Ретроспективная проверка

?????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? **НЕ** ???????? ??????????? ????????????? ???????.

??????????? ???????????? ?? ??????? ??????? ????????? ? ??????-??????? ?? ???????: https://support.kaspersky.ru/kuma/4.0/217979

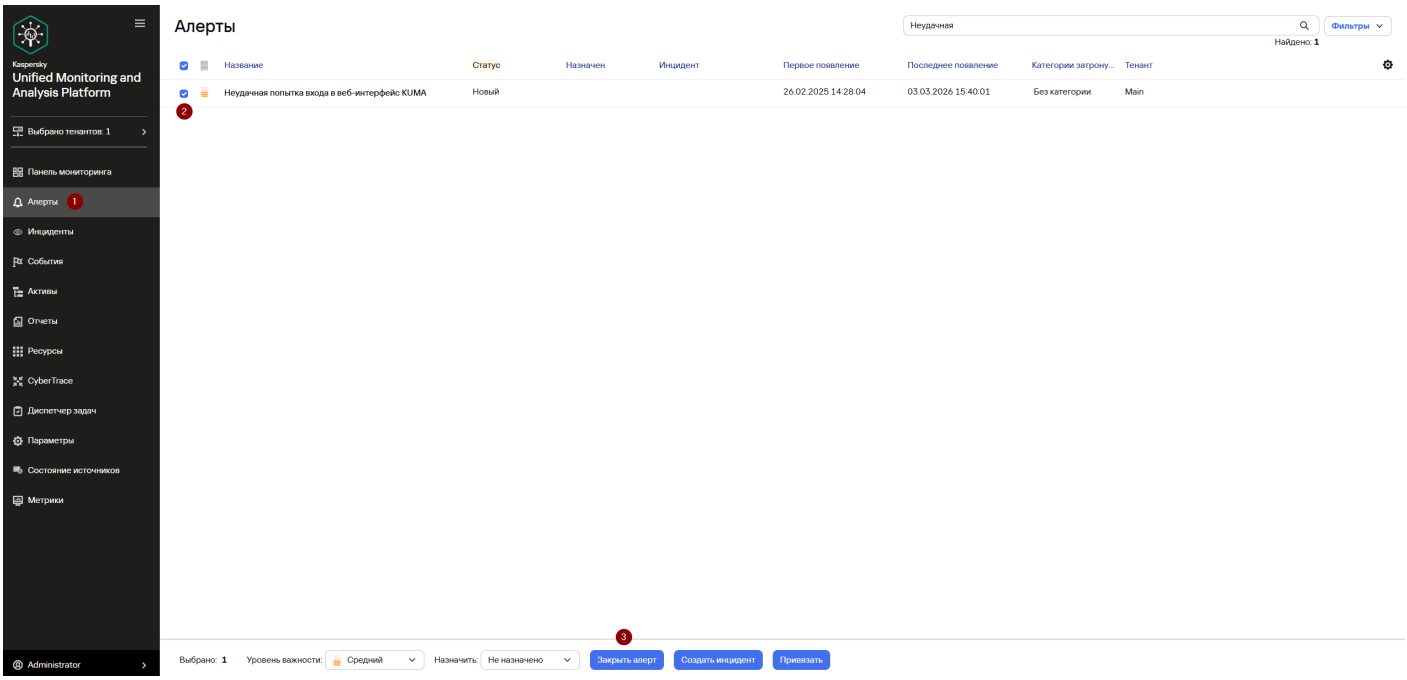
? ??????? ?????? ?????????? ???????? ?????? ? ?????????, ???????????? ?? ??????????? ? ???????? ???????, ???????? ????????? ???????????.

?????????????? ???????? ????????? ????????? ??????? ?????????? ? ???????????? ????????, ??? ??????????? ? ?????????. ??? ??????, ???? ?? ?????? ????????? ? ???????????? ??????? ?????????? ??? ????????? ????? ? ?????? ????????? ??????? ??????????? ?????????? ??? ?????????? ? ????? ??????????? ????????.

? ??????? ?????????? ??????? ????? ?????????? ?????? ???????????? ???????, ??? ??????? ????? ????????? ?????????????? ????????, ?????? ?????? ?????? ? ??????? ?????????, ? ??????? ??????? ?????? ???????. ????? ????? ????????? ?????? ???, ????? ?? ????? ?????????????? ???????? ??????????? ?????? ? ??????????? ??????? ????????????.

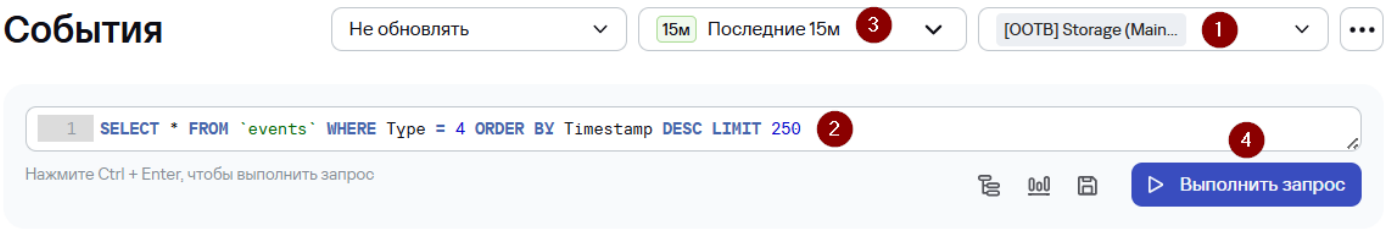
??? ???????????? ?????????????? ????????:

- ???????? ??????? ?????????? ????????? ??????? ????? ? ???-????????? KUMA (??. **Создание правила корреляции типа Simple**).
- ????????? ????????? ??????? ????? ? ???-????????? KUMA.
- ????????? ? **Алерты** ? ???????? ????? **Неудачная попытка входа в веб-интерфейс KUMA** (??? ???????).



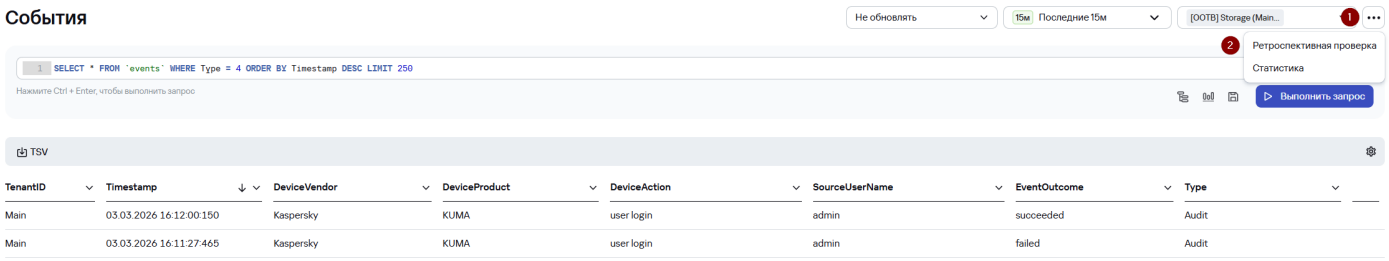
????? ????????? ??????????????? ????????:

- ????????? ? ?????? **События** ? ??????????? ??????????? ??????? ???????:
  - ???????? ?????????.
  - ??????? ????????? ??????.
  - ??????? ??????????? ????????? ??????.
- ??????? **Выполнить запрос**.



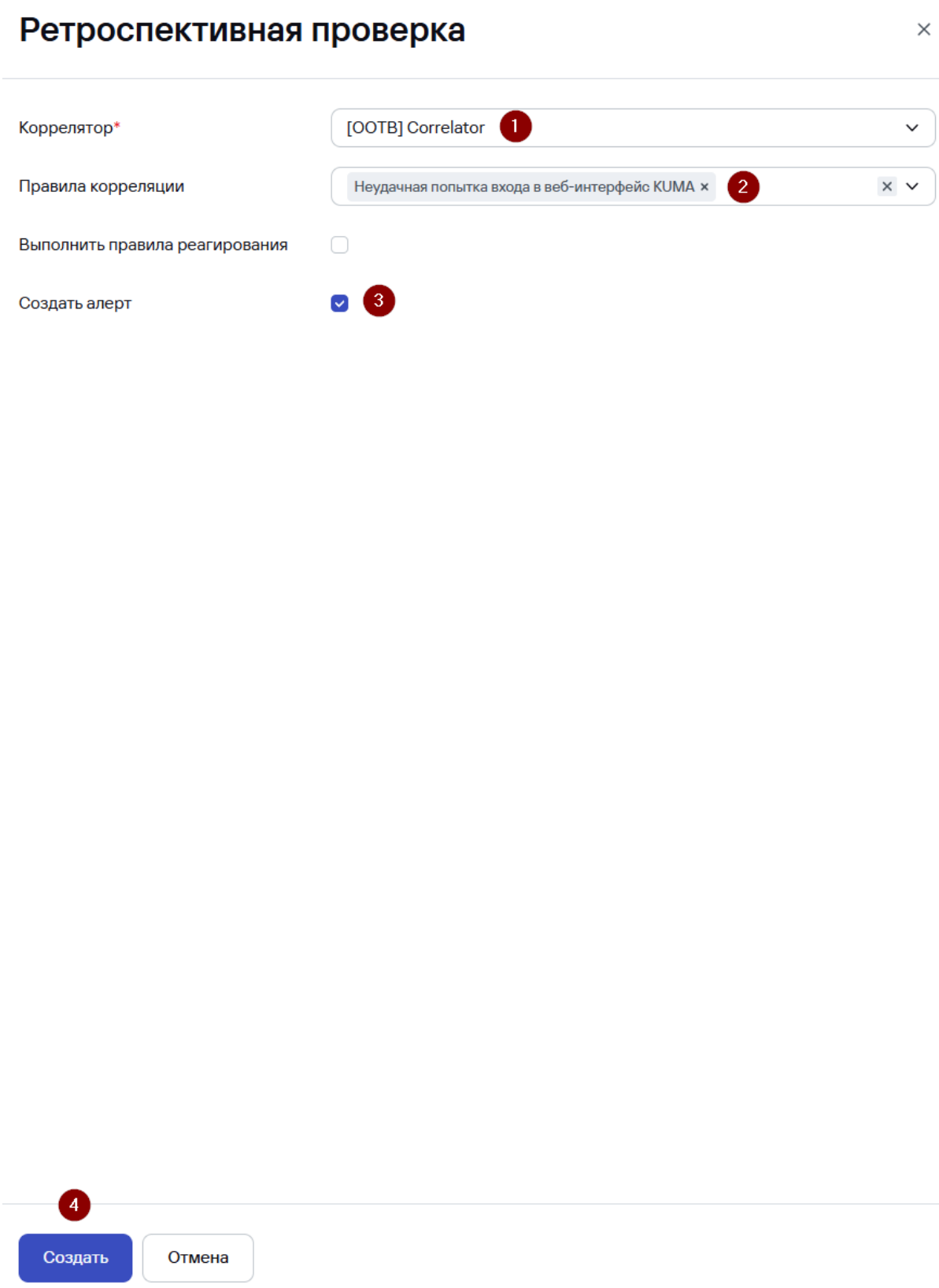

```
SELECT * FROM `events` WHERE Type = 4 ORDER BY Timestamp DESC LIMIT 250
```

- ? ?????????????? ?????? ⋯ ???????? **Ретроспективная проверка**.



- ? ??????????? ???? **Ретроспективная проверка**:

- ? ?????????????? ?????? **Коррелятор** ???????? ?????? ???????????, ? ??????? ????? ????????? ????????? ???????.
- ? ?????????????? ?????? **Правила корреляции** ???????? ??????? ??????????, ? ??????? ??????? ?????????? ?????????? ????????? ???????. ???? ?? ???? ???? ?? ??????? ?? ?????? ???????, ???????? ????? ????????? ? ???????????? ???? ?????? ??????????.
- ???? ??????????, ????? ? ???????? ????????? ??????? ???????????? ??????? ????????????, ???????? ????????????? **Выполнить правила реагирования**.
- ???? ??????????, ????? ? ???????? ????????? ??????? ???????????? ??????, ???????? ????????????? **Создать алерты**.
- ??????? ?? ?????? **Создать**.

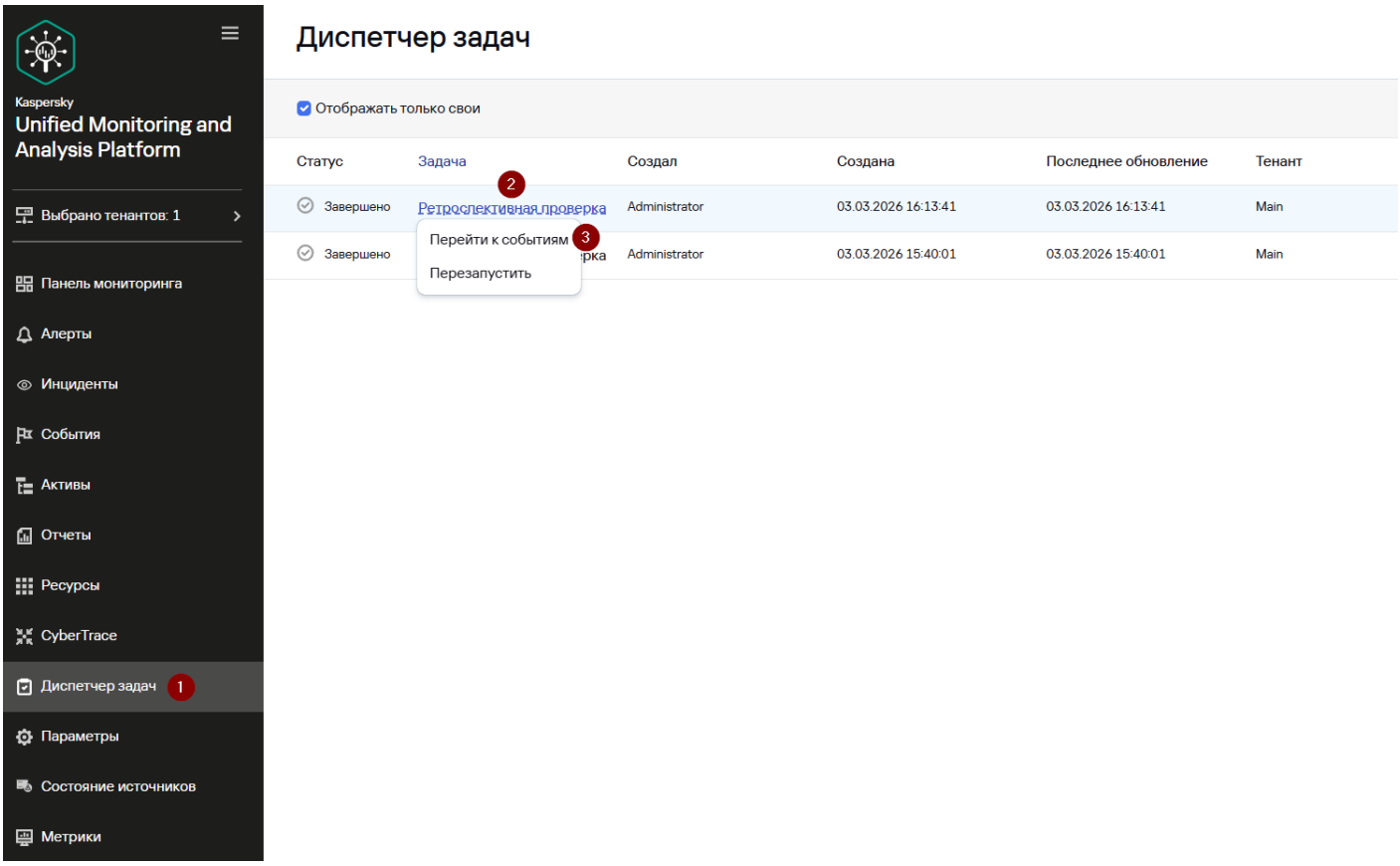


? ??????? **Диспетчер задач** ??????? ?????? ?????????????? ????????.

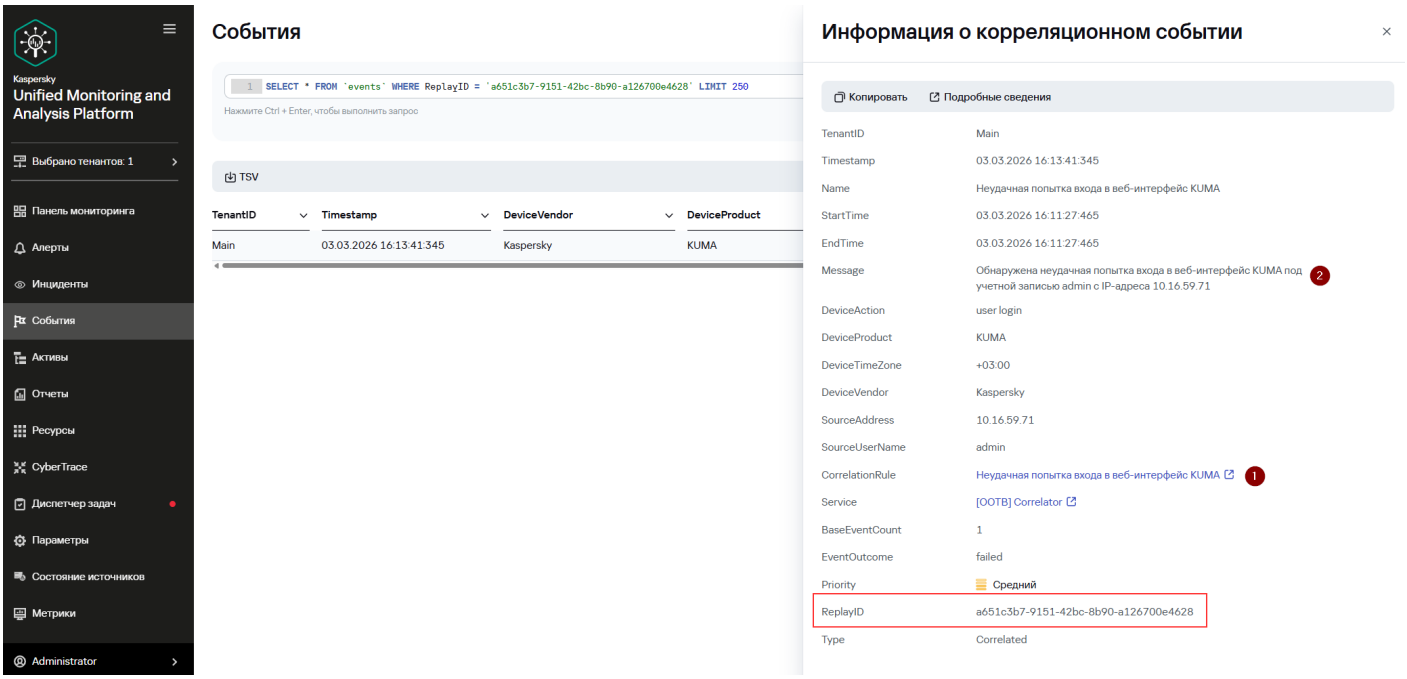
????? ??????????? ?????????? ????????:

- ????????? ? **Диспетчер задач**.

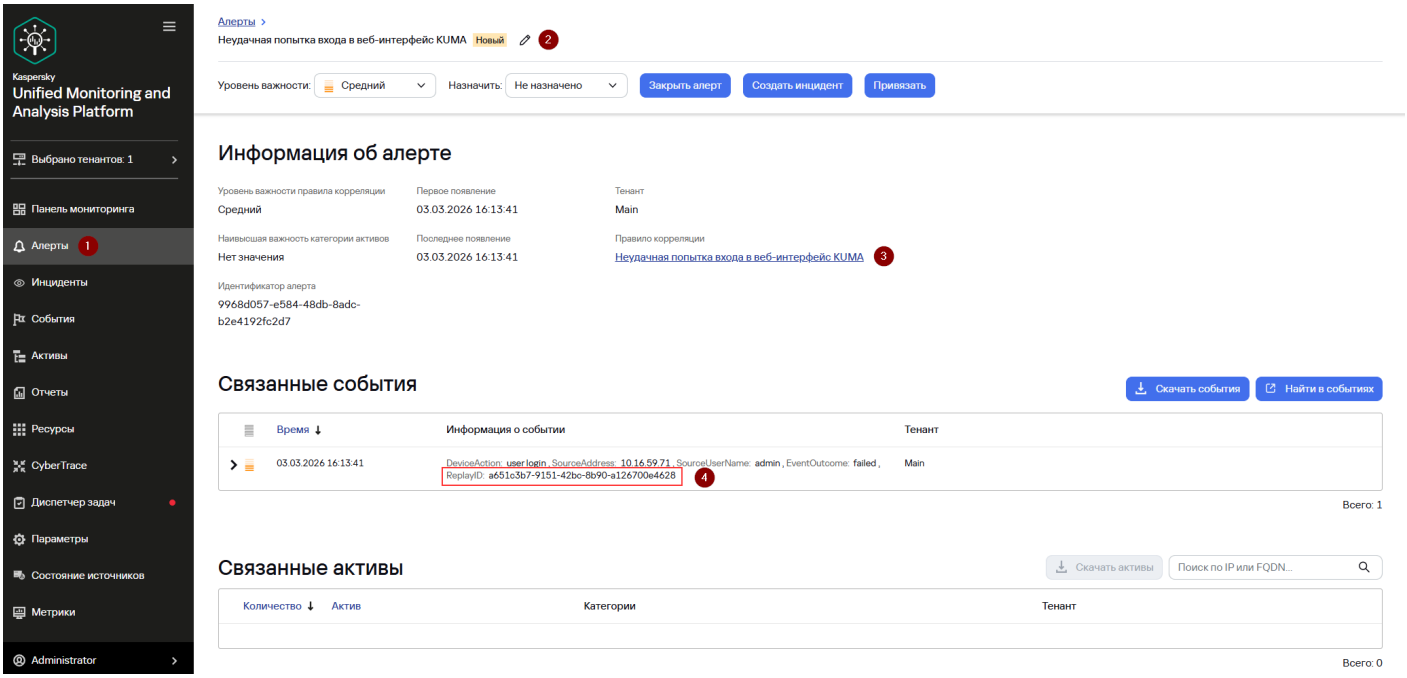
- ??????? ?? ????????? ?????? **Ретроспективная проверка** ? ? ????????????? ?????? ???????? **Перейти к событиям**.



- ????????? ????? ??????? ???????? ? ???????? ????????????? ???????, ????????? ? ???????? ??????????????? ???????? ???????????? ???????. ????????????? ???????, ???????? ????????????? ???? **ReplayID**, ? ??????? ???????? ?????????? ????????????? ?????????? ????????????? ????????.



????? ? ???? ??????????????? ???????? ????? ?????? ????? **Неудачная попытка входа в веб-интерфейс KUMA** (???? ????????????? **Создать алерты был активирован**).



????? ???????, ? ???? ??????????????? ???????? ??????? ???????????? ??????? ???? ???????? ??????? ????????? ??????? ????? ? ???-????????? KUMA, ??? ??????? ? ???????????? ??????? ??????????.

Revision #2
Created 2026-08-12 13:06:04 UTC by Dmitry Borisov
Updated 2026-08-12 14:04:57 UTC by Dmitry Borisov