Ретроспективная проверка

> 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/4.0/217979

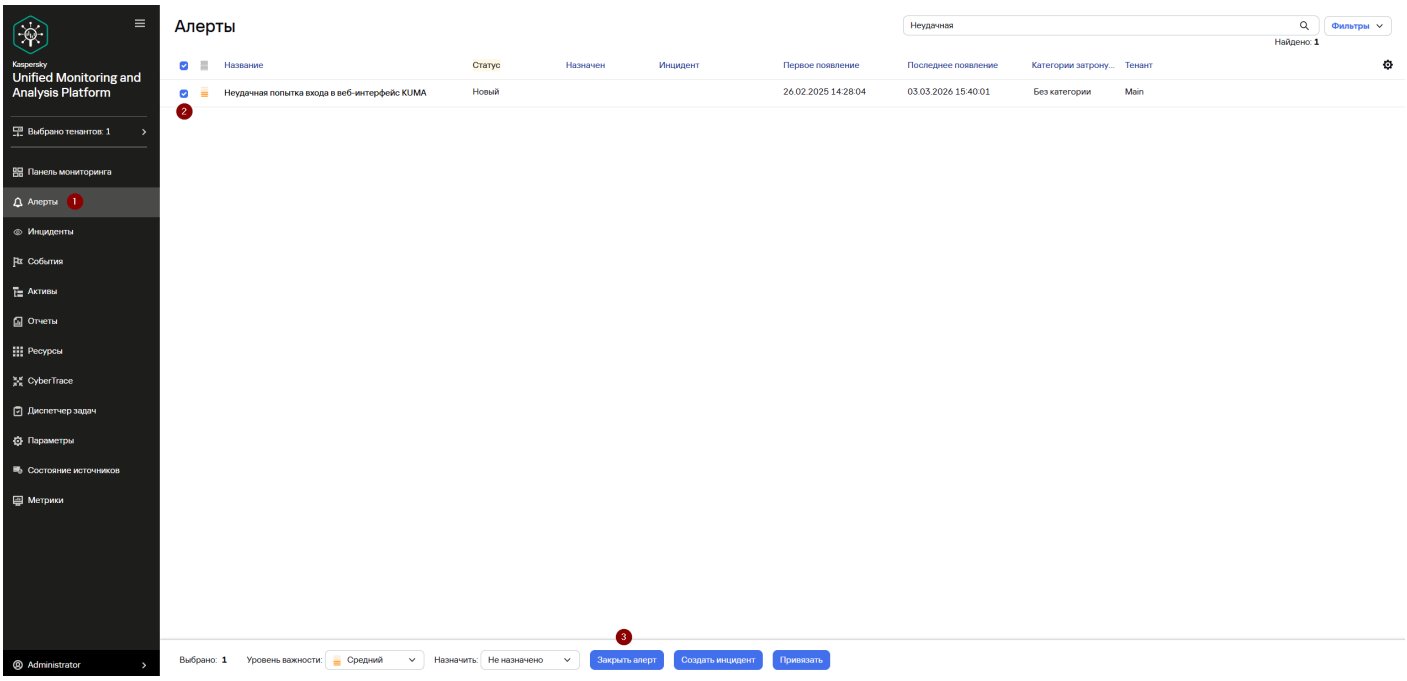
В обычном режиме коррелятор работает только с событиями, поступающими от коллекторов в реальном времени, выполняя потоковую корреляцию.

Ретроспективная проверка позволяет применять правила корреляции к историческим событиям, уже сохранённым в хранилище. Это удобно, если вы внесли изменения в существующие правила корреляции или загрузили новые и хотите проверить наличие вредоносной активности или инцидентов в ранее сохранённых событиях.

С помощью поискового запроса можно определить список исторических событий, для которых будет выполнена ретроспективная проверка, задать период поиска и указать хранилище, в котором следует искать события. Также можно настроить задачу так, чтобы во время ретроспективной проверки создавались алерты и применялись правила реагирования.

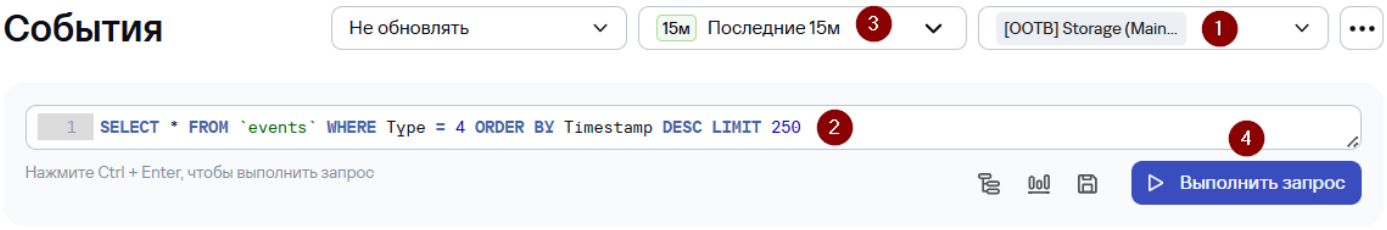
Для тестирования ретроспективной проверки:

- Создайте правило корреляции Неудачная попытка входа в веб-интерфейс KUMA (см. **Создание правила корреляции типа Simple**).
- Выполните неудачную попытку входа в веб-интерфейс KUMA.
- Перейдите в **Алерты** и закройте алерт **Неудачная попытка входа в веб-интерфейс KUMA** (при наличии).



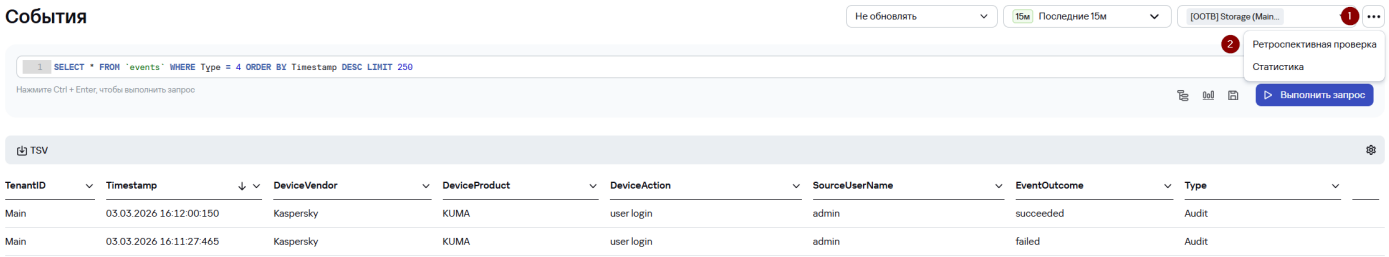
Чтобы выполнить ретроспективную проверку:

- Перейдите в раздел **События** и сформируйте необходимую выборку событий:
  - Выберите хранилище.
  - Укажите поисковый запрос.
  - Задайте необходимый временной период.
- Нажмите **Выполнить запрос**.



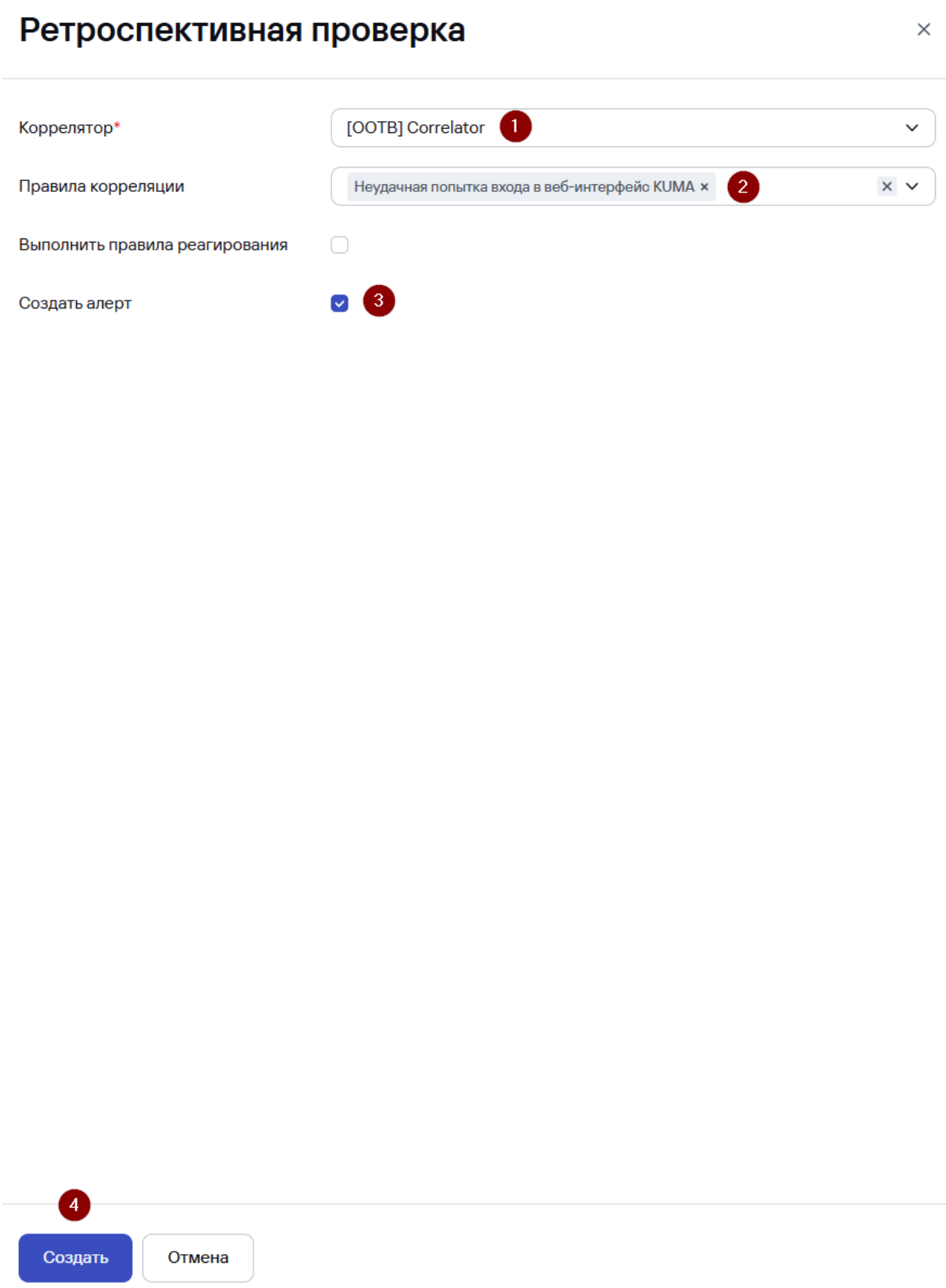

```
SELECT * FROM `events` WHERE Type = 4 ORDER BY Timestamp DESC LIMIT 250
```

- В раскрывающемся списке ⋯ выберите **Ретроспективная проверка**.



- В появившемся окне **Ретроспективная проверка**:
  - В раскрывающемся списке **Коррелятор** выберите сервис коррелятора, в который будут загружены выбранные события.

- В раскрывающемся списке **Правила корреляции** выберите правила корреляции, с помощью которых необходимо обработать выбранные события. Если на этом шаге не выбрано ни одного правила, проверка будет выполнена с применением всех правил корреляции.
- Если необходимо, чтобы в процессе обработки событий срабатывали правила реагирования, включите переключатель **Выполнить правила реагирования**.
- Если необходимо, чтобы в процессе обработки событий создавались алерты, включите переключатель **Создать алерты**.
- Нажмите на кнопку **Создать**.

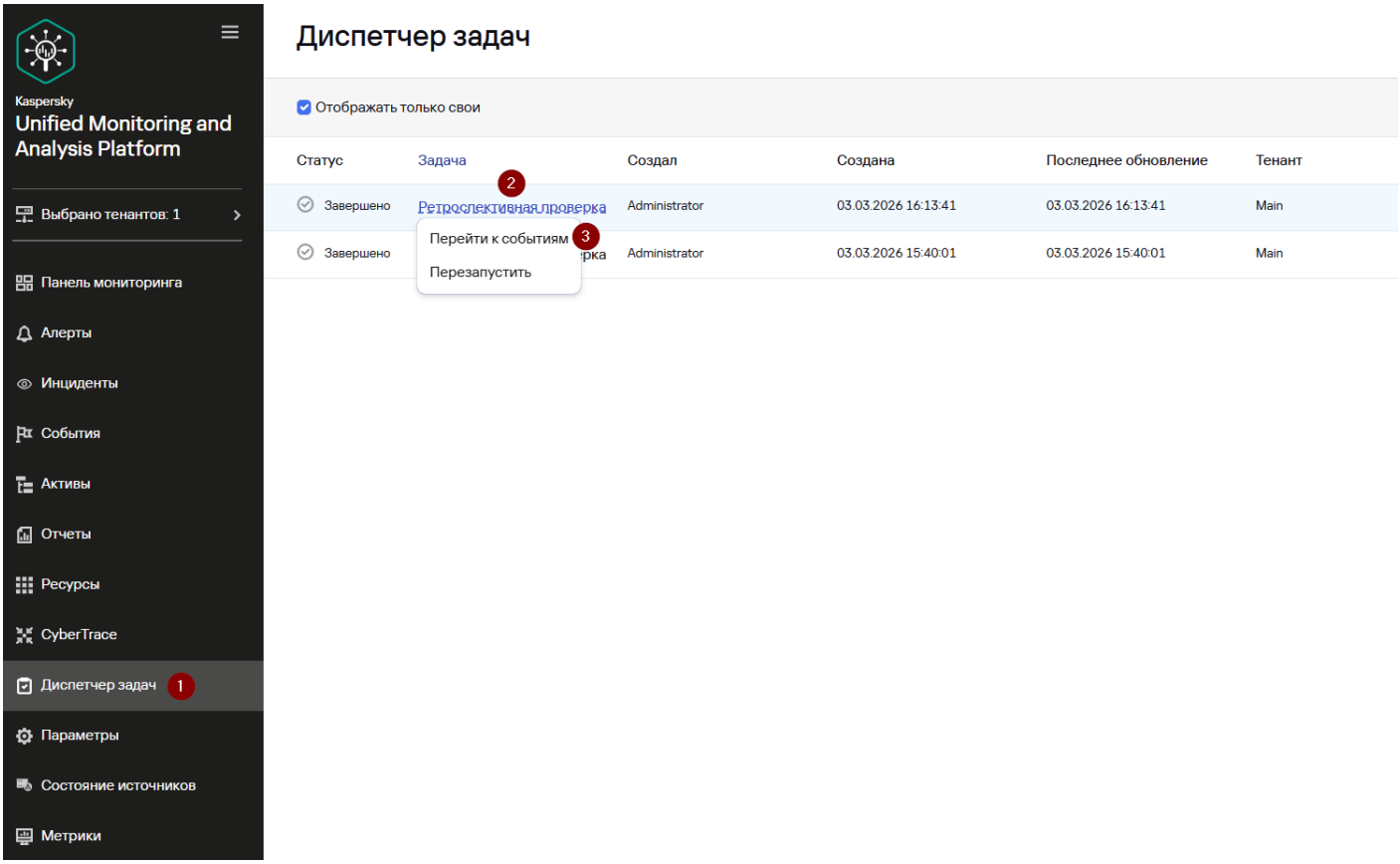


В разделе **Диспетчер задач** создана задача ретроспективной проверки.

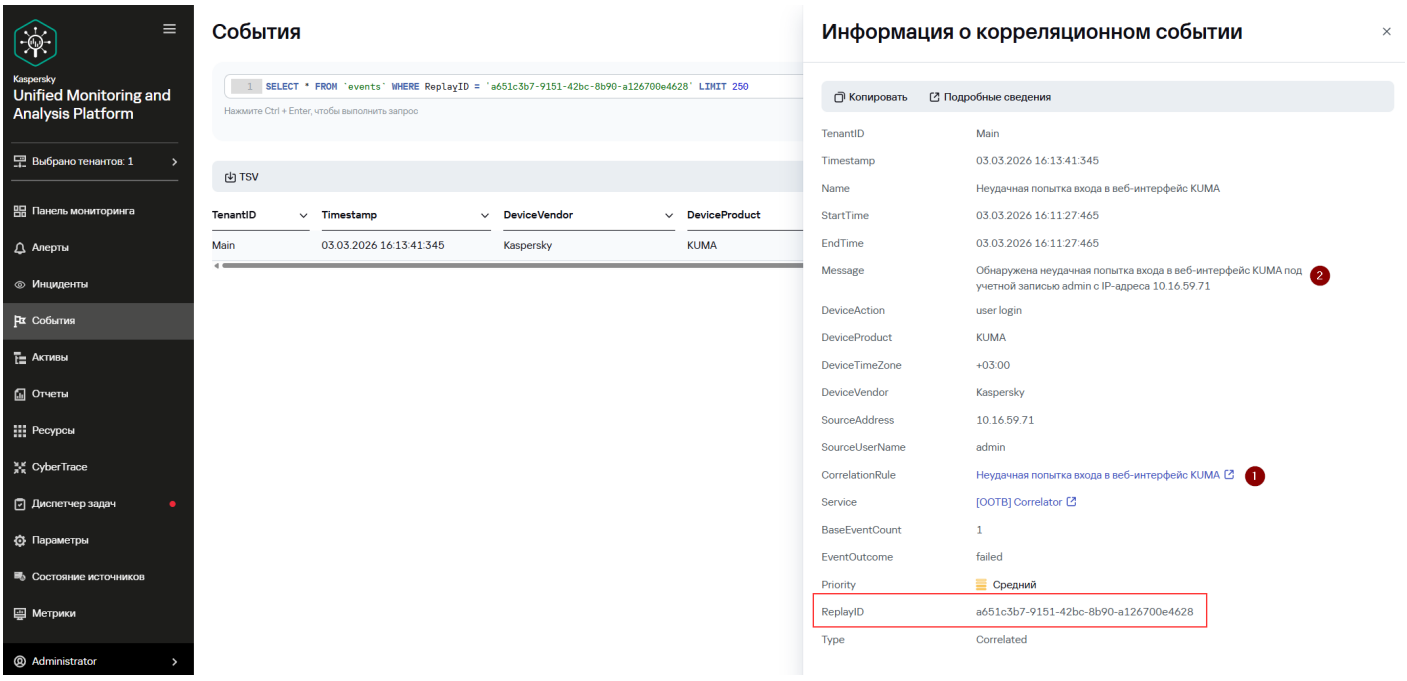
Чтобы просмотреть результаты проверки:

- Перейдите в **Диспетчер задач**.

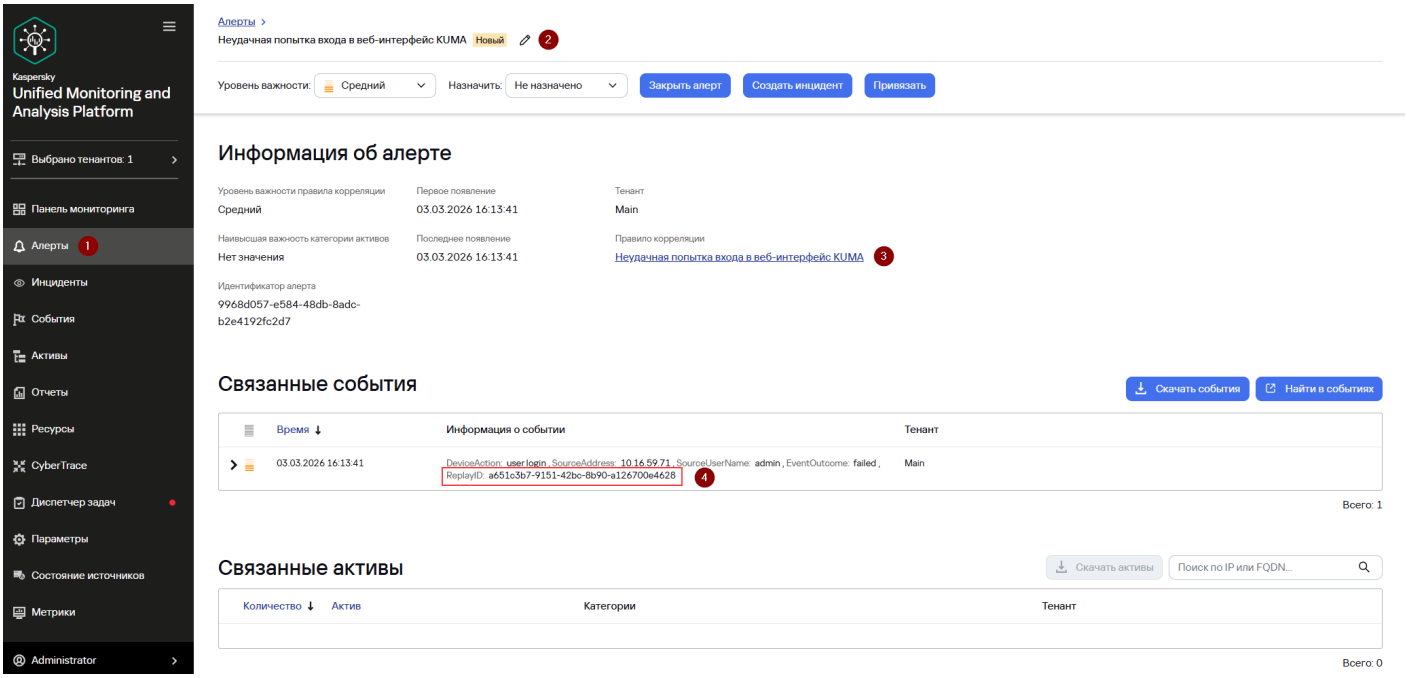
- Нажмите на созданную задачу **Ретроспективная проверка** и в раскрывающемся списке выберите **Перейти к событиям**.



- Откроется новая вкладка браузера с таблицей корреляционных событий, созданных в процессе ретроспективной проверки исторических событий. Корреляционные события, содержат дополнительное поле **ReplayID**, в котором хранится уникальный идентификатор выполнения ретроспективной проверки.



Также в ходе ретроспективной проверки будет создан алерт **Неудачная попытка входа в веб-интерфейс KUMA** (если переключатель **Создать алерты был активирован**).



Таким образом, в ходе ретроспективной проверки выборки исторических событий было выявлено событие неудачной попытки входа в веб-интерфейс KUMA, что привело к срабатыванию правила корреляции.

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