Работа с событиями

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

??????????? ???????????? ?? ??????? ??????? ????????? ? ??????-??????? ?? ???????: https://support.kaspersky.ru/kuma/4.0/228267

????? ??????????? ?????????? ??????? ?? ?????? ????????????? ?????????? KUMA ??????? ? ??????? **События** ???-?????????? KUMA.

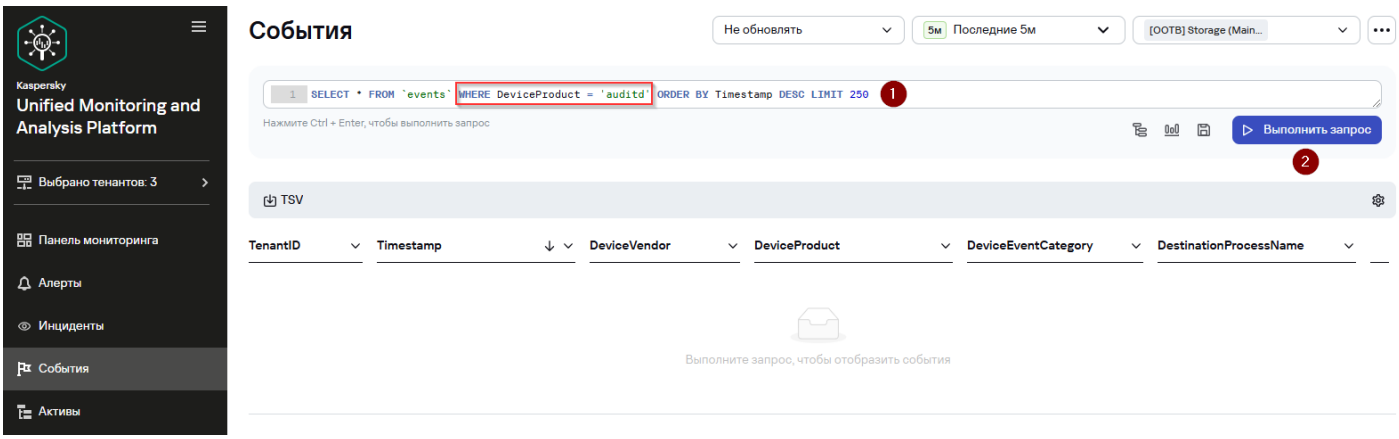
????? «?????? ? ?????????»: https://rutube.ru/video/61eaf7b9ba77f32ed778ed174a9693a9/?playlist=540937

Формирование SQL-запроса

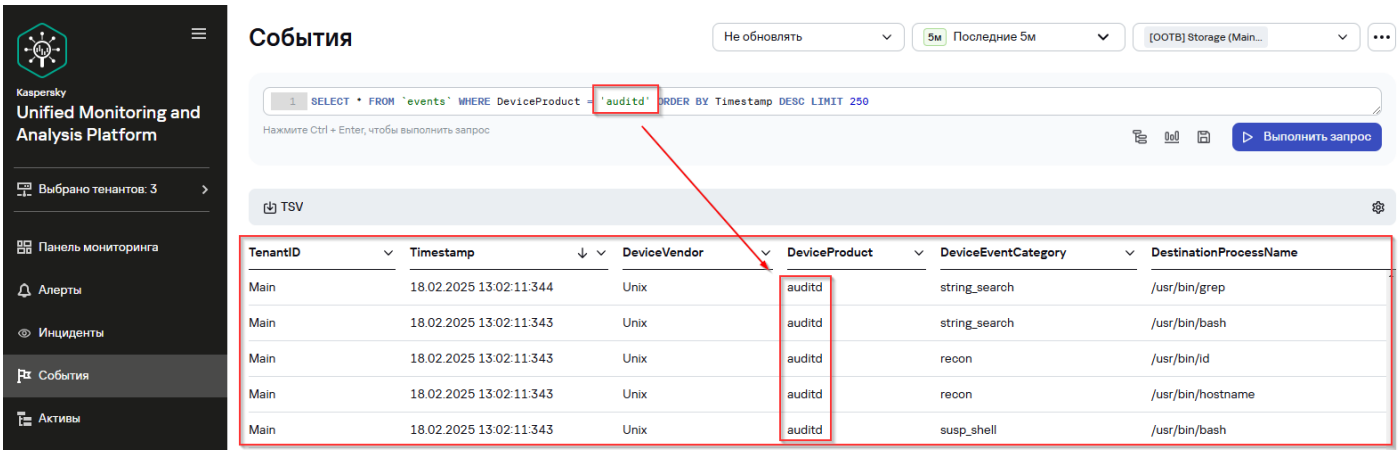
?? ????????? ? ??????? **События** ?????? ?? ????????????. ??? ????????? ??????? ? ???? ?????? ????? ?????? SQL-?????? ? ?????? ?? ?????? **Выполнить запрос**. SQL-?????? ????? ?????? ??????? ??? ???????????? ? ??????? **конструктора запросов.**

??? ???????? SQL-??????? ???????:

- ??????? SQL-?????? ? ???? ?????. ??????????? ????????? ??????? ? ????????.
- ??????? ?? ?????? **Выполнить запрос**.

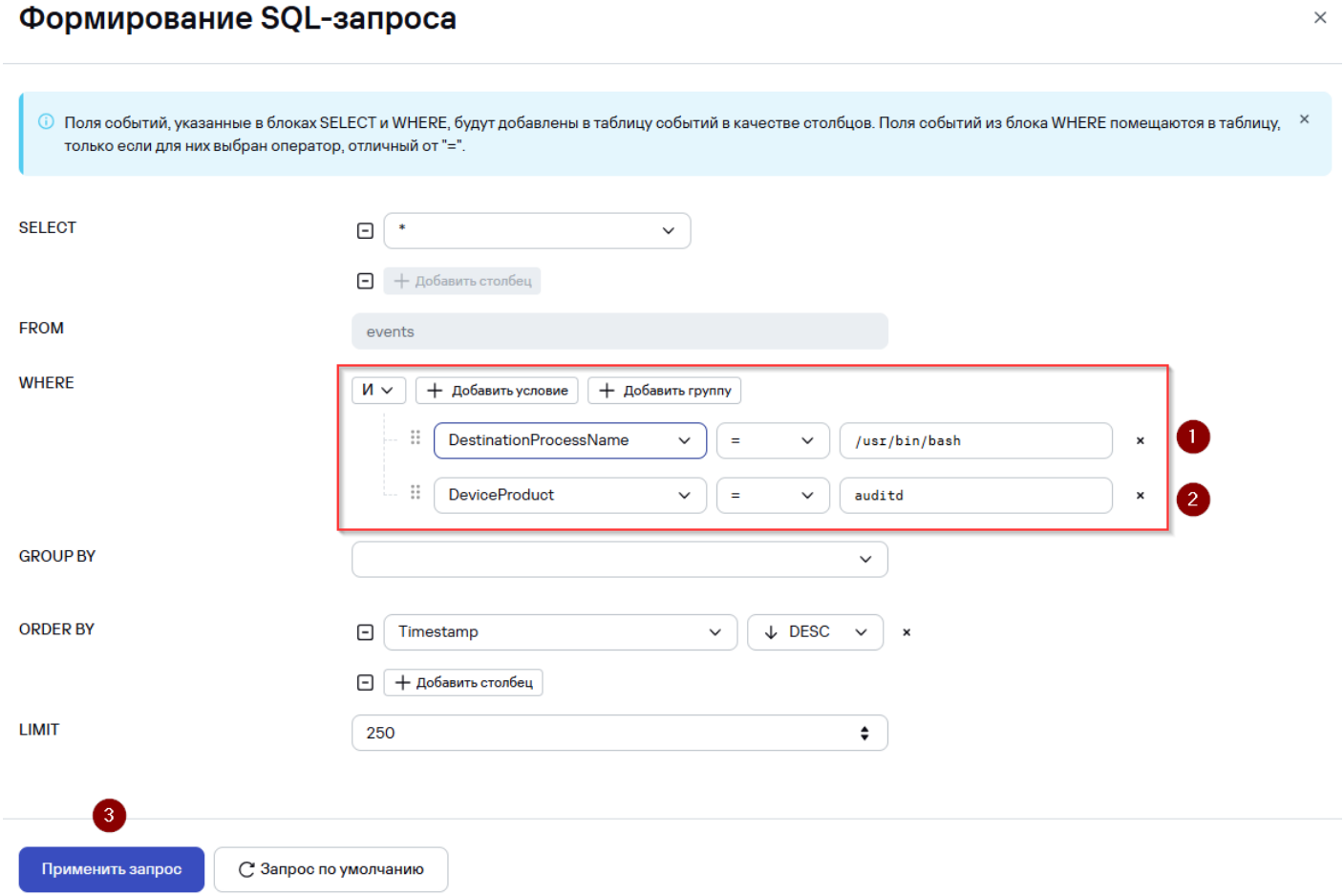


- ??????????? ??????? ???????, ?????????????? ???????? ?????? ???????.



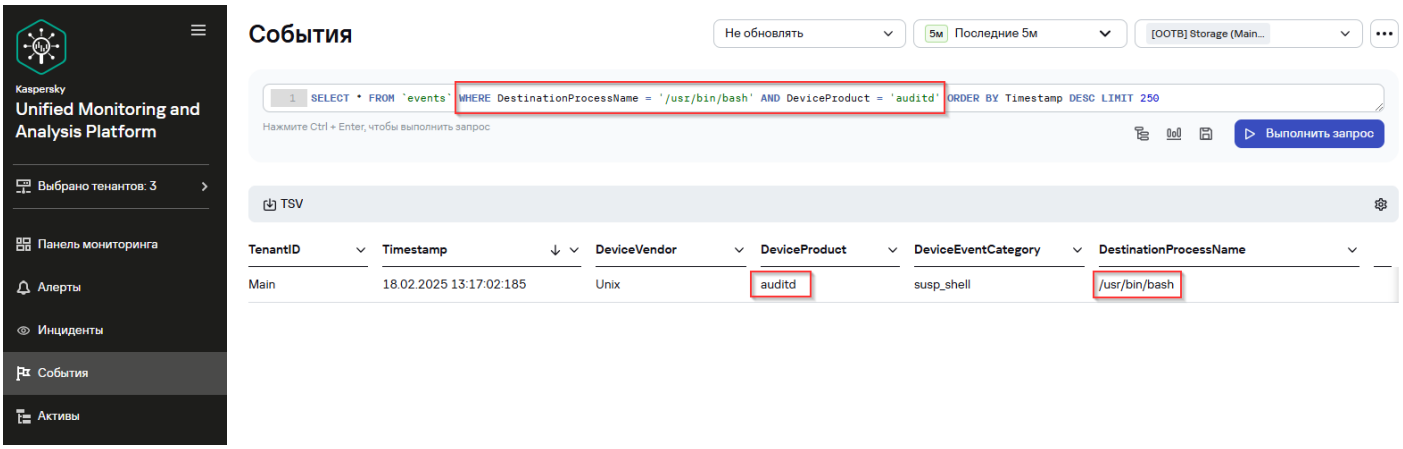
??? ???????? SQL-??????? с ??????? ????????????:

- ??????? ?? ?????? ..
- ? ??????????? ???? ???????????? ???????? ????????????? ????????? ??????.
- ??????? ?? ?????? **Применить запрос.**



- ??????? SQL-?????? ????? ???????????. ? ???? ?????? ??????????? ?????????????? SQL-??????.
- ??? ??????????? ?????? ? ??????? ??????? ?? ?????? **Выполнить запрос**.

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



Примеры запросов

```
SELECT * FROM `events` WHERE Type IN ('Base', 'Audit') ORDER BY Timestamp DESC LIMIT 250
```

??? ??????? ??????? events ? ????? Base ? Audit, ?????????????? ?? ??????? Timestamp ? ??????? ????????. ?????????? ???????????? ? ??????? ????? – 250.

```
SELECT * FROM `events` WHERE BytesIn BETWEEN 1000 AND 2000 ORDER BY Timestamp ASC LIMIT 250
```

??? ??????? ??????? events, ??? ??????? ? ???? BytesIn ???????? ?????????? ??????? ????????? ? ????????? ?? 1000 ?? 2000 ????, ?????????????? ?? ??????? Timestamp ? ??????? ??????????. ?????????? ???????????? ? ??????? ????? – 250.

```
SELECT * FROM `events` WHERE Message LIKE '%ssh:%' ORDER BY Timestamp DESC LIMIT 250
```

??? ??????? ??????? events, ??????? ? ???? Message ???????? ??????, ?????????????? ????????? ??????? %ssh:% ? ?????? ????????, ? ????????????? ?? ??????? Timestamp ? ??????? ????????. ?????????? ???????????? ? ??????? ????? – 250.

```
SELECT * FROM `events` WHERE inSubnet(DeviceAddress, '00.0.0.0/00') ORDER BY Timestamp DESC LIMIT 250
```

??? ??????? ??????? events ??? ??????, ??????? ?????? ? ??????? 00.0.0.0/00, ?????????????? ?? ??????? Timestamp ? ??????? ????????. ?????????? ???????????? ? ??????? ????? – 250.

```
SELECT * FROM `events` WHERE match(Message, 'ssh.*') ORDER BY Timestamp DESC LIMIT 250
```

??? ??????? ??????? events, ??????? ? ???? Message ???????? ?????, ?????????????? ??????? ssh.*, ? ????????????? ?? ??????? Timestamp ? ??????? ????????. ?????????? ???????????? ? ??????? ????? – 250.

```
SELECT max(BytesOut) / 1024 FROM `events`
```

???????????? ?????? ?????????? ??????? (??) ?? ????????? ?????? ???????.

```
SELECT count(ID) AS "Count", SourcePort AS "Port" FROM `events` GROUP BY SourcePort ORDER BY Port ASC LIMIT 250
```

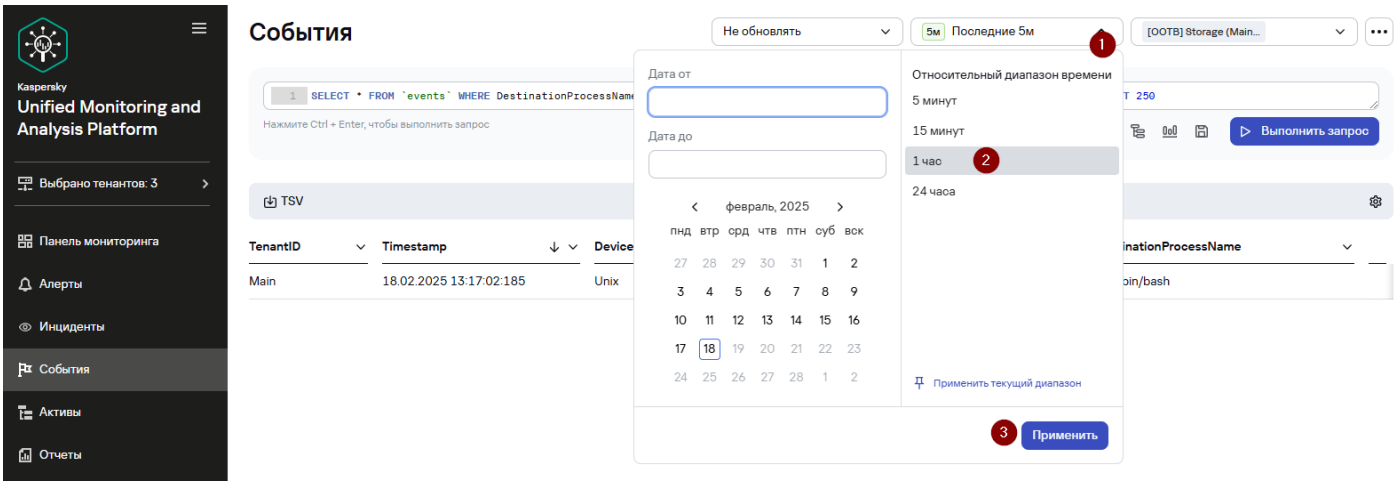
?????????? ??????? ? ????? ?????. ??????? ????????????? ?? ?????? ????? ? ????????????? ?? ??????? Port ? ??????? ??????????. ?????????? ???????????? ? ??????? ????? – 250. ??????? ID ? ??????? ??????? ????????? ??? Count, ??????? SourcePort ????????? ??? Port.

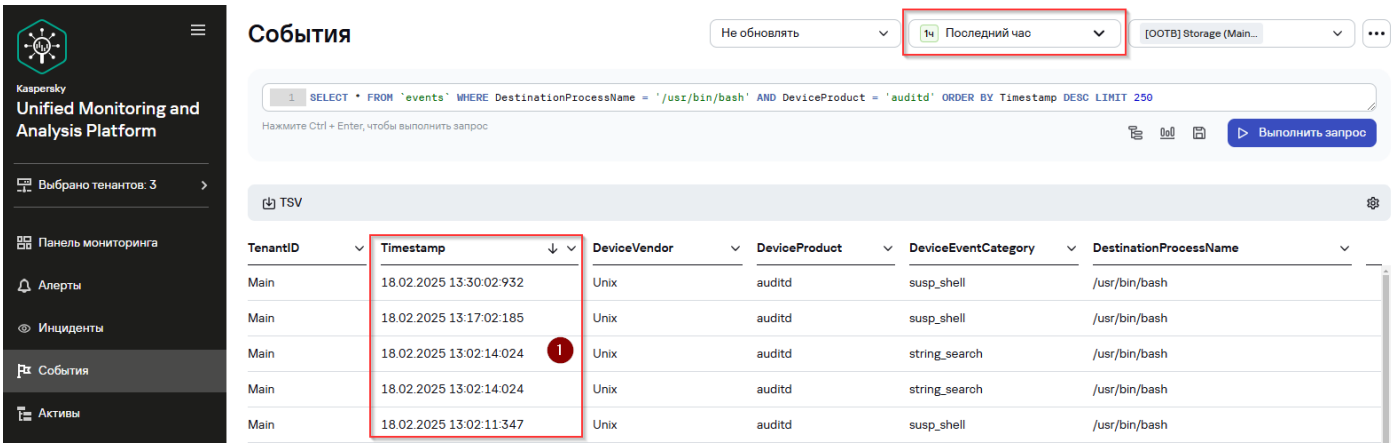
Фильтрация событий по периоду

? KUMA ?? ?????? ????????? ??????????? ???????, ??????????? ? ???????????? ????????? ???????. ? ?????????? ???????? ????? ??????? ?????????? ?? ????????? 5 ????? (???????? ?? ?????????).

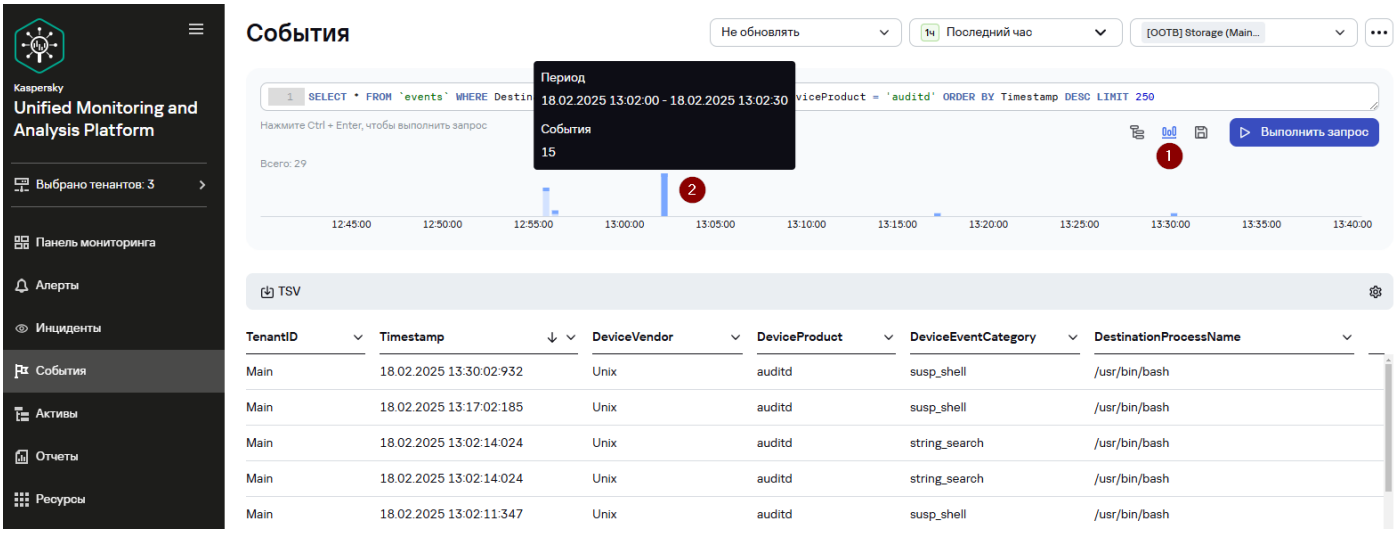
????? ????????????? ??????? ?? ???????:

- ? ??????? **События** ???-?????????? KUMA ? ??????? ????? ???? ???????? ????????????? ?????? ?????????? ???????.
- ????????? ???? ?? ????????? ????????, ????? ??????? ????????? ??????:
  - ???? ?? ?????? ????????? ?????????? ?? ????????????? ?????????? ???????, ???????? ???? ?? ????????? ????????? ???????? ? ????? **Относительный диапазон времени** ??????. ????????, ?? ?????? ??????? ????????? ?????? 5 ?????, 15 ?????, 1 ???, 24 ????.
  - ???? ?? ?????? ????????? ?????????? ?? ?????????? ?????????? ???????, ? ????????? ????? ???????? ???? ?????? ? ????????? ??????? ? ??????? ?? ?????? **Применить**. ?????? ???? ? ??????? ??????? ?? ???????? ????? ???????????? ???????. ??? ????????????? ?? ????? ?????? ??????? ???????? ???? ??????? ? ????? **Дата от** ? **Дата до**.
- ??????? ?? ?????? **Выполнить запрос**.





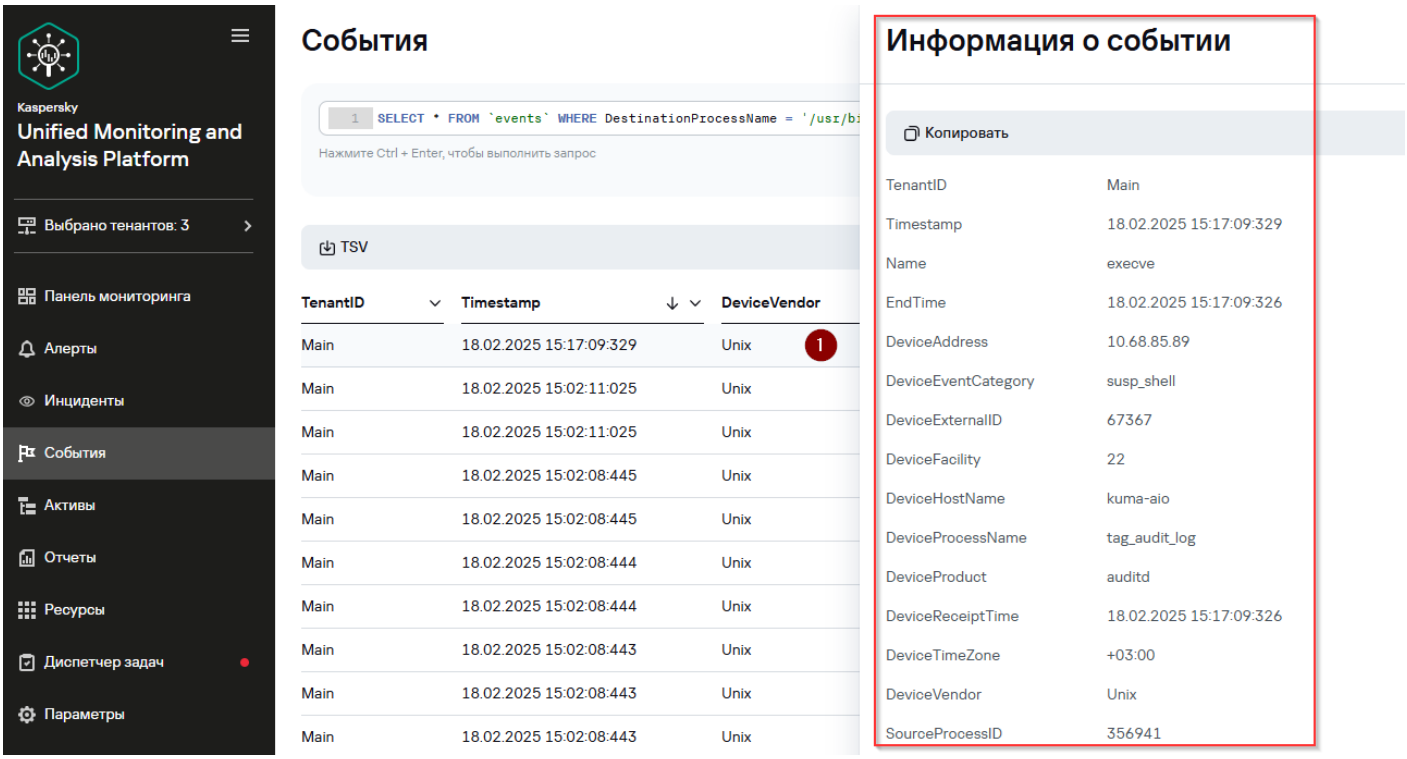
?? ????? ?????? ????????? ??????????? ??????? ? ??????? **гистограммы событий**, ??????? ???????????? ??? ??????? ?? ?????? ? ??????? ????? ??????? **События**. ??????? ???????????, ???? ?????? ?? ?????? ??????? ?????? ??? ???????? ????????? ?????? ??????? ? ?????? ?? ?????? **Показать события**.



Просмотр информации о событии

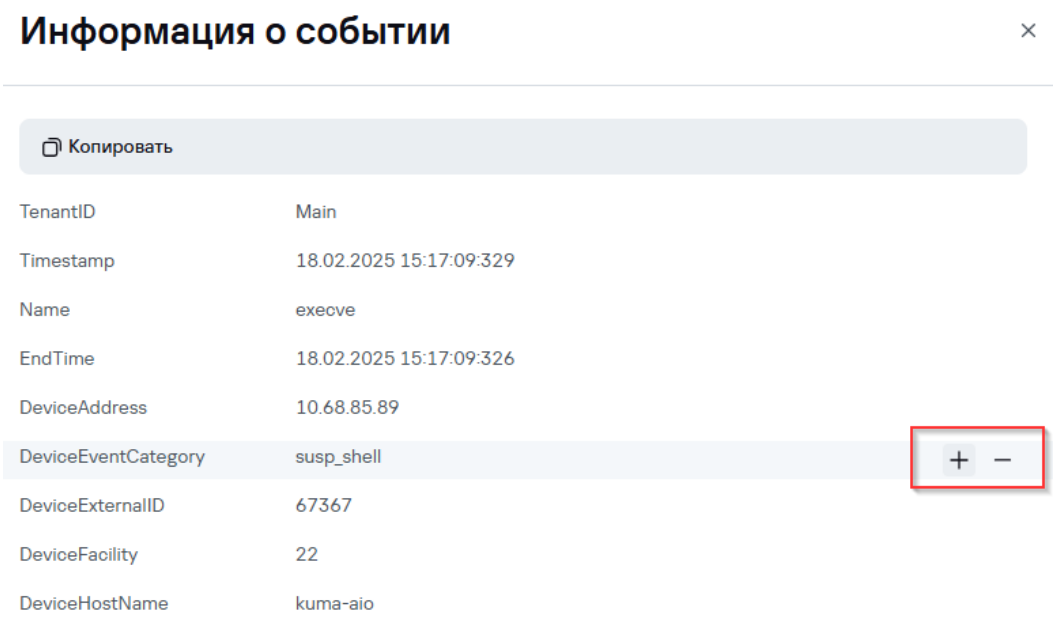
????? ??????????? ?????????? ? ??????? (???????? ???????):

- ? ??????? ??????? ???????? ???????, ?????????? ? ??????? ?? ?????? ???????????.
- ????????? ???? **Информация о событии** ?? ??????? ????? ??????? ? ?? ????????.



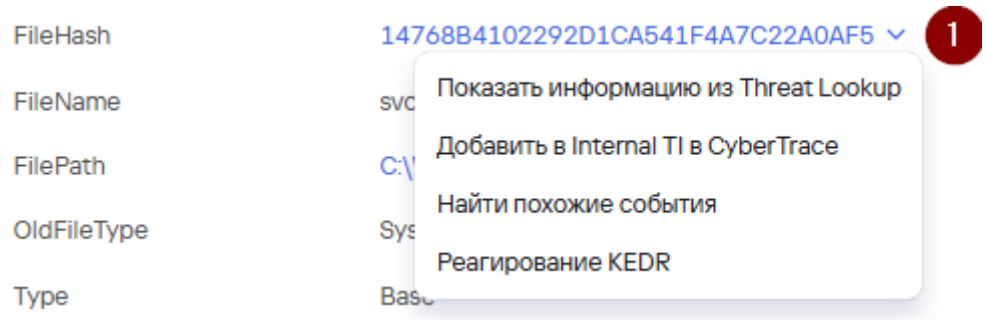
? ???? **Информация о событии** ???????? ????????? ????????:

- ???????? ????????? ???? ? ????? ??? ????????? ??? ?? ??????, ????? ?? + ??? − ????? ?? ????????? ????.



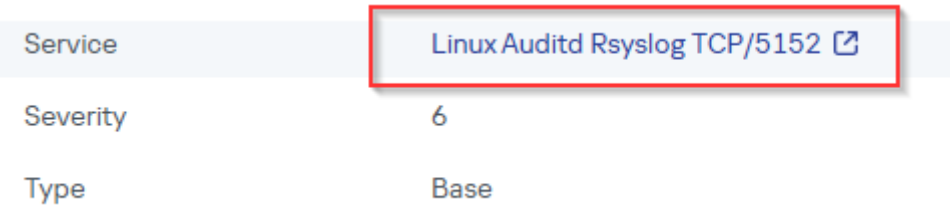
- ?? ???? ????? ? ????? **FileHash** ??? **OldFileHash** ???????? ??????, ? ??????? ????? ??????? ???? ?? ????????? ????????:

- ???????? ?????????? ? ????? ?? Threat Lookup (???????? ??? ?????????? ? Kaspersky Threat Intelligence Portal. ??. ?????? ?????????? ? Kaspersky Threat Intelligence Portal).
- ???????? ? Internal TI CyberTrace (???????? ??? ?????????? ? Kaspersky CyberTrace. ??. ?????? ?????????? ? Kaspersky CyberTrace).



- ????? ??????? ??????? (? ?????? ?????? ????? ????????? ??????? ???? FileHash = '<???????? ???-?????>' OR OldFileHash = '<???????? ???-?????>')

- ??????? ???? ?? ?????????? ?? ??????, ???? ??????? ????????? ??????????? ?? ?????? (??. ?????? ?????????? ? Kaspersky Security Center).
- ??????????? ????????? ???????, ????????????? ???????, ??????? ?? ?????? ? ?????? ?????????? ? ???? Service.



??? ????????? ????????? ??????? ? ??????? ????? ?????????????? «???????? ?????????» - ??????? ????/?????.

Настройка таблицы событий

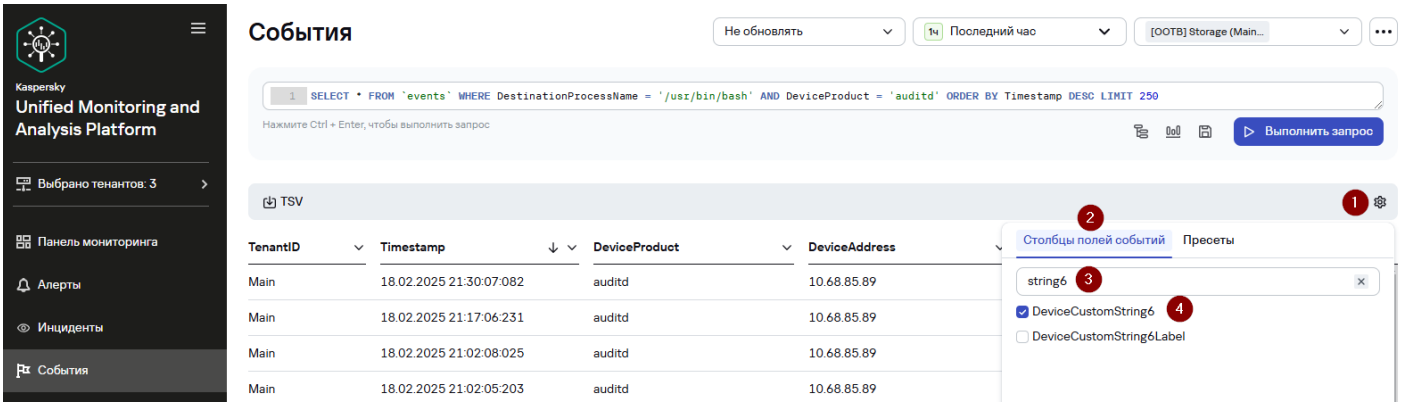
? KUMA ????????????? ????????? ???????????? ?????? ???????? ????? ??????? ? ??????? ?? ??????????? (**пресет**). ????????? ???????????? ???????? ????? ?????????.

????????, ??????????, ????? ??? ??????? Linux ?????? ???????????? ??????? ????? TenantID, Timestamp, DeviceProduct, DeviceAddress, DeviceEventCategory, DestinationProcessName ?

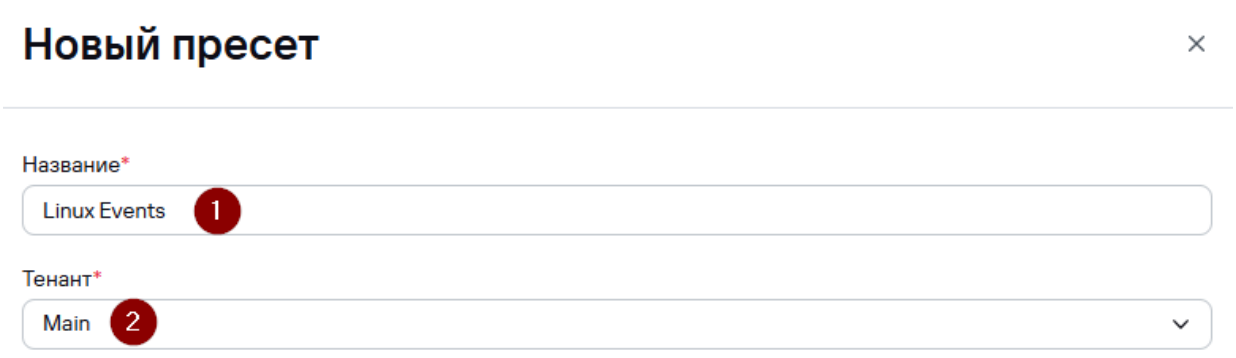
DeviceCustomString6.

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

- ? ??????? **События** ??????? ?? ?????? .
- ? ??????????? ???? ?? ??????? **Столбцы полей событий** ???????? ??????????? ???? (??. ????). ??? ????????? ?????? ????? ?????? ???????? ???????? ???? ? ??????? **Поиск**.



- ????? ????????? ????????? ????, ??????? **Сохранить текущий пресет.**
- ? ??????????? ???? **Новый пресет** ??????? **Название пресета** ? ???????? **Тенант** ? ????????????? ??????.



- ??????? **Сохранить**.

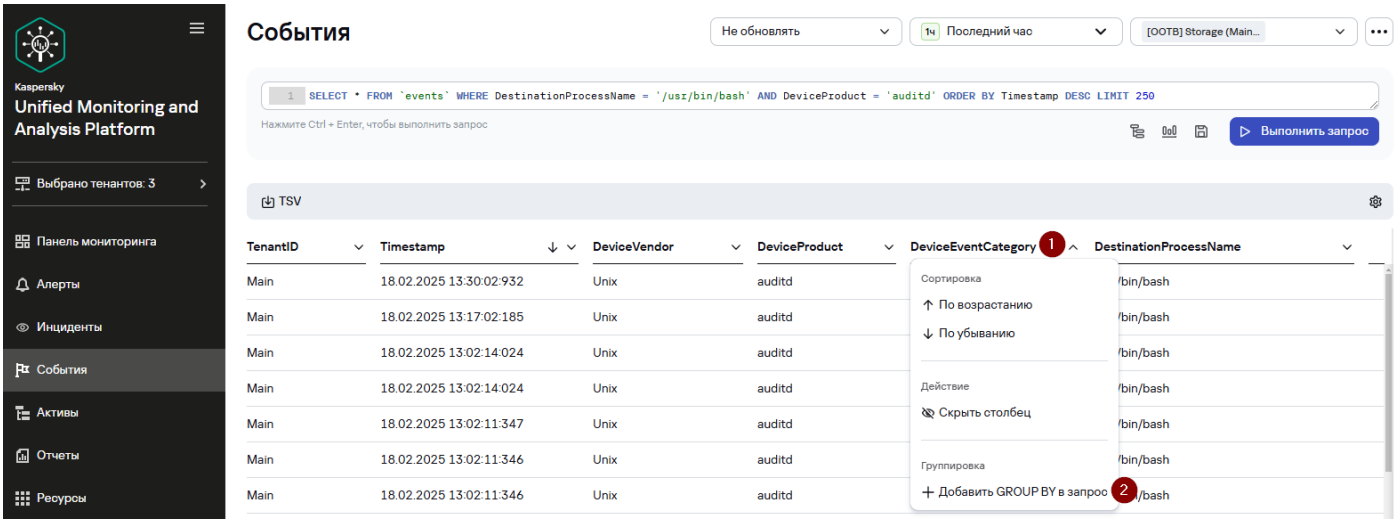
?????? ?????? ? ????????. ??????????? ??????? ???????? ??? ??????? ?? ?????? ?? ??????? **Пресеты**.

Группировка событий

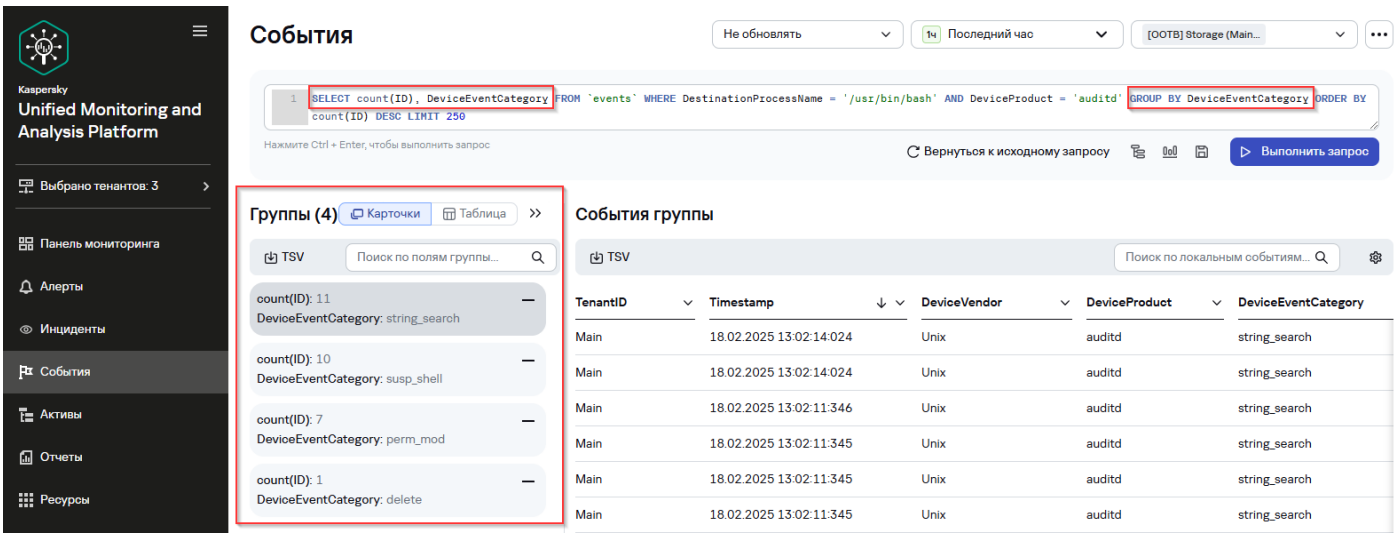
????? ????????? ?????? ??????? ????? ????????? ??????????? ????????? ?????????? ??????? ?? ???????, ????? ???????????? ??????? ?????????????? ????????????. ? KUMA ???? ?????????? ????????????? ??????? ?? ?????? ??? ?????????? ????? ??? ?????????? ?????? ???????.

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

- ? ??????? **События** ??????? ?? ????????? ???????, ?? ???????? ?????????? ????????? ??????????? ? ? ??????????? ???? ???????? **Добавить GROUP BY в запрос**. ?? ?????? ??????? ?????????????? ????????? ???????? ??? ???????????, ???? ????? ????????????? ????????? ? ?????? ???????.



- ????? ???? ??? ?? ??????? ?????? ???????, ??????? **Выполнить запрос**. ? ?????????? ????? ????????? ??????????? ??????? ?? ???????? ?????. ????????? ?????? ????? ???????????? ? ??????? **Группы**.



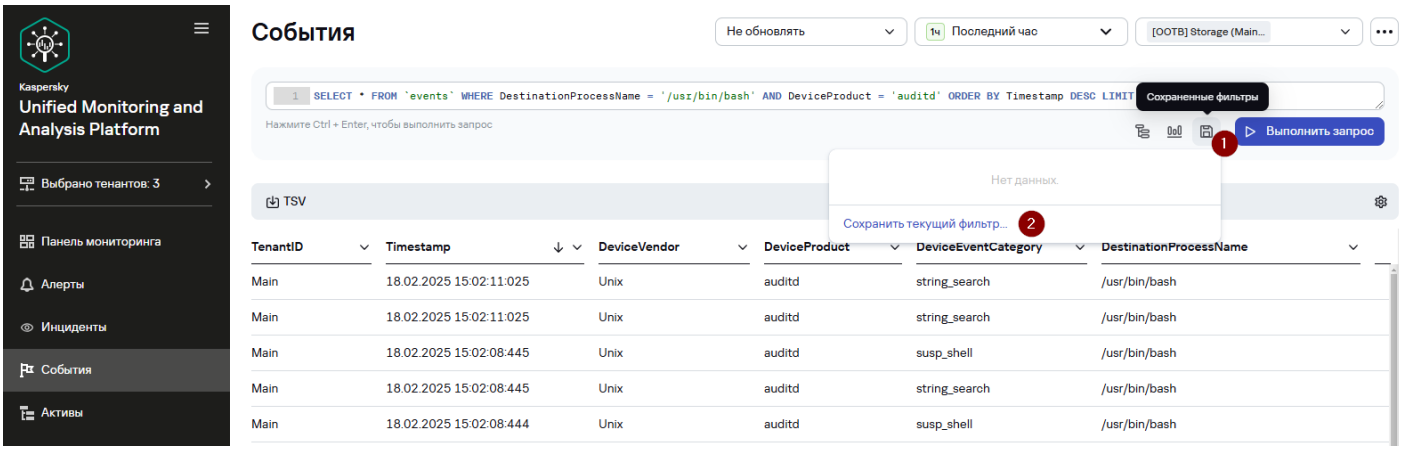
?????????? ???????? ? ???? ??????? ? ? ???? ????????. ?? ?????? ???????????? ????? ???????? ???????????. ????? ?????????? ?? ??????? ? ???????????? ?????????? ?????? ??????.

Фильтры

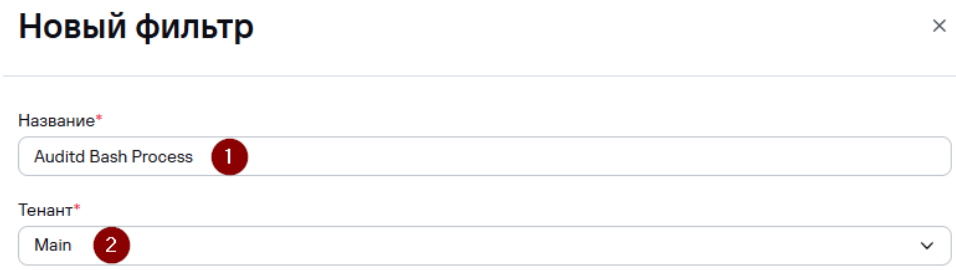
??? ?????????? ????? ???????????? ????????? ???????? ???????????? ???????? ????????. ??? ?????????? ??????? ???????????? ????? **настроенные параметры поискового запроса**: ?????? ?? ???????, ???????????? ???????? ? ???????????? ??????? ????? ???????.

????? ????????? ??????? ????????? ???????, ??????? ? ???????:

- ? ??????? **События** ??????? ?? ??????  ? ???????? **Сохранить текущий фильтр**.



- ? ?????????? ???? ? ???? **Название** ??????? ???????? ???????.
- ? ?????????????? ?????? **Тенант** ????????? ??????, ???????? ????? ???????????? ?????????? ??????.
- ??????? **Сохранить**.



???????????? ??????? ?????????.

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

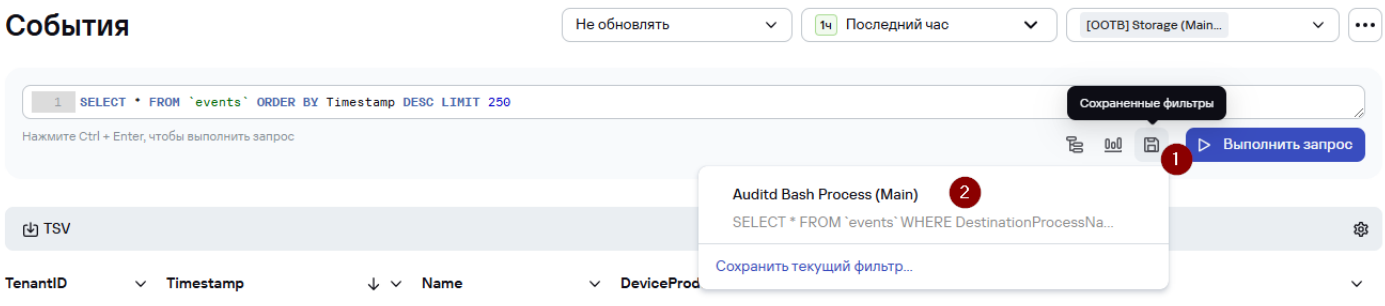
- ????????? ????????? ?????? ?? ?????????

```
SELECT * FROM `events` ORDER BY Timestamp DESC LIMIT 250
```

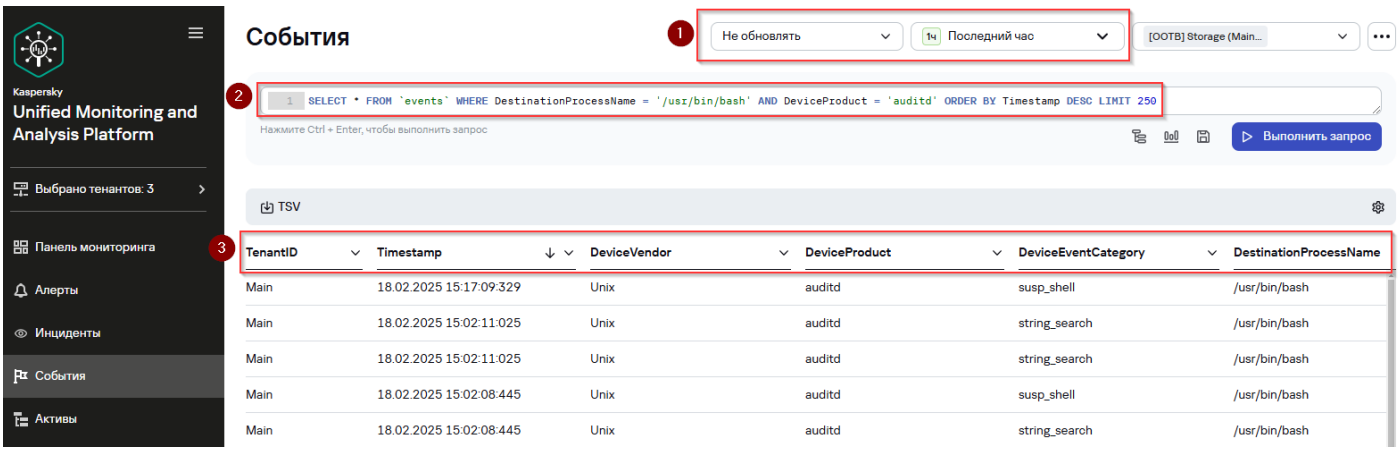
- ??????? ?? ?????? ? ????????? ?? ??????? **Пресеты.**
- ??????? ?? **Пресет по умолчанию.**
- ???????? ????????? ?????????? ????????? ?? **5 минут.**
- ????? ???????? ????? ???????, ??????? ???????, ????????? ???????? ???????? ? ???? ?? ?????????.

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

- ? ??????? **События** ??????? ?? ?????? ? ???????? ?????? ??????.



- ????????? ???????????? ??????? ?????? ???????: ? ???? ?????? ?????????? ?????????? ????????? ??????, ? ??????? ????? ???? ?????????? ?????????? ????????? ???????, ??????? ?????????? ?????????? ??????.
- ??? ???????? ?????????? ??????? ??????? ?? ?????? **Выполнить запрос**.



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

???? ?????? ?? ?????? ☆ ????? ? ????????? ??????????? ???????????? ???????, ?????? ?????? ?????? ?????????????? ? ???????? ??????? ?? ?????????.

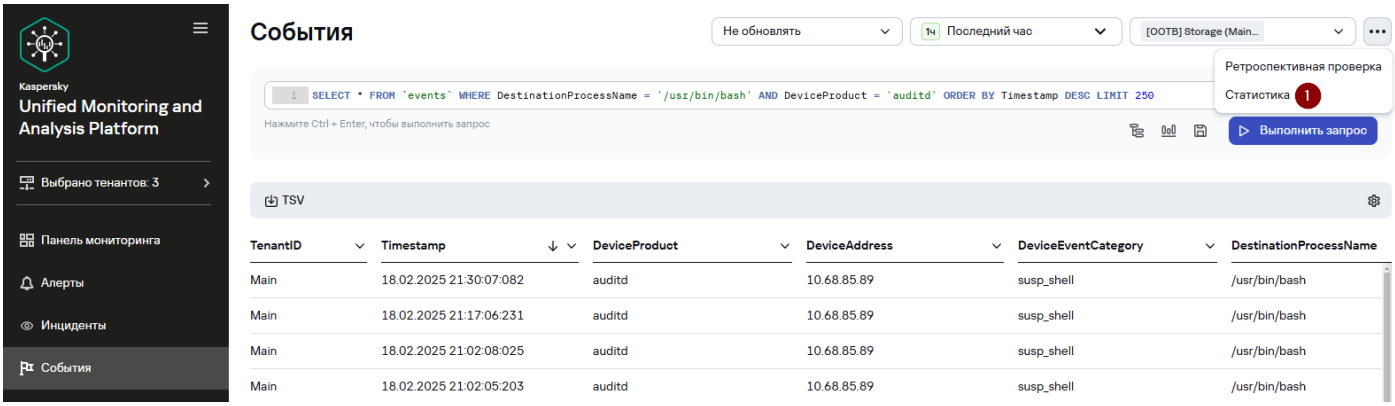
?????? ???????????? KUMA ????? ????? ???????????? ??????????? ??????? ??? ???????, ??? ? ??? ???? ?????????????? ????? ???????.

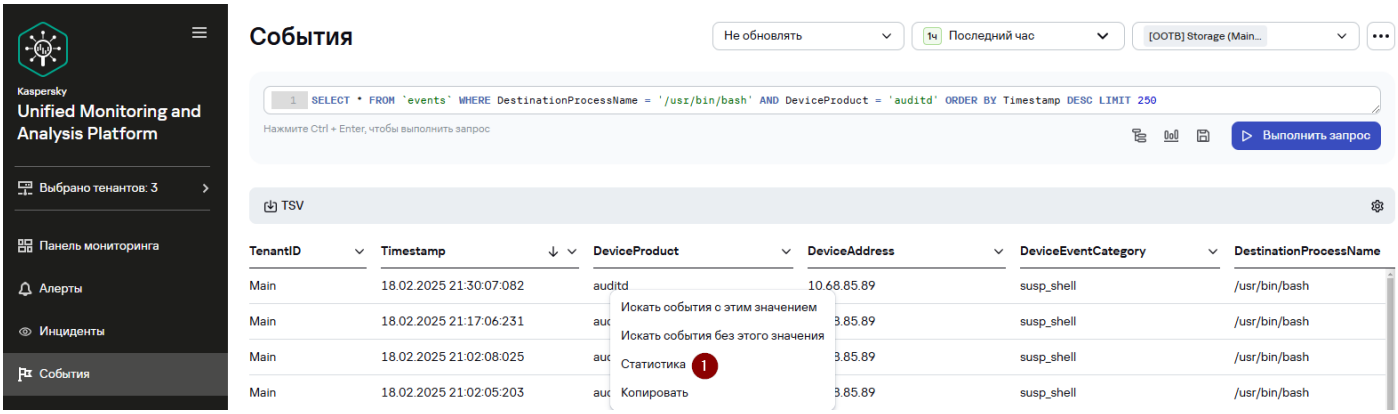
Получение статистики по событиям в таблице

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

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

- ? ??????? **События** ? ?????? ??????? ???? ??????? ??????? ? ?????????????? ?????? ⋯ ???????? **Статистика** ??? ? ??????? ??????? ??????? ?? ????? ???????? ? ? ??????????? ??????????? ???? ???????? **Статистика**



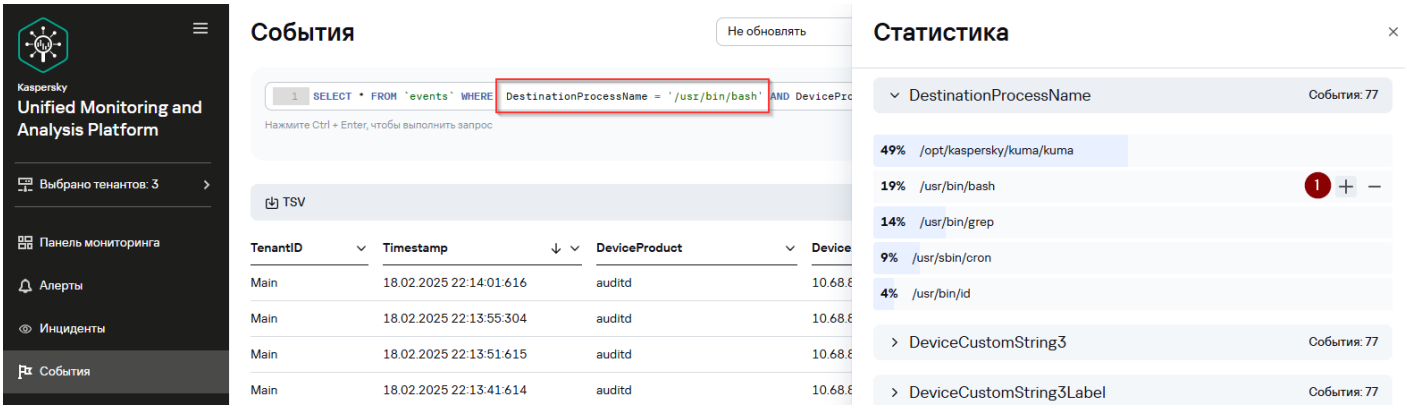


- ? ??????????? ???? ?????? ??????????? **статистика** ?? ??????? ????? ??????? ??????? ???????. ????? ????? ??????? ???? ????????? ?? ?????????? ??????? ? ??????? ? ?????? ?????. ??? ????????? ???? ???????????? ???? ???????? ??????

????????. ? ??????? ???? **Поиск** ????? ????? ????? ?????? ????.



??? ??????? ?? + ??? − ???????? ???????? ????? ????????? ???????? ???? ? ????????? ?????? ? ???????? ??????? ?????? ???????.

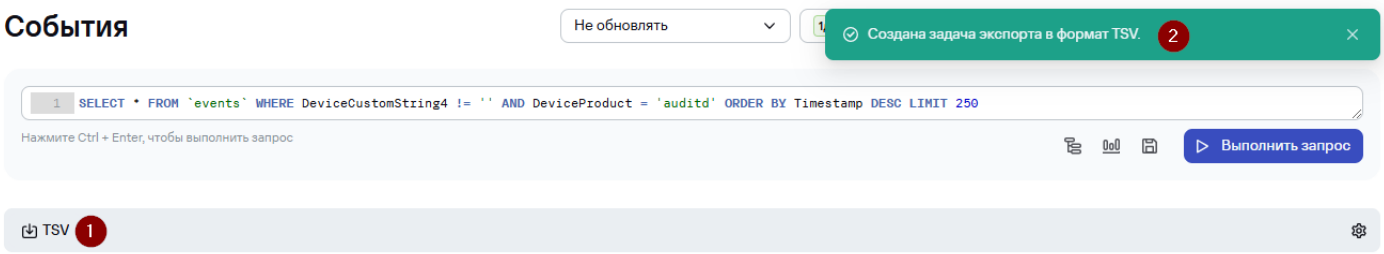


Экспорт событий

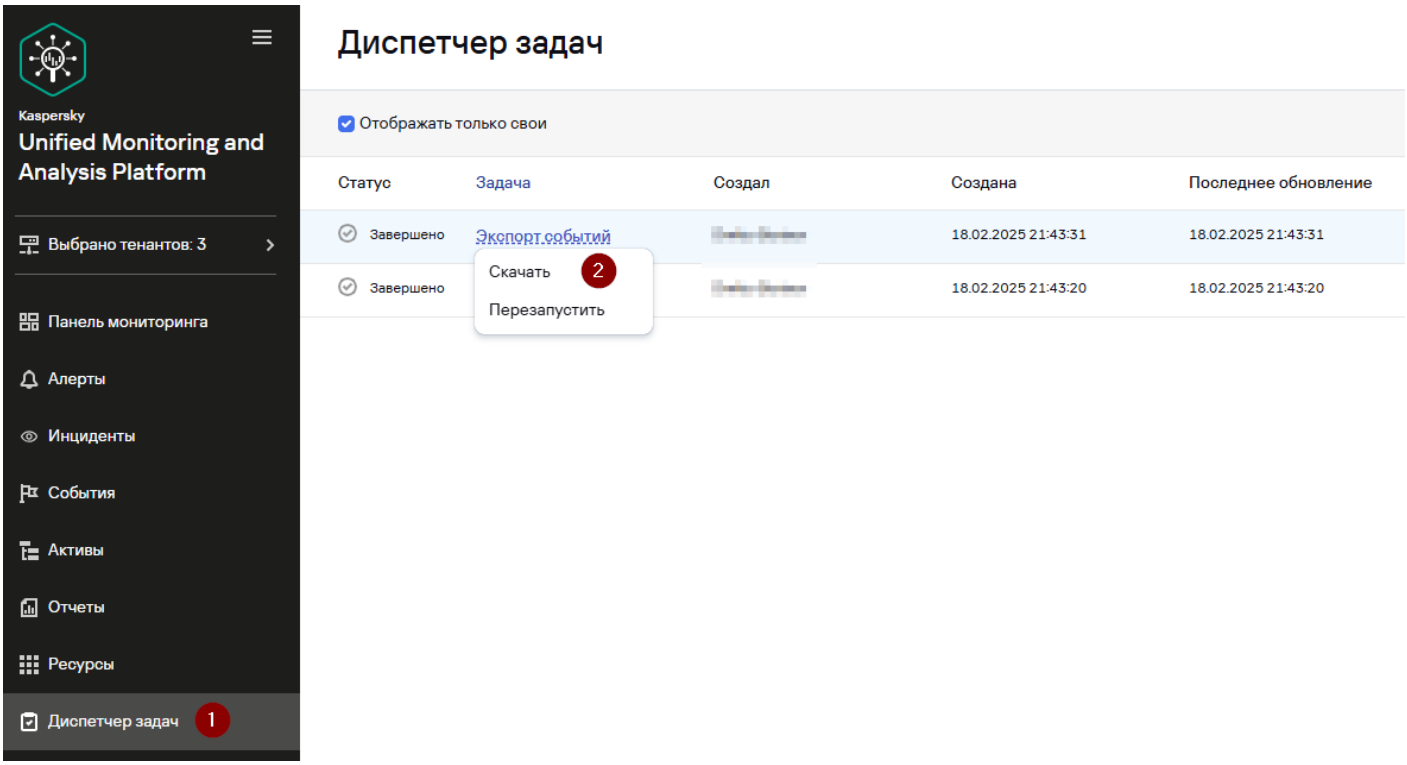
?? KUMA ????? ?????????????? ?????????? ? ???????? ? TSV-????. ??????? ???????, ??????? ????? ?????????????? ? TSV-????, ??????? ?? ????????????? ?????????? ??????? ? ????????? ???????. ?????????? ?????????????? ?? ????????, ??????? ? ?????? ???????? ??????????? ? ??????? ???????.

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

- ? ??????? **События** ??????? ?? ?????? TSV .
- ????? ????? ? ??????? **Диспетчере задач** ????? ??????? ????? ?????? ???????? TSV-?????.



- ??????? ????????? ?????? ? ??????? **Диспетчер задач**.
- ????? ???? ????? ????? ? ????????, ? ?????? ?????? ? ??????? **Статус** ?????????? ?????? **Завершено** ? ?????? .
- ??????? ?? ???????? ???? ?????? ? ? ????????????? ?????? ???????? **Загрузить**.



- TSV-???? ? ??????????? ? ???????? ????? ???????? ? ????????????? ???????? ?????? ????????. ??? ????? ?? ?????????: `event-export-<date>_<time>.tsv.`

Revision #17
Created 2026-06-11 13:00:54 UTC by lerat
Updated 2026-08-07 13:14:48 UTC by Dmitry Borisov