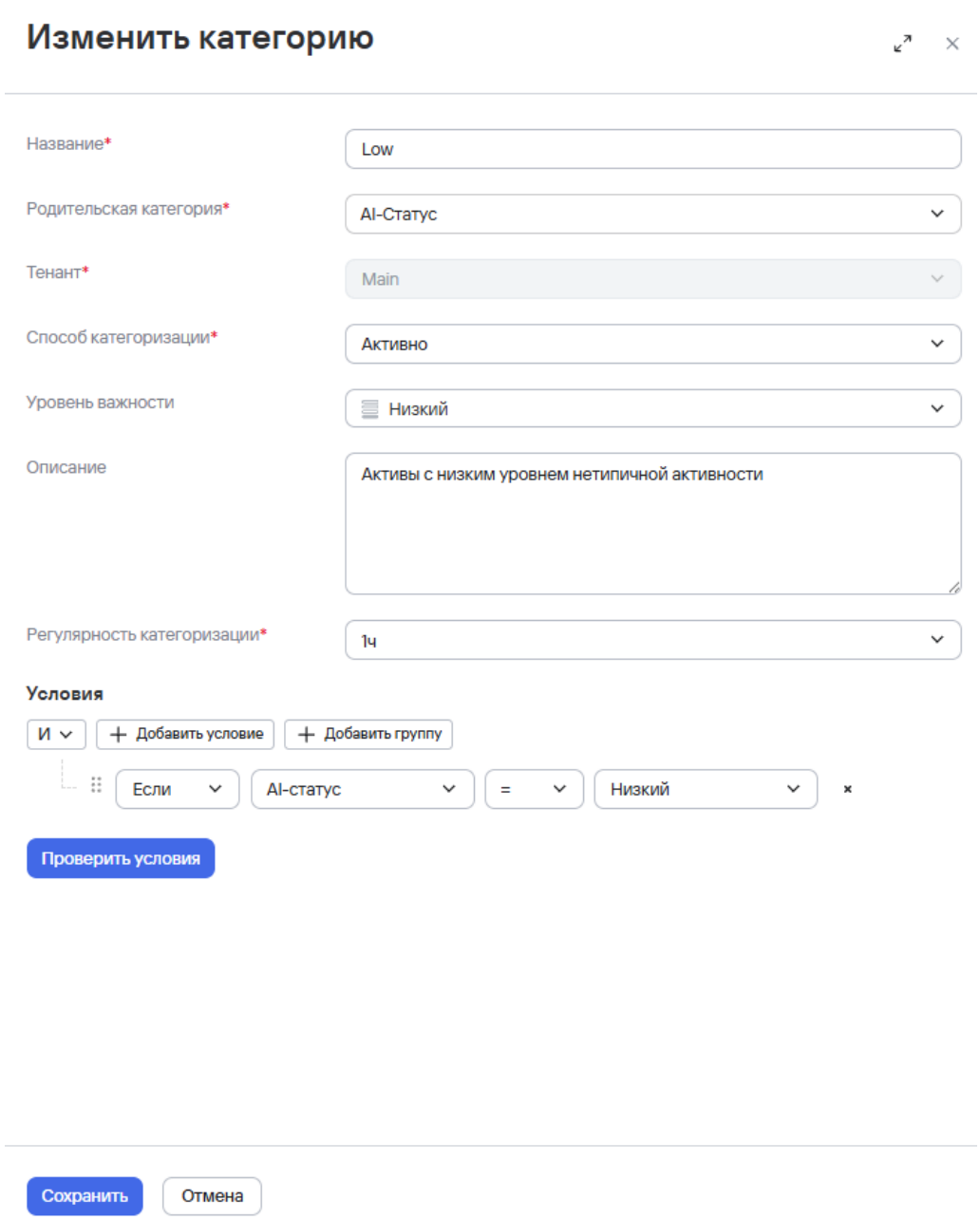
Условия

И | + Добавить условие | + Добавить группу

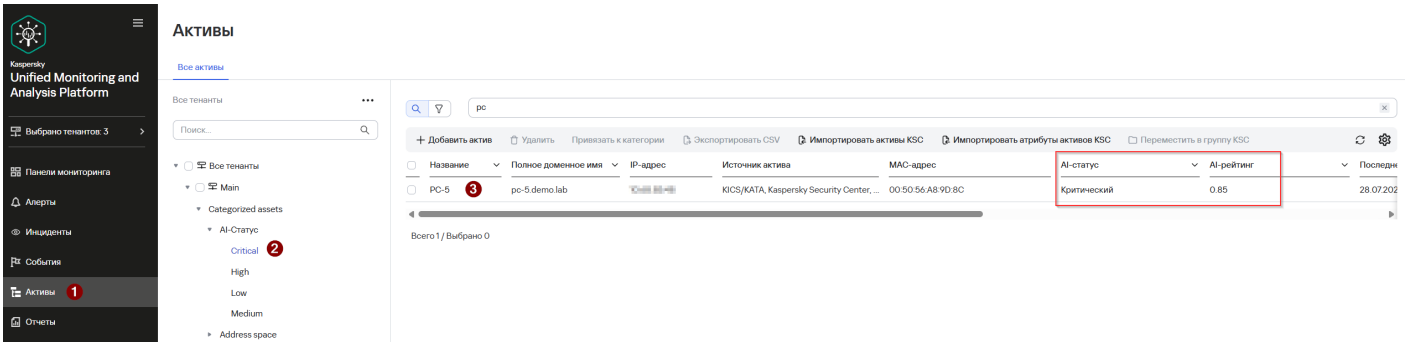
Если | AI-статус | = | Средний

Проверить условия

Сохранить | Отмена

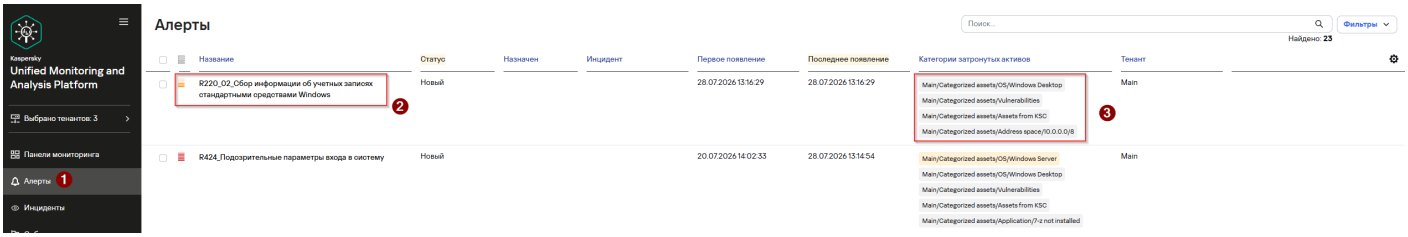


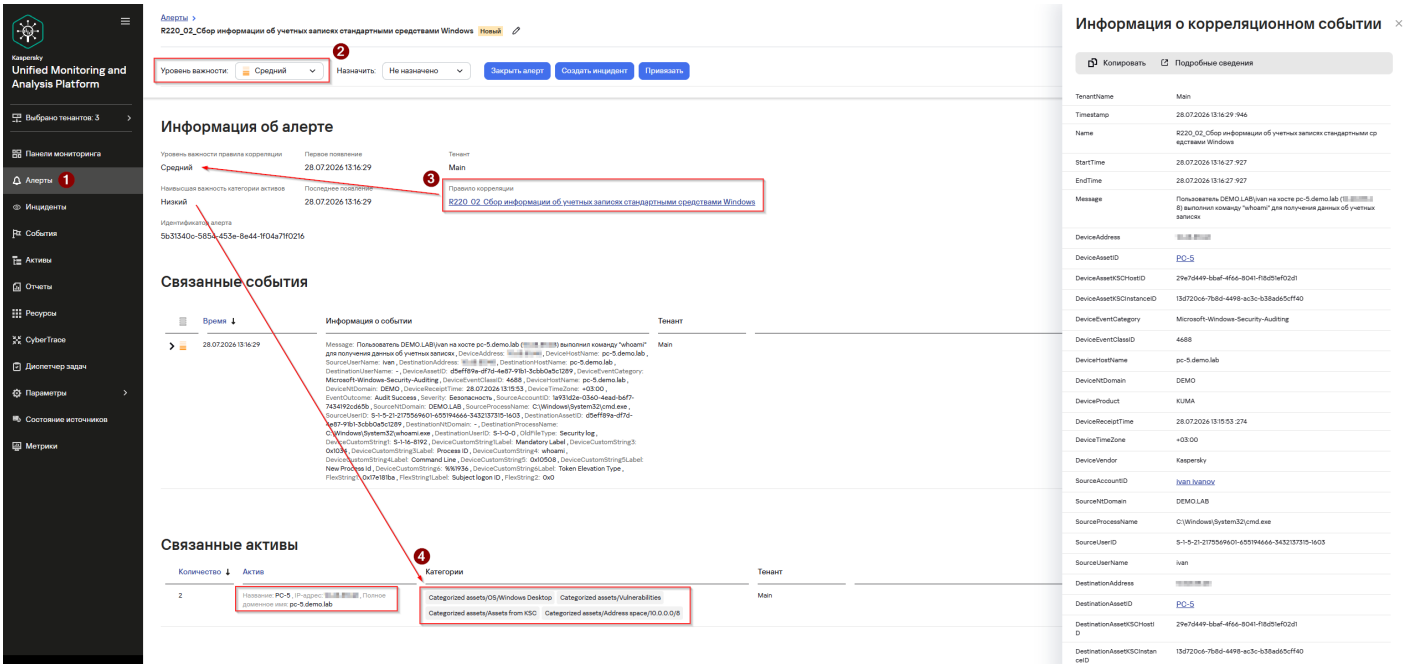
- После создания категорий убедитесь, что в них присутствуют активы с соответствующим AI-статусом.



Пример алерта без использовании скоринга активов и активной категоризации

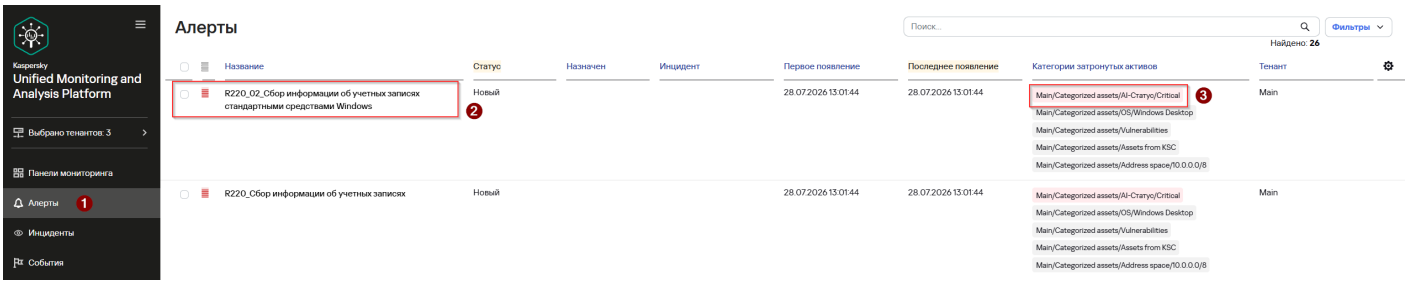
- Итоговый уровень важности алерта **Средний** и равен уровню важности сработавшего правила корреляции.



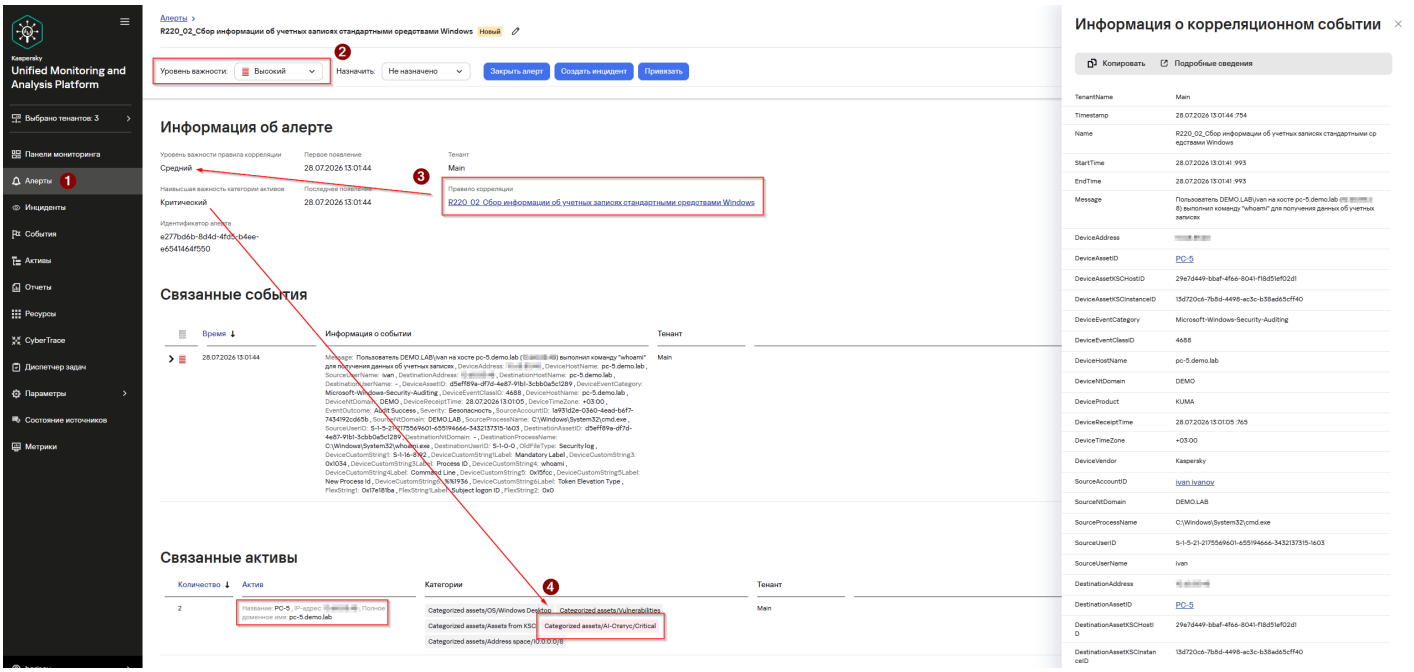


Пример алерта с использованием скоринга активов и активной категоризацией

- Итоговый уровень важности алерта **Высокий**, так как с алертом связан актив **PC-5**, на котором зафиксирован критический уровень нетипичной активности и который автоматически определен в категорию **AI-Статус/Critical**



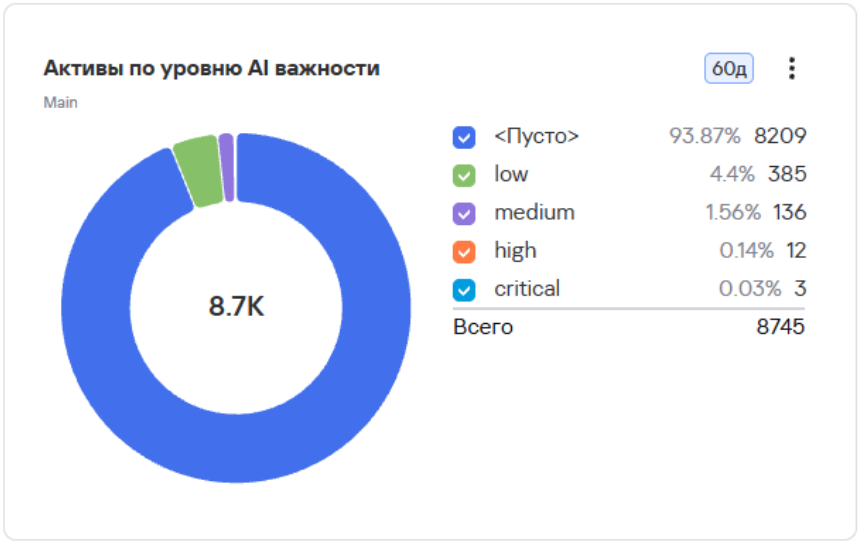
- При этом сработавшее правило корреляции с уровнем важности **Средний,** но за счет критического уровня важности категории актива алерт получил более высокий приоритет.



Use Case 2. Мониторинг уровня нетипичной активности на активах

Для отслеживания распределения активов по уровню нетипичной активности в KUMA доступен виджет **Активы по уровню важности**. На круговом графике будет отображаться количество активов с группировкой по AI-Статусу.

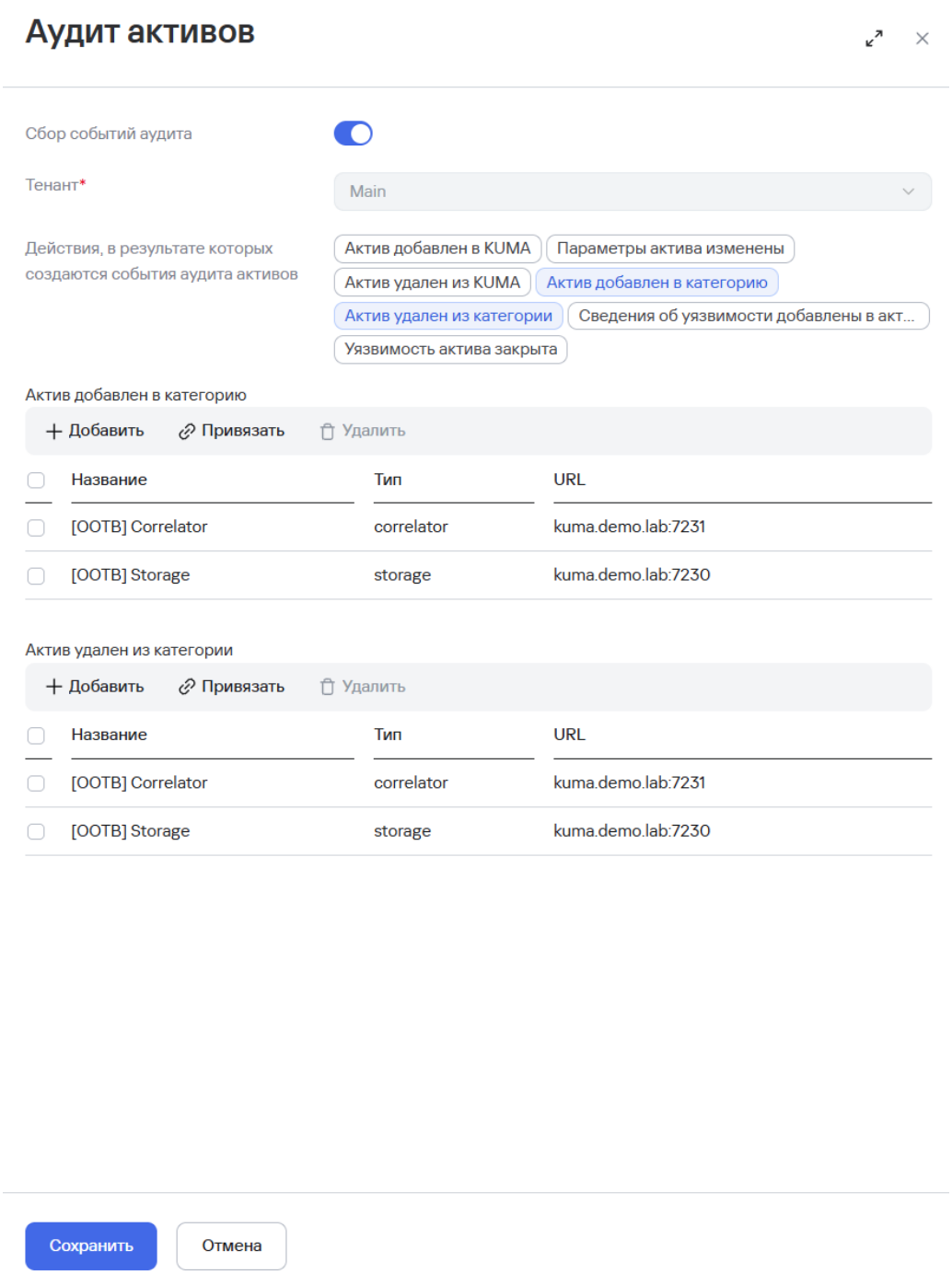
> Виджет **Активы по уровню важности** доступен, если лицензия содержит модуль AI.



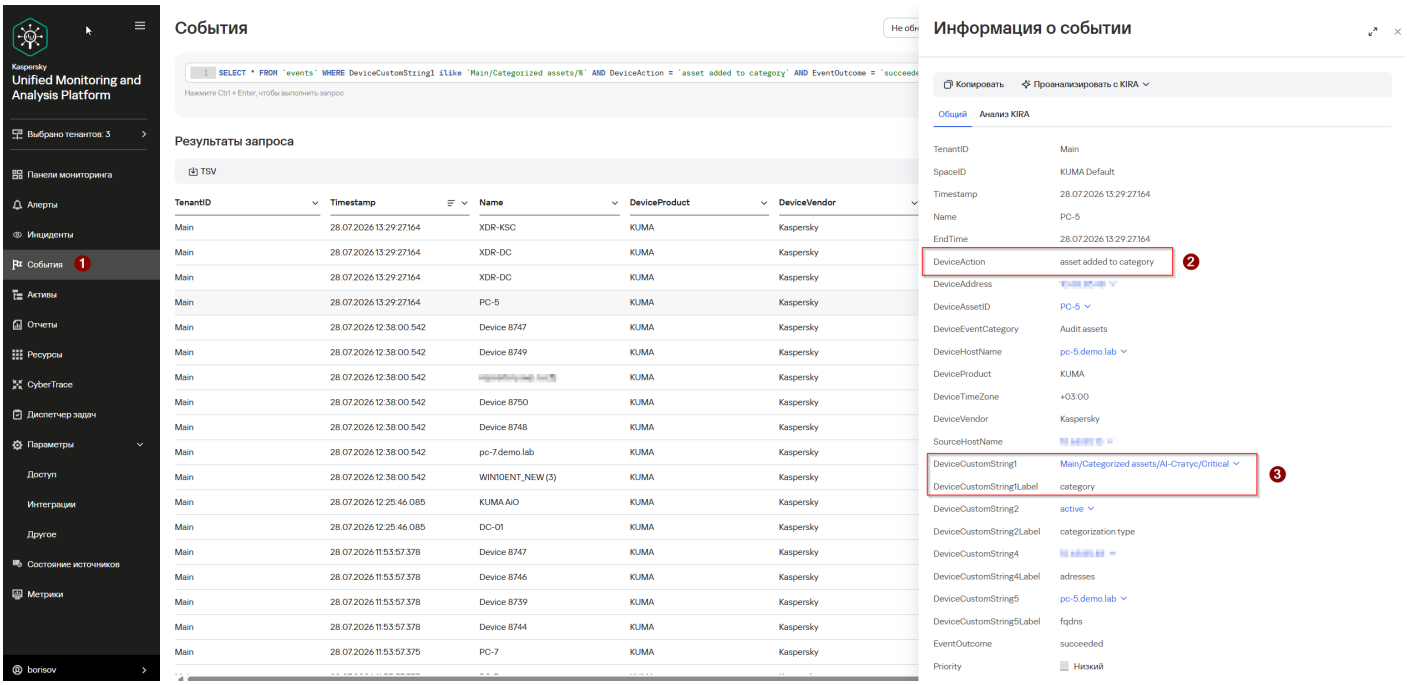
Кроме этого можно отслеживать перемещение активов между разными категориями (см. Use Case 1) на основании событий аудита активов KUMA.

Для настройки аудита активов:

- Перейдите в **Параметры → Другое → Активы →** вкладка **Аудит активов**.
- Нажмите **Добавить параметры для нового тенанта**.
- Выполните настройку параметров аудита активов, как на скриншоте ниже.

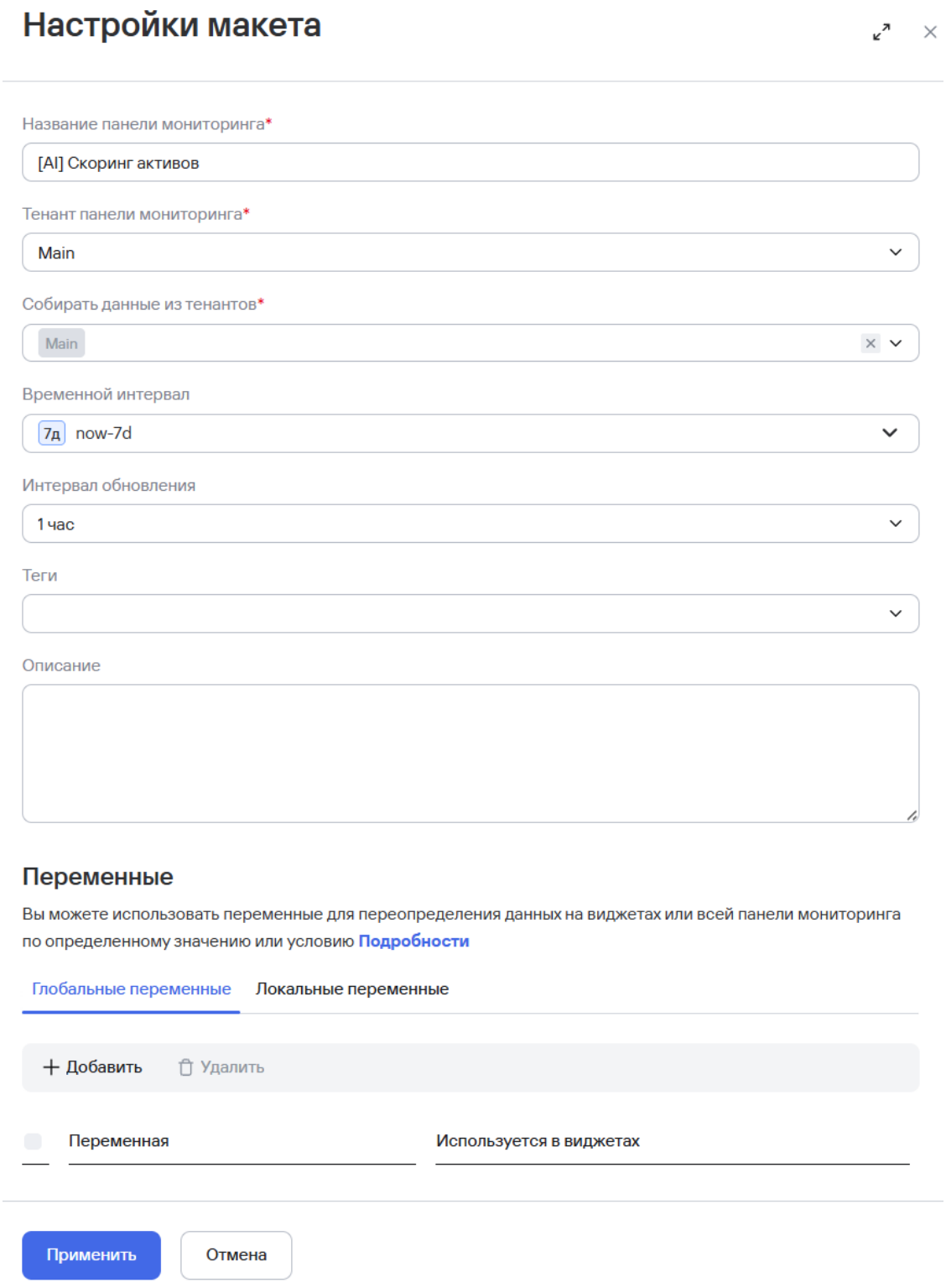


Теперь при изменении категории актива, например, при переходе из категории High в Critical будет создано событие аудита активов.

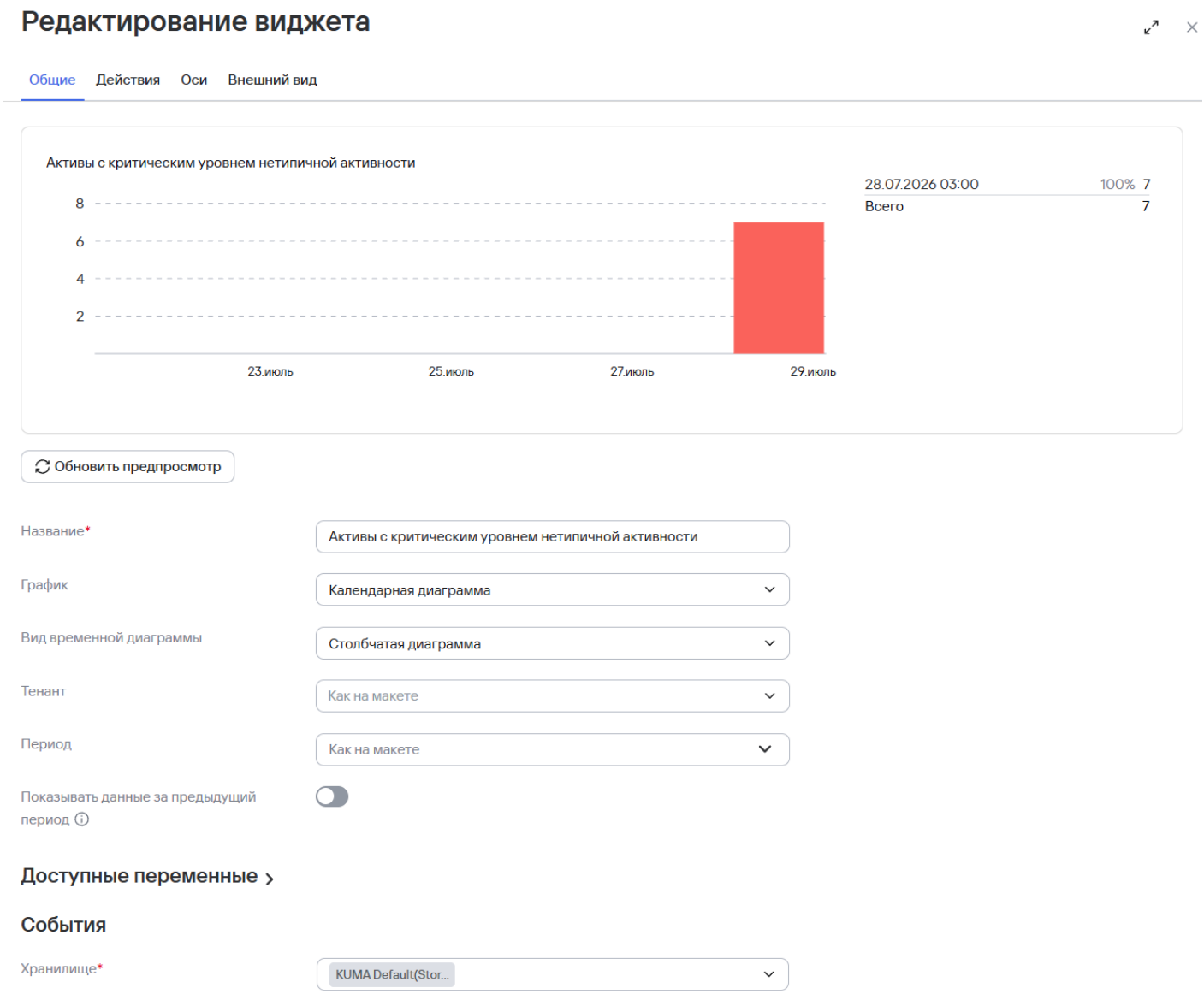


Перемещение активов между категориями можно визуализировать с помощью виджетов. Для этого:

- Перейдите в **Панель мониторинга** и нажмите **Создать панель мониторинга**.
- Нажмите **Добавить параметры для нового тенанта**.
- В окне **Настройки макета** укажите параметры, как на скриншоте ниже, и нажмите **Применить**.

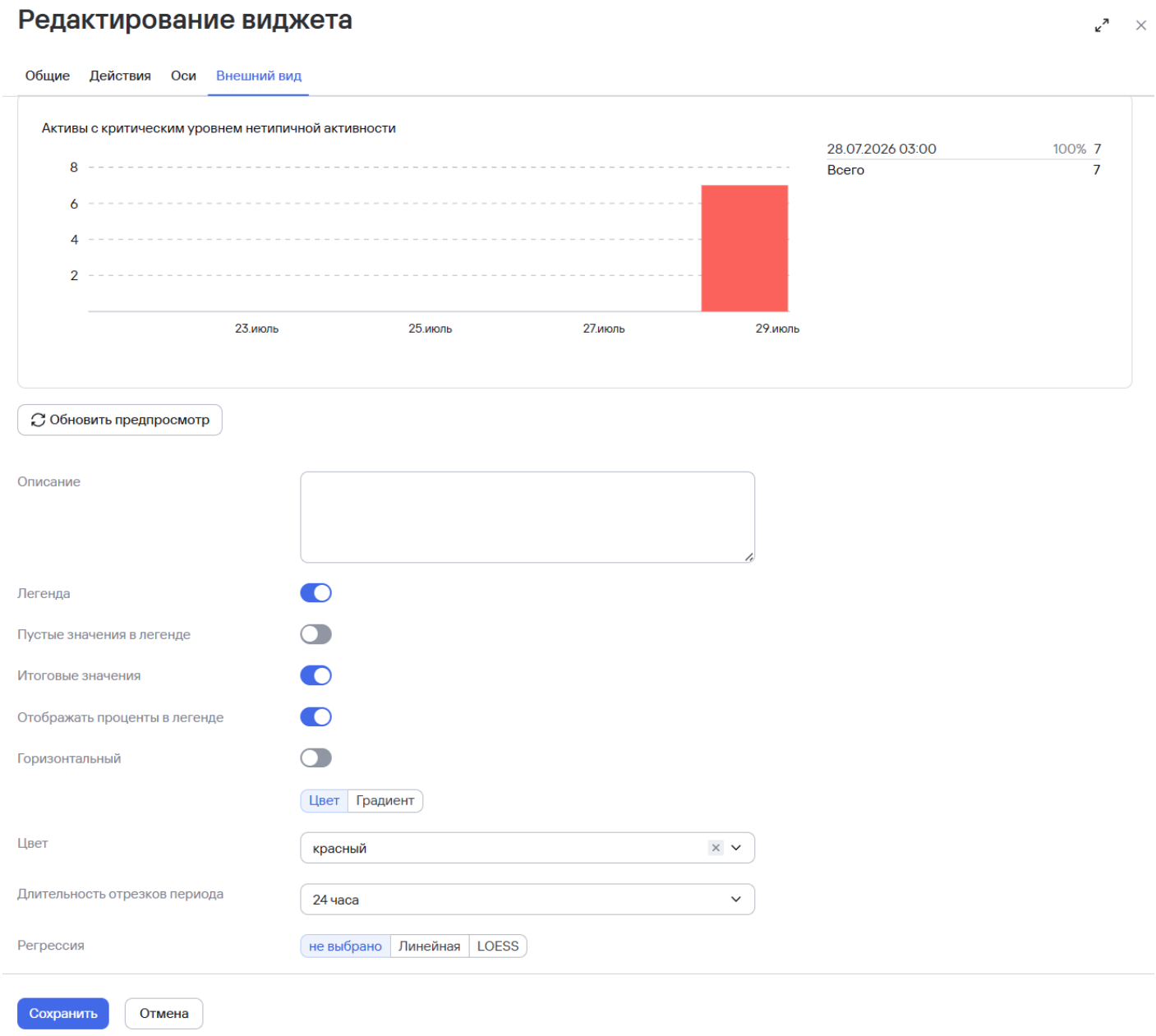


- На новой панели мониторинга добавьте следующие виджеты:
  - "Коробочный" виджет **Активы по уровню AI важности** (**Добавить виджет → Активы → Активы по уровню AI важности)**
  - Виджеты (**Добавить виджет → События)** на основе событий:
    - **Активы с критическим уровнем нетипичной активности**

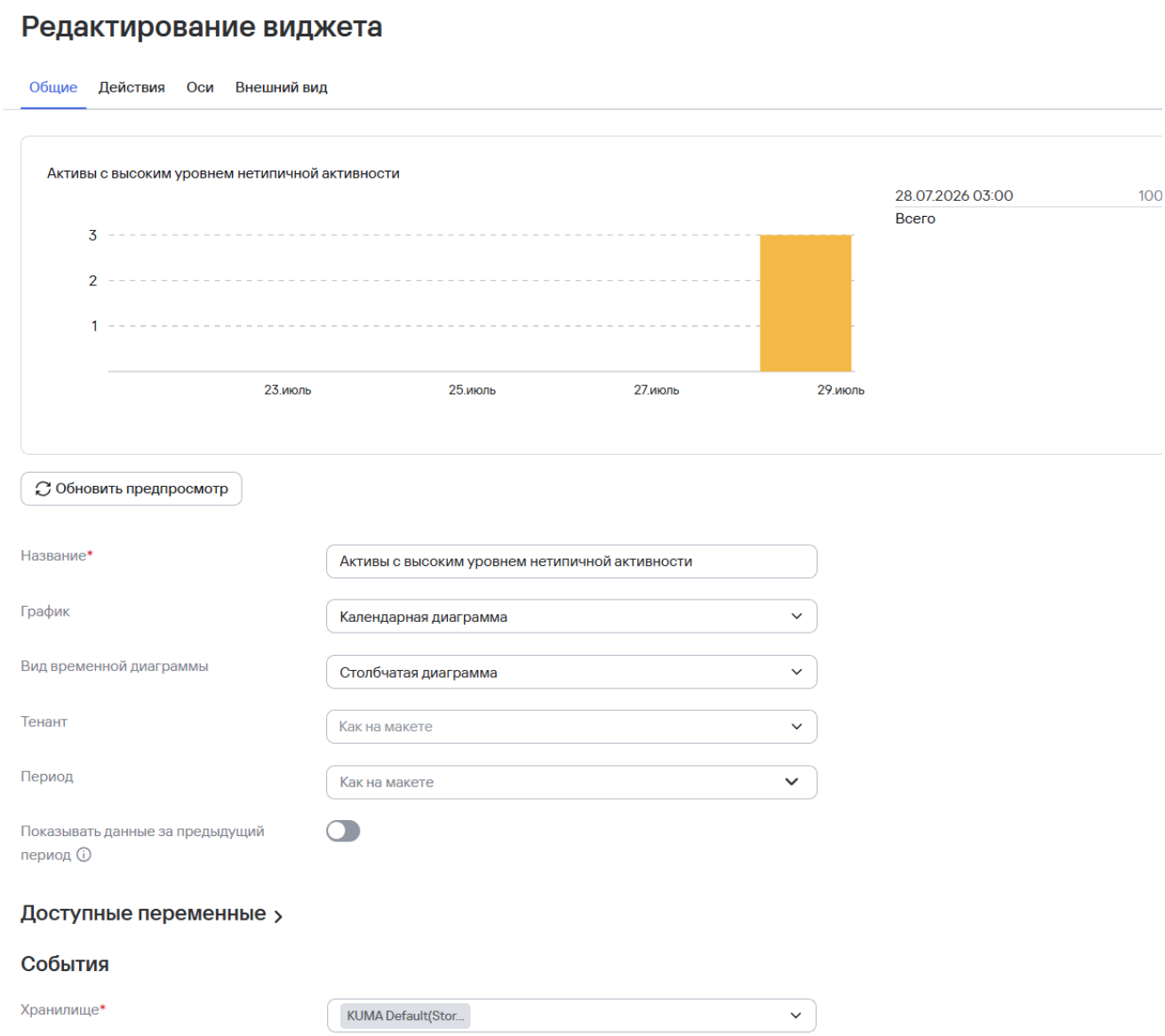


SQL-запрос

```
SELECT count(ID) AS `metric`, formatDateTime(toTimeZone(fromUnixTimestamp64Milli(Timestamp), 'Europe/Moscow'), '%d.%m.%Y %H:%m:%S') AS `value`
FROM `events`
WHERE DeviceCustomString1 = 'Main/Categorized assets/AI-Статус/Critical' AND DeviceAction = 'asset added to category' AND EventOutcome = 'succeeded' AND DeviceEventCategory = 'Audit assets'
GROUP BY Timestamp
ORDER BY value
LIMIT 250
```

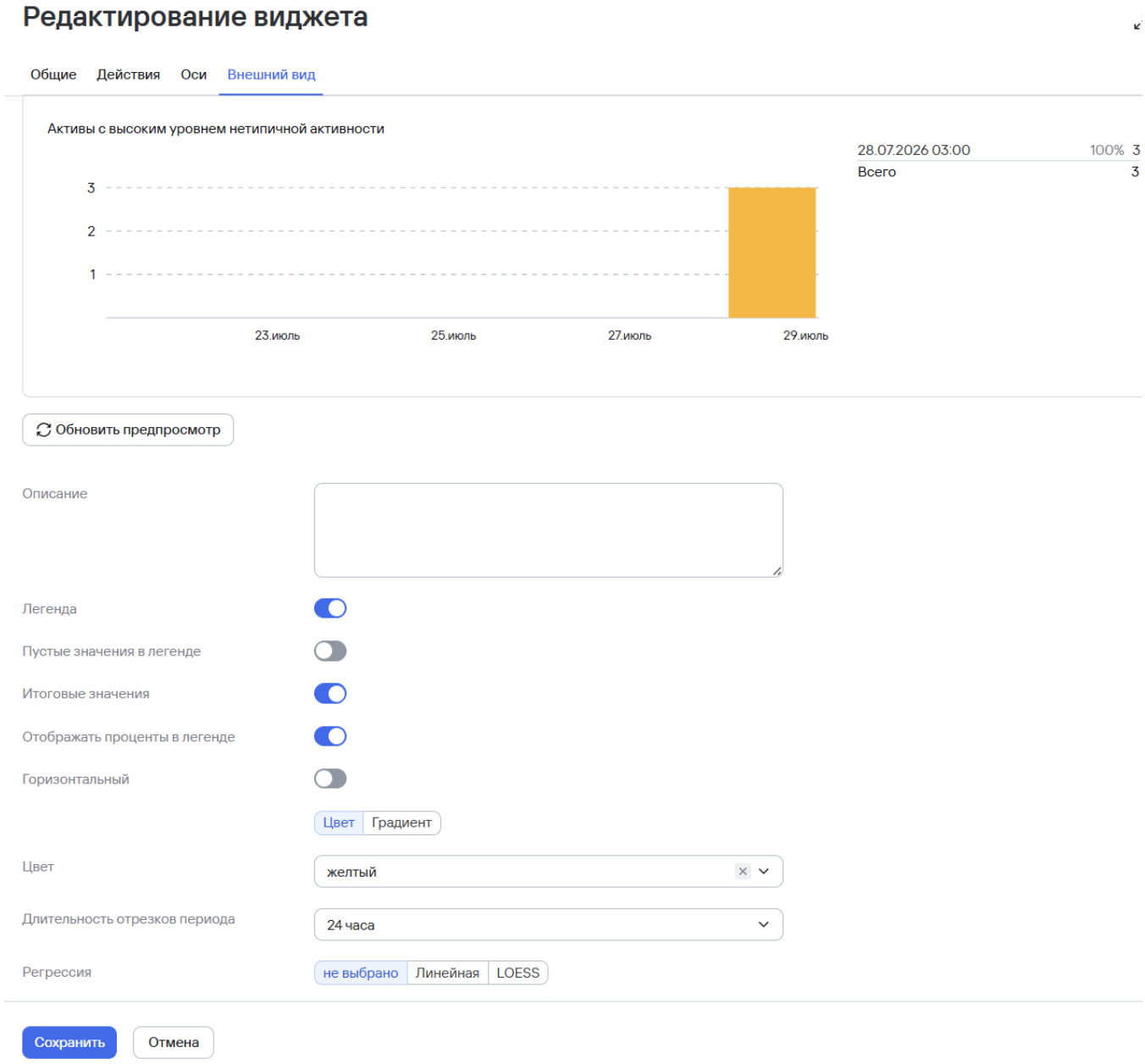


- **Активы с высоким уровнем нетипичной активности**

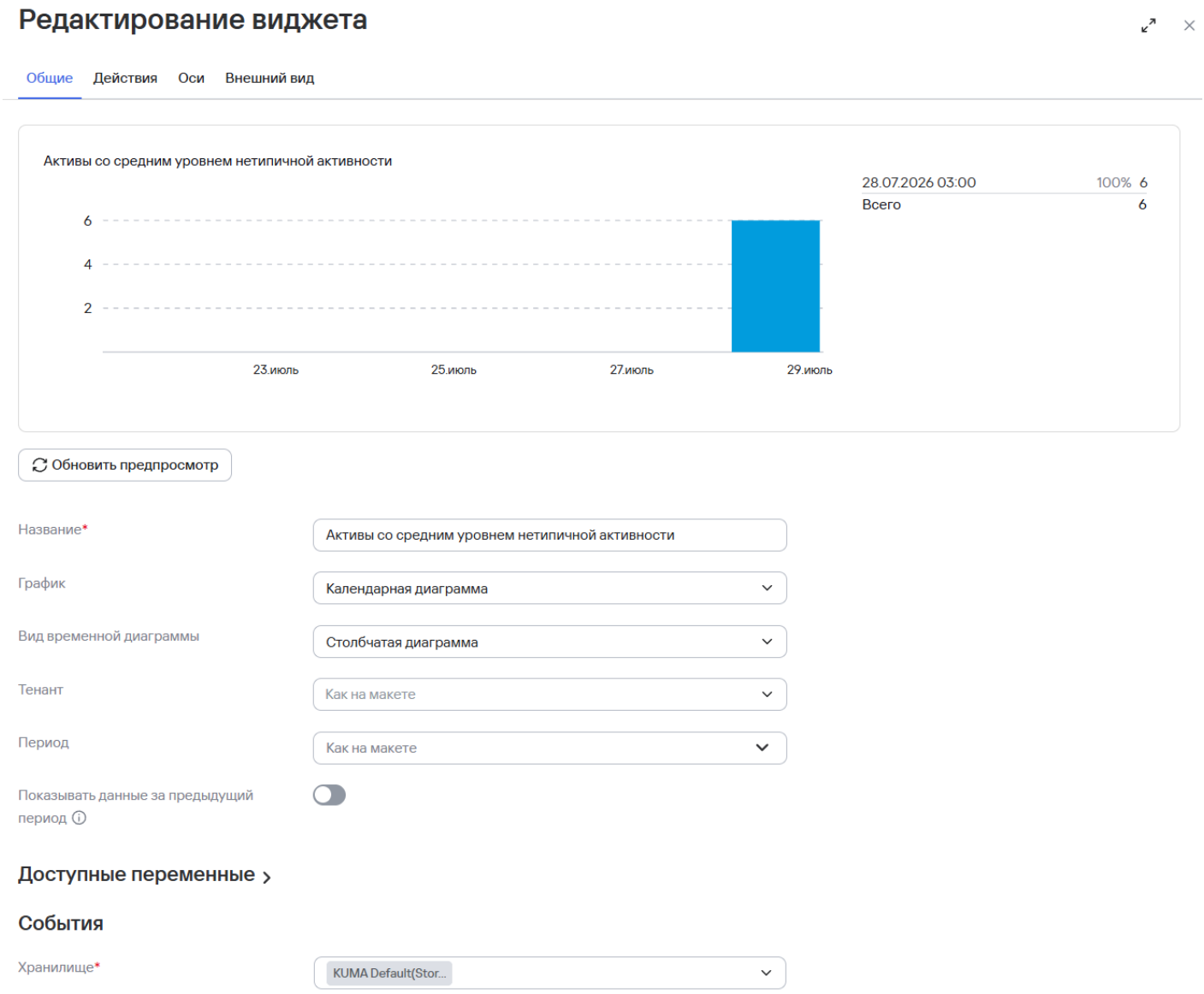


SQL-запрос:

```
SELECT count(ID) AS `metric`,
formatDateTime(toTimeZone(fromUnixTimestamp64Milli(Timestamp), 'Europe/Moscow'),
'%d.%m.%Y %H:%m:%S') AS `value`
FROM `events`
WHERE DeviceCustomString1 = 'Main/Categorized assets/AI-Статус/High' AND DeviceAction
= 'asset added to category' AND EventOutcome = 'succeeded' AND DeviceEventCategory =
'Audit assets'
GROUP BY Timestamp
ORDER BY value
LIMIT 250
```

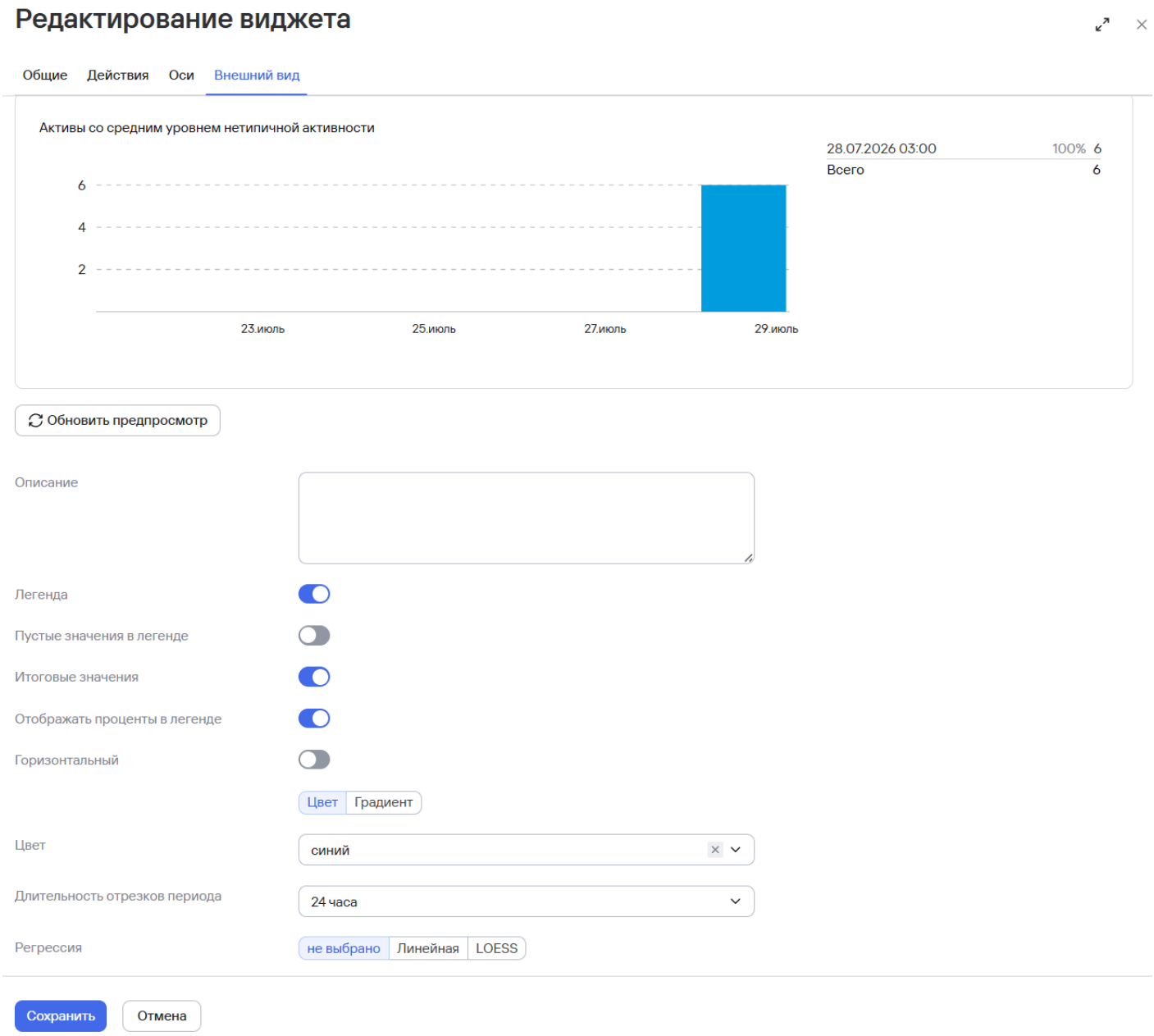


- **Активы с средним уровнем нетипичной активности**

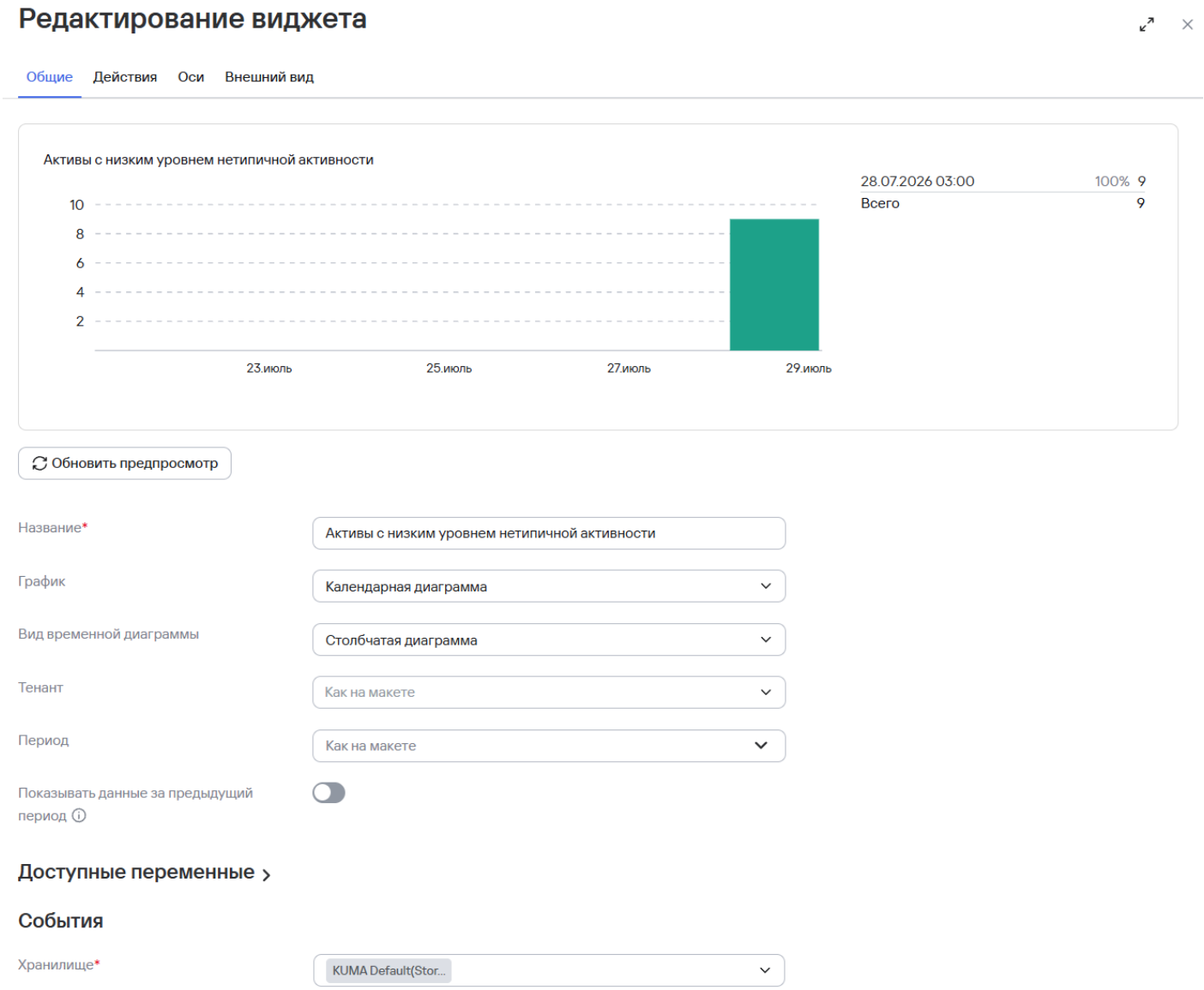


SQL-запрос:

```
SELECT count(ID) AS `metric`, formatDateTime(toTimeZone(fromUnixTimestamp64Milli(Timestamp), 'Europe/Moscow'), '%d.%m.%Y %H:%m:%S') AS `value`
FROM `events`
WHERE DeviceCustomString1 = 'Main/Categorized assets/AI-Статус/Medium' AND DeviceAction = 'asset added to category' AND EventOutcome = 'succeeded' AND DeviceEventCategory = 'Audit assets'
GROUP BY Timestamp
ORDER BY value
LIMIT 250
```

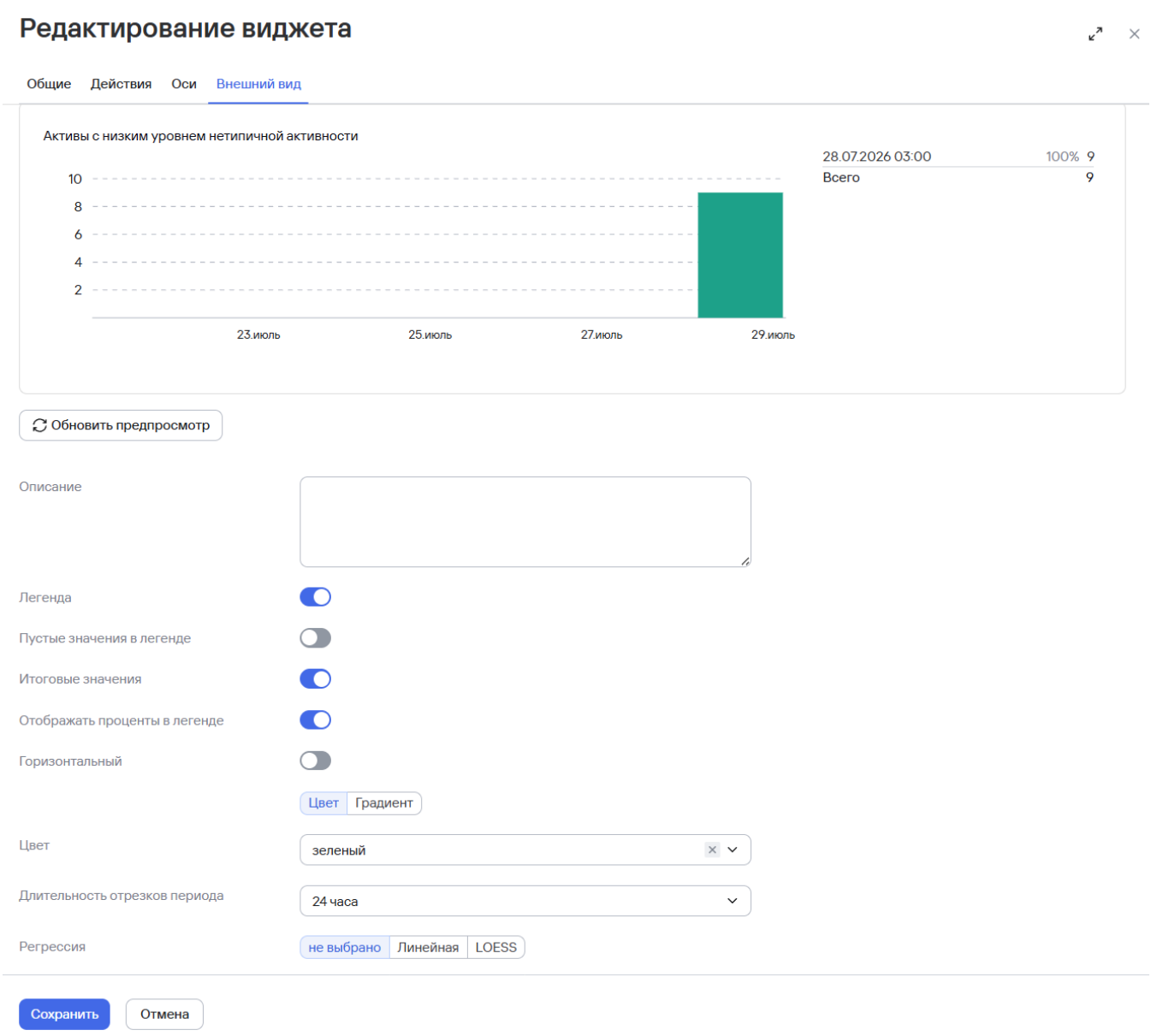


- **Активы с низким уровнем нетипичной активности**

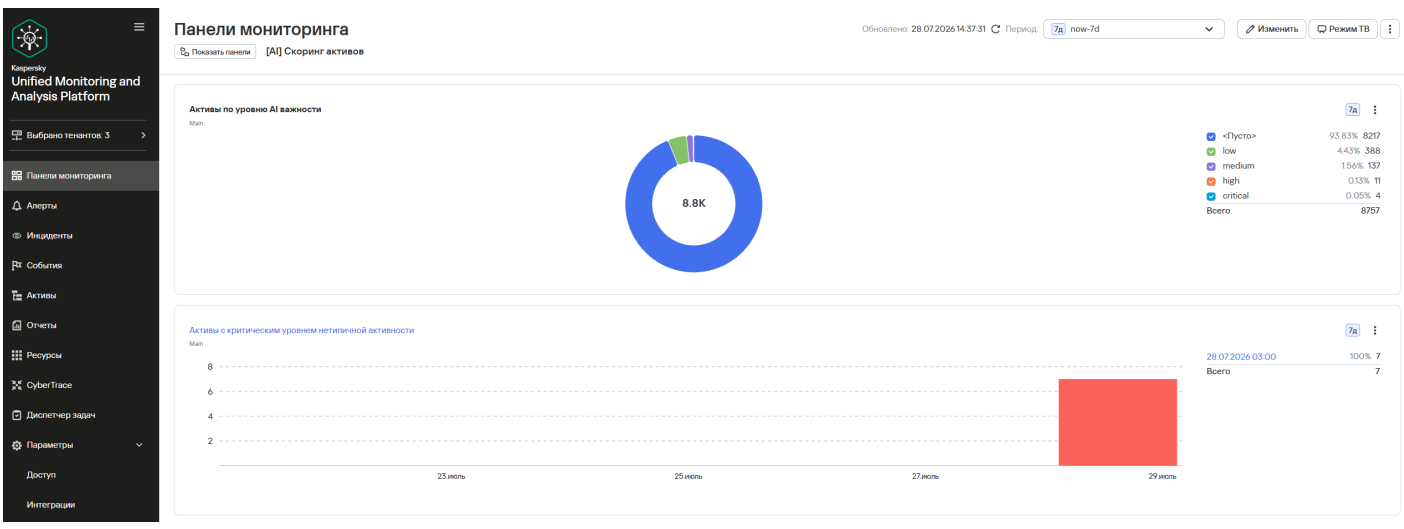


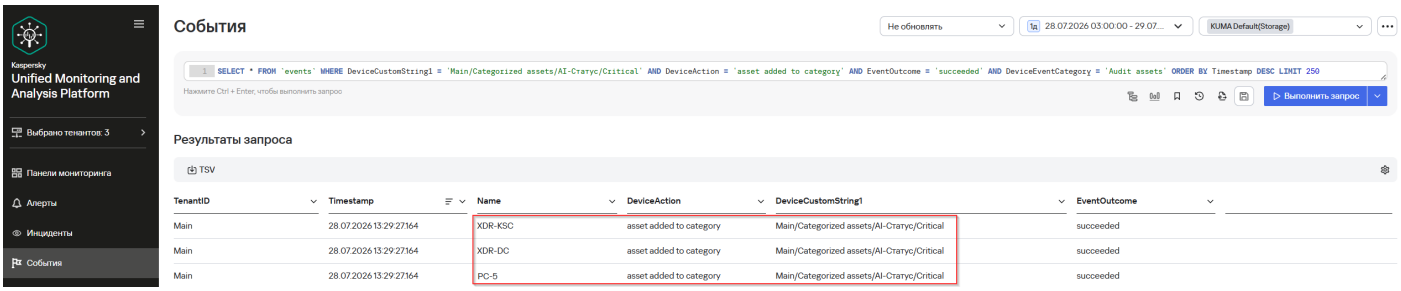
SQL-запрос:

```
SELECT count(ID) AS `metric`, formatDateTime(toTimeZone(fromUnixTimestamp64Milli(Timestamp),
'Europe/Moscow'), '%d.%m.%Y %H:%m:%S') AS `value`
FROM `events`
WHERE DeviceCustomString1 = 'Main/Categorized assets/AI-Статус/Low' AND DeviceAction = 'asset
added to category' AND EventOutcome = 'succeeded' AND DeviceEventCategory = 'Audit assets'
GROUP BY Timestamp
ORDER BY value
LIMIT 250
```



Виджеты для мониторинга перемещений активов между категорями настроены. При нажатии на дату в легенде виджета будет выполнен переход в раздел **События** для просмотра событий аудита активов и определения какие активы были перемещены в категорию.

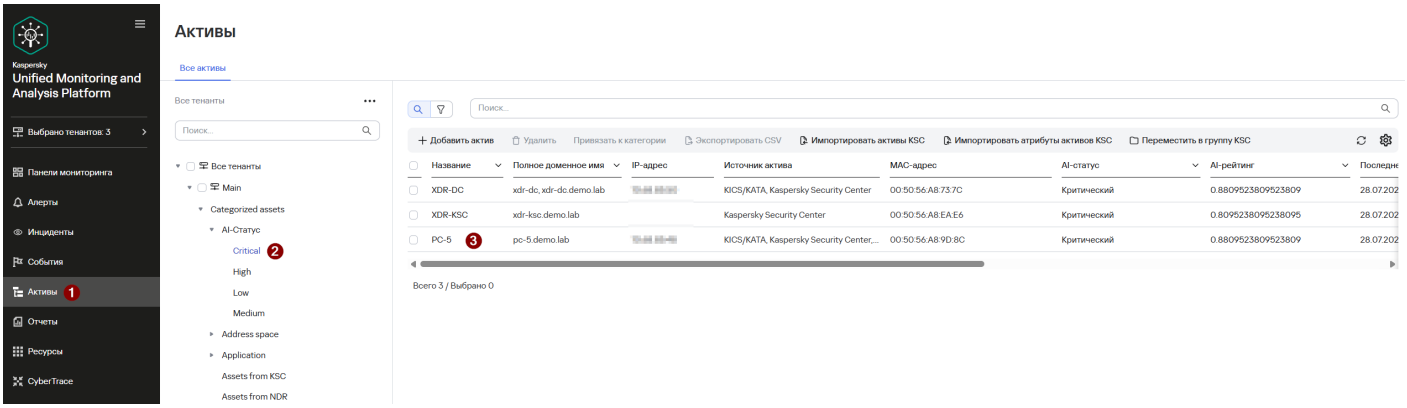


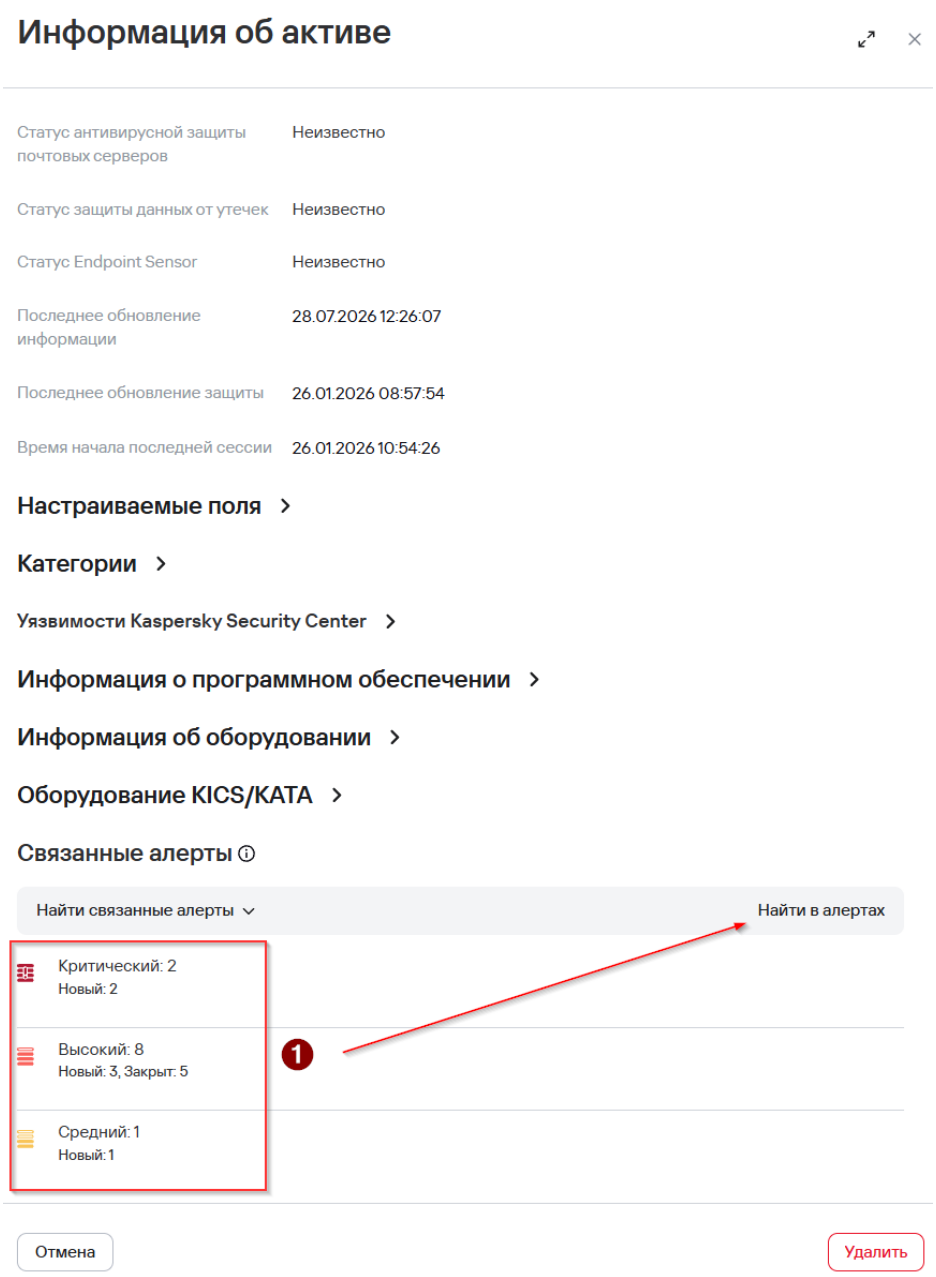


Дополнительно можно настроить аналогичный шаблон отчета и правила корреляции для создания алертов в случае перемещения активов в заданную категорию, например, в категорию Critical.

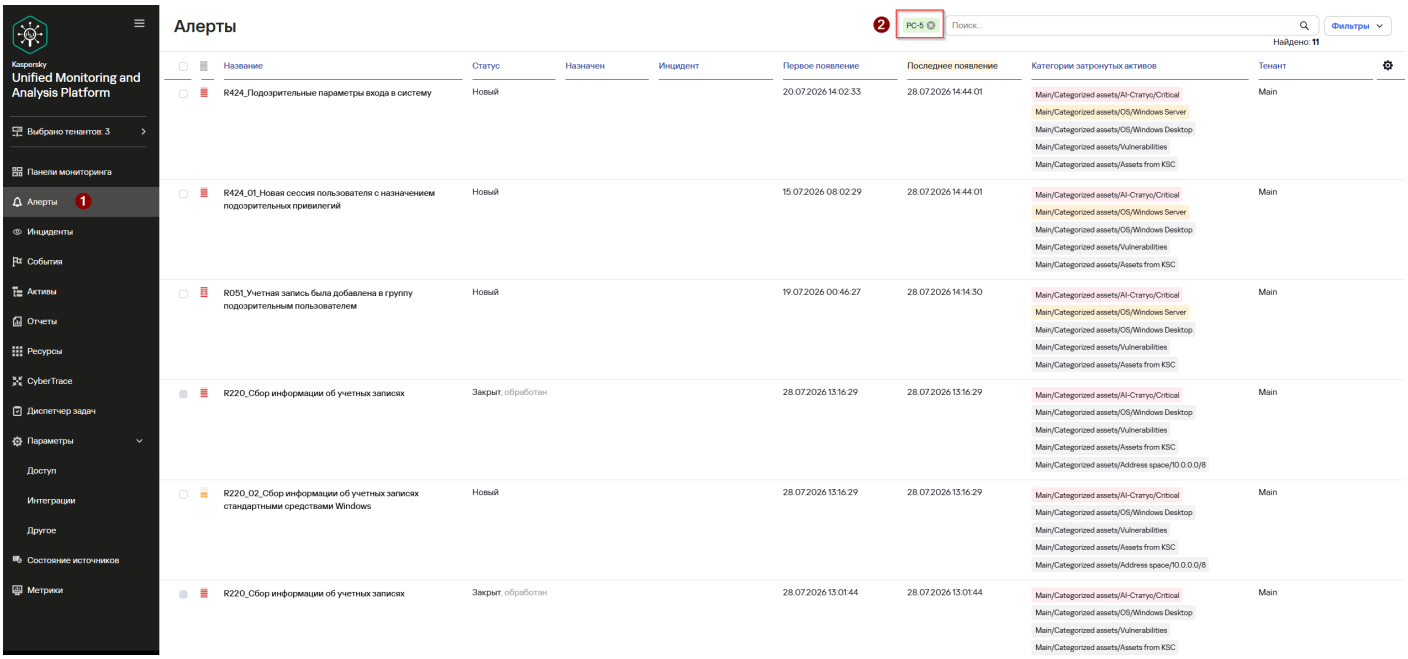
Use Case 3. Проактивный поиск угроз

Для активов с критическим или высоким уровнем нетипичной активности аналитик может вручную исследовать алерты и события с этих активов в поисках признаков вредоносной активности и проработки гипотез.





При нажатии на **Найти в алертах** будет выполнен переход в раздел **Алерты** и автоматически применен фильтр по активу для отображения только тех алертов, в которых фигурирует выбранный актив.



Revision #17
Created 2025-02-26 09:28:25 UTC by Boris Rzr
Updated 2026-08-17 18:11:19 UTC by Dmitry Borisov