Простое правило (simple)

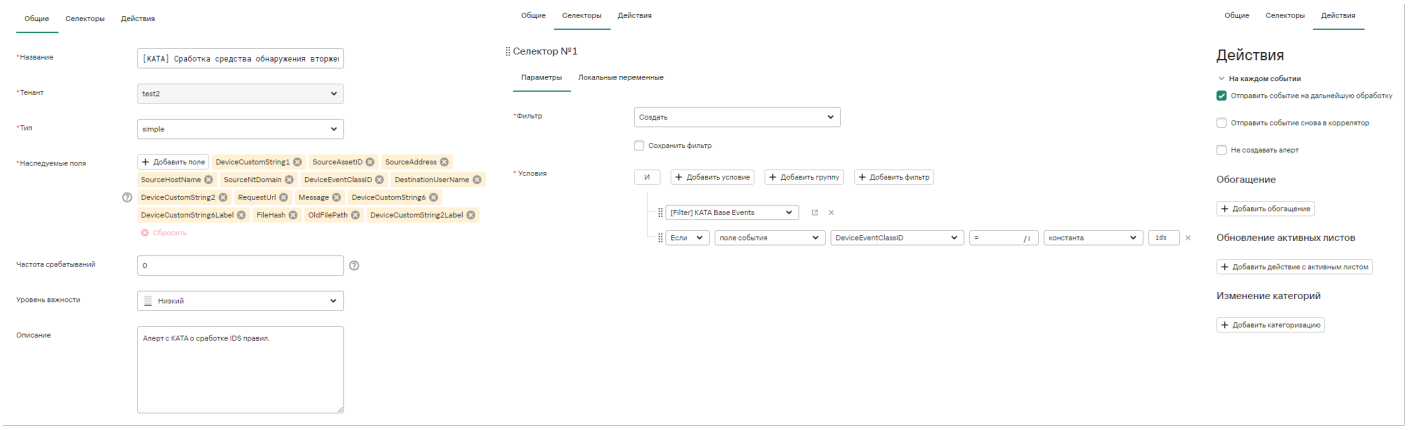
?????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? ?? ???????? ??????????? ????????????? ???????.

??????????? ???????????? ?? ??????? ??????? ????????? ? ??????-??????? ?? ???????: https://support.kaspersky.ru/kuma/4.0/221199

????? ???????? ?????? ?????????? ? ???????? ?? ??????????? ??? ???????? ????????? ? ??????? ?????????? ?????????? ????????? "**Обновление параметров**" ???????????.

Простое правило (simple) — ??????????? ??? ??????????? ??????? ???????, ???????????????? ???????? ? ????? ?????????.

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



???????? **Наследуемые поля (Identical fields)** ????? ?????? ?????, ? ??????????? ?? ???? ???????. ? ??????? ??????? ?? ?????? ???????????, ????? ???? ???????? ??????? ?????????? ????????? ? ?????????????? ??????? ??? ???????????? ???????. ???? ???????? ????????????, ??????? ???? ?? ???? ????? ???? ????? ??????.

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

??????? ??????? ????????????, ????? ????? ??????? ????? ??? ?????????? ?????? ???????, ??????? ????????????? ???????????? ????????. ? ???? ??????? ???? ?????? ???? **селектор**, ??????? ?????????? ??? ???????.

???????? ???????? ??? ??????. ? ?????????? ????????? ????? ??????? ?????? ?? ???????????? ???????? ??? ??????? ????? ????? ? ???? ???????. ?????, ??? ? ? ?????? ????????, ????? ???????????? ?????? ?? ?????? ??????? ? ????? ??????? ????????. ????????, ????? ?????? ???????: "???? ???? ??????? ????? ?" ??? "???? ?????????? ??????? ??????? Y".

??? ???????????? ??????? ???????? ????? ????????? ???? ??? ????????? ?? ????????? **действий**:

- **В дальнейшую обработку** - ??????, ?????????? ???????? ????????????? ??????? ?? ????-????????? – ?? ??????? ?????????? ??? ?????????????? ???????, ??? ???????????? ? ? ????? ?????????? (?????? ??? ?????????). ?? ????????? ???? ?????? ????.
- **В коррелятор** - ??????, ?????????? ????????? ?????????? ?????????????? ??????? ???????? ?????? ???????? ???????????. ??? ???????? ??????? ???????????? ??????????. ?? ????????? ???? ?????? ????.

  ???? ?? ????????????? ?????? **В дальнейшую обработку** ? **В коррелятор**, ??????? ?????????? ????? ?????????? ??????? ?? ????-?????????, ? ????? ? ????????? ???????? ??????? ??????????.
- **Не создавать алерт** - ??????, ?????????? ???????? ??????? ??? ???????????? ??????? ??????????. ?? ????????? ???? ?????? ????.
  ???? ?? ??????, ????? ????? ?? ?????????? ??? ???????????? ??????? ??????????, ?? ????????????? ??????? ???-????? ???????????? ? ?????????, ?????????? ?????? **В дальнейшую обработку** ? **Не создавать алерт**. ???? ?????????? ?????? ?????? **Не создавать алерт**, ????????????? ??????? ?? ????? ?????????? ? ?????????.

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

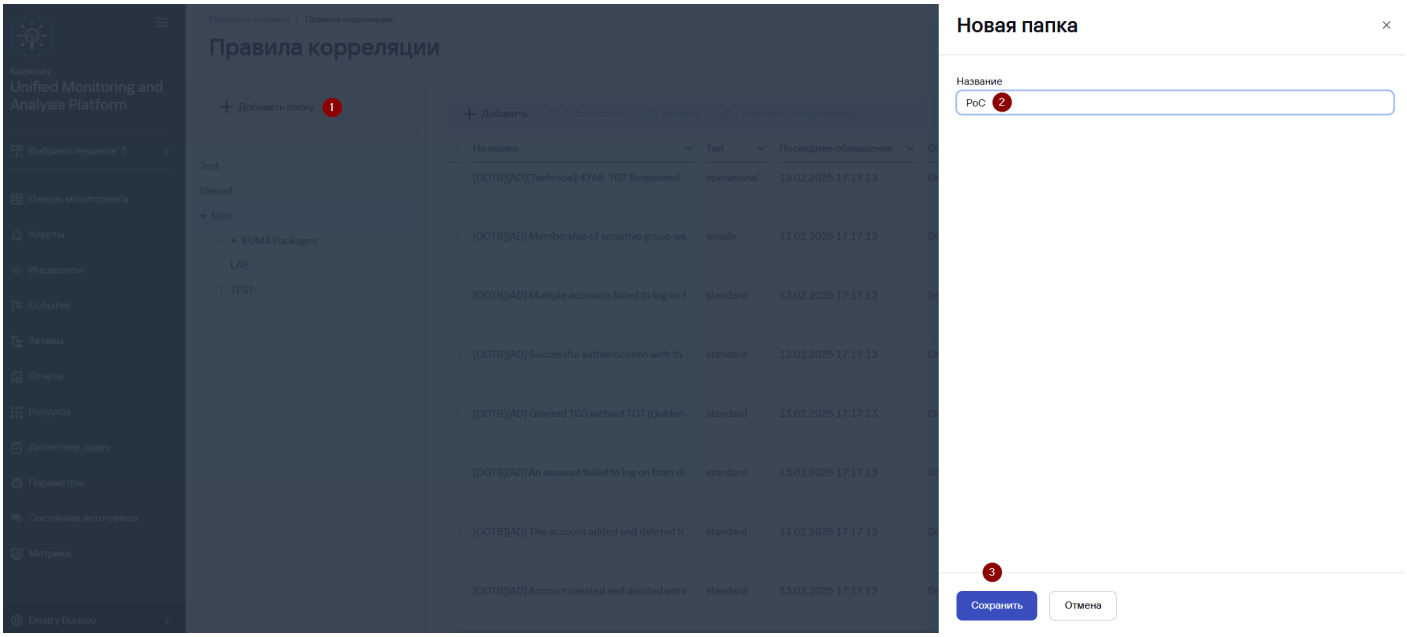
> ?????????? ????????? ??? ???? ? ??????????, ??????? ???? ???????????? ? ?????????, ? ?????????? ?????.

Создание правила корреляции типа Simple

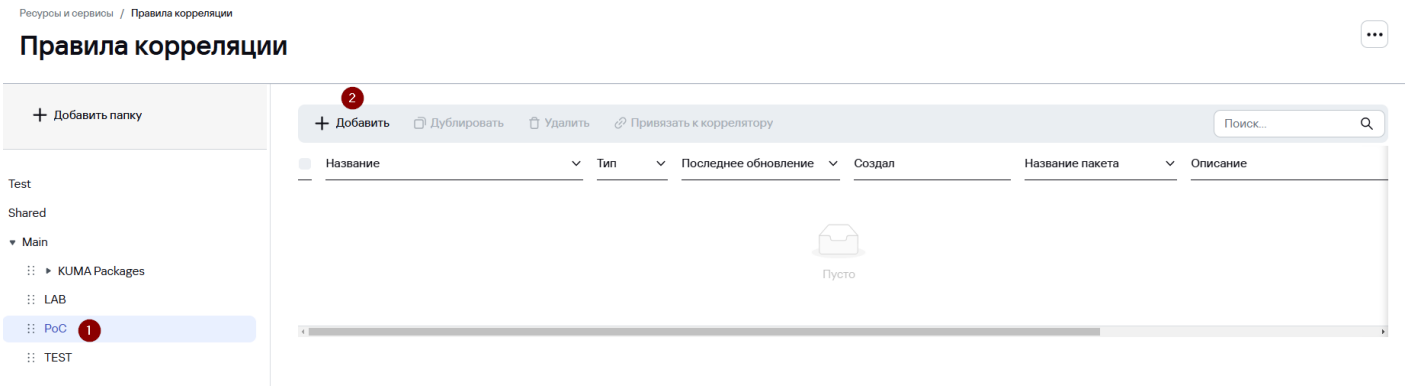
? ???????? ??????? ???????? ??????? ??????? ?????????? ??? ?????????? ????????? ??????? ????? ? ???-????????? KUMA.

????? ????????? ??????? ?????????? ???? Simple:

- ????????? ? ?????? **Ресурсы → Правила корреляции.**
- ?????????? ????? ??????? **Добавить папку** ??? ???????? ????????? ????? ??? ???????????????? ???????.
- ? ???? **Новая папка** ??????? **Название** ? ??????? **Сохранить**.



- ? ?????? ????? ???????? ????????? ????? ? ????? ??????? **Добавить.**



- ? ?????????? ???? **Создание правила корреляции** ?? ??????? **Общие** ???????:
  - **Название** ??????? ??????????
  - **Тенант**
  - **Тип** (? ????? ??????? **simple**)

- **Наследуемые поля** (? ????? ??????? ??? ???? DeviceAction, SourceAddress, SourceUserName ? EventOutcome).

Наследуемые поля – ??? ???? ???????? ???????, ??????? ?????????? ????????? ? ????????????? ??????? ??? ??????????? ???????.

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

????? ???? ? ???????? ??????????? ?????????? ???????? ? ??????????? ????? « ???????????» ? ??????? ???????, ?? ??????? ?? ??????????, ????? ??????????? ??????? ?????????? ? ?????????? ?????.

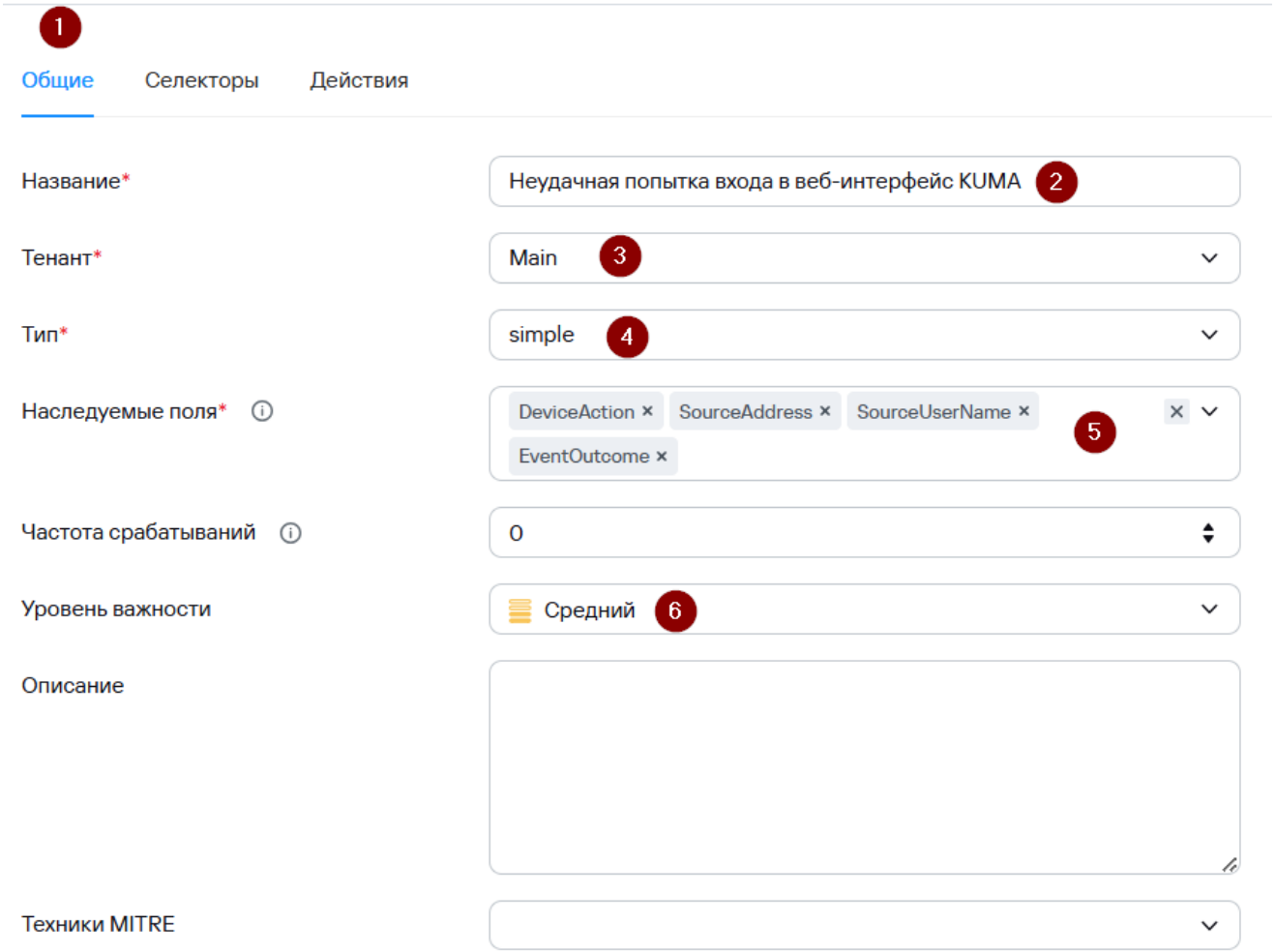
Информация о событии

Копировать

TenantID	Main
Timestamp	26.02.2025 14:28:02:473
EndTime	26.02.2025 14:28:02:473
Message	Invalid credentials
DeviceAction	user login
DeviceHostName	kuma-aio.truecompany.local
DeviceProduct	KUMA
DeviceTimeZone	+03:00
DeviceVendor	Kaspersky
SourceAddress	10.68.85.93
SourcePort	62967
SourceUserName	admin
EventOutcome	failed
Type	Audit

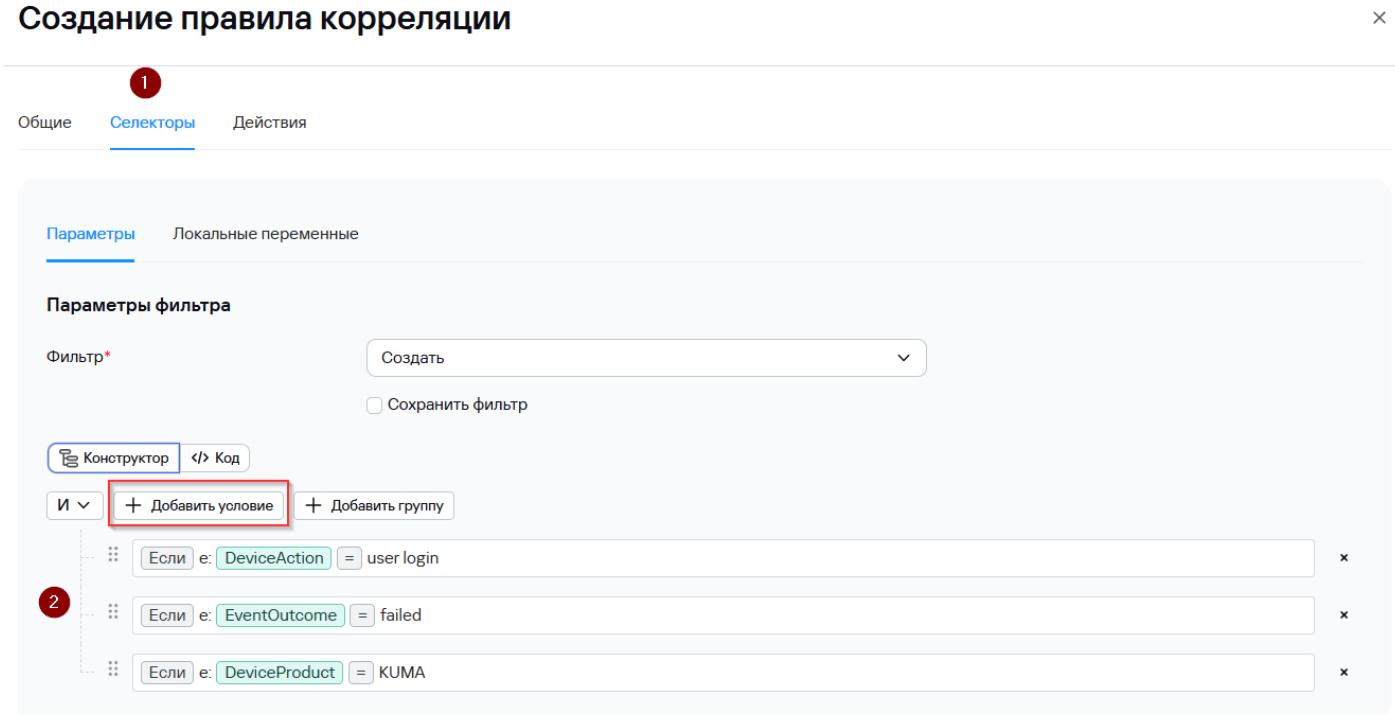
- ??????? ???????? (? ????? ??????? **Средний**)
- ??????????? **Описание**

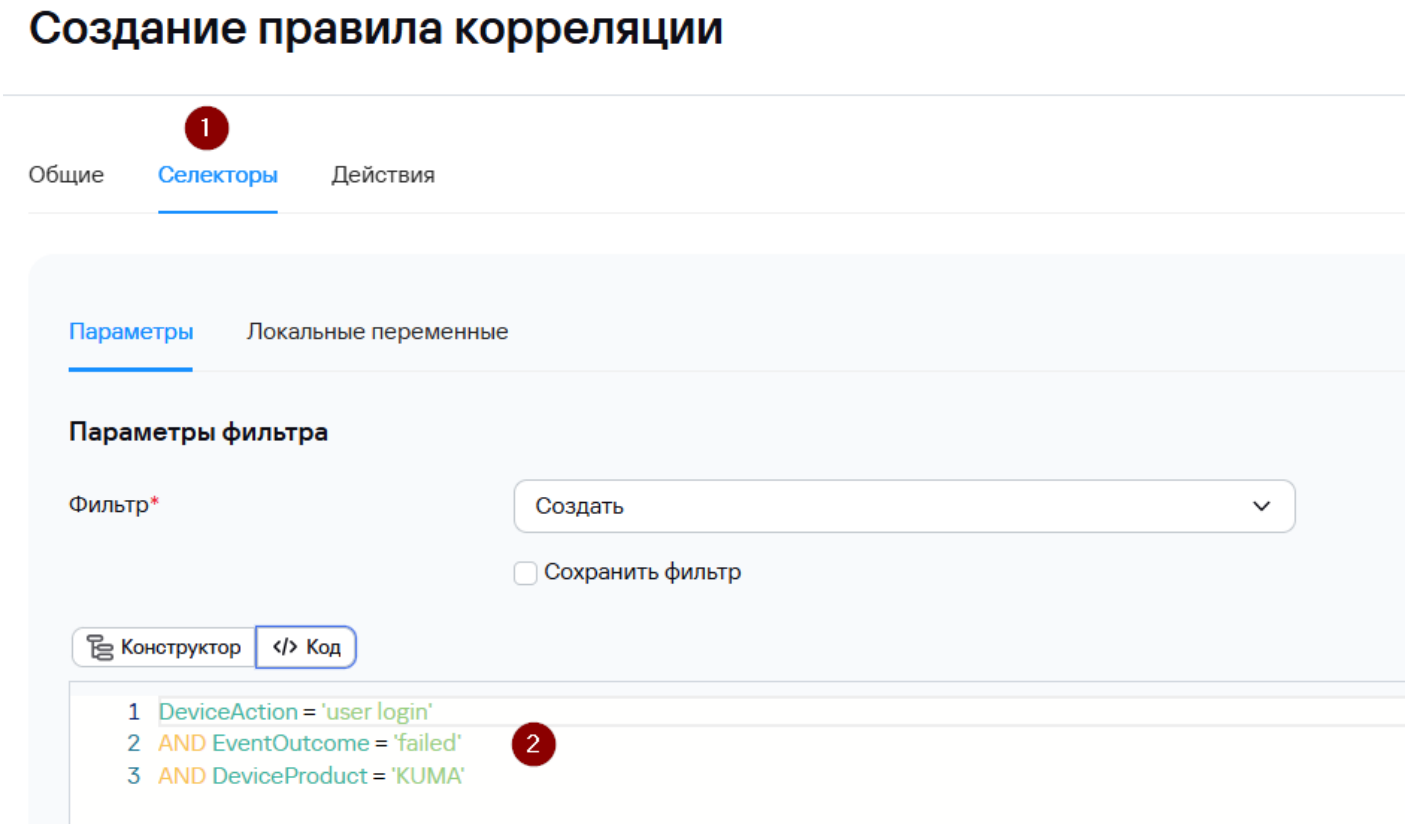
Создание правила корреляции



- ????????? ?? ??????? **Селекторы** ? ???????? ??????? (**Добавить условие**)

  ???????? ????????? ????. ?? ??????? **Селекторы** ???????????? ???????, ??????? ?????? ????????????? ????????????? ??????? ??? ???????????? ??????? ??????????.





??????? ????? ???????? ??? ? ???? **конструктора**, ??? ? ? ???? **кода**.

????? ???? ? ?? ???????? ?????????? ???????????? ? ???????? ??????? **Селектора** ????? «????????????» ? ??????? ???????, ?? ??????? ?? ??????????, ????? ???????????

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

??? ????????? ???????????????????? ????? ?????????? ??????? ????????????? ????????? ????, ????????, ??????? DeviceAction = ‘user login’ ???????? ????? ??????????, ??? ??????? DeviceProduct = ‘KUMA’.

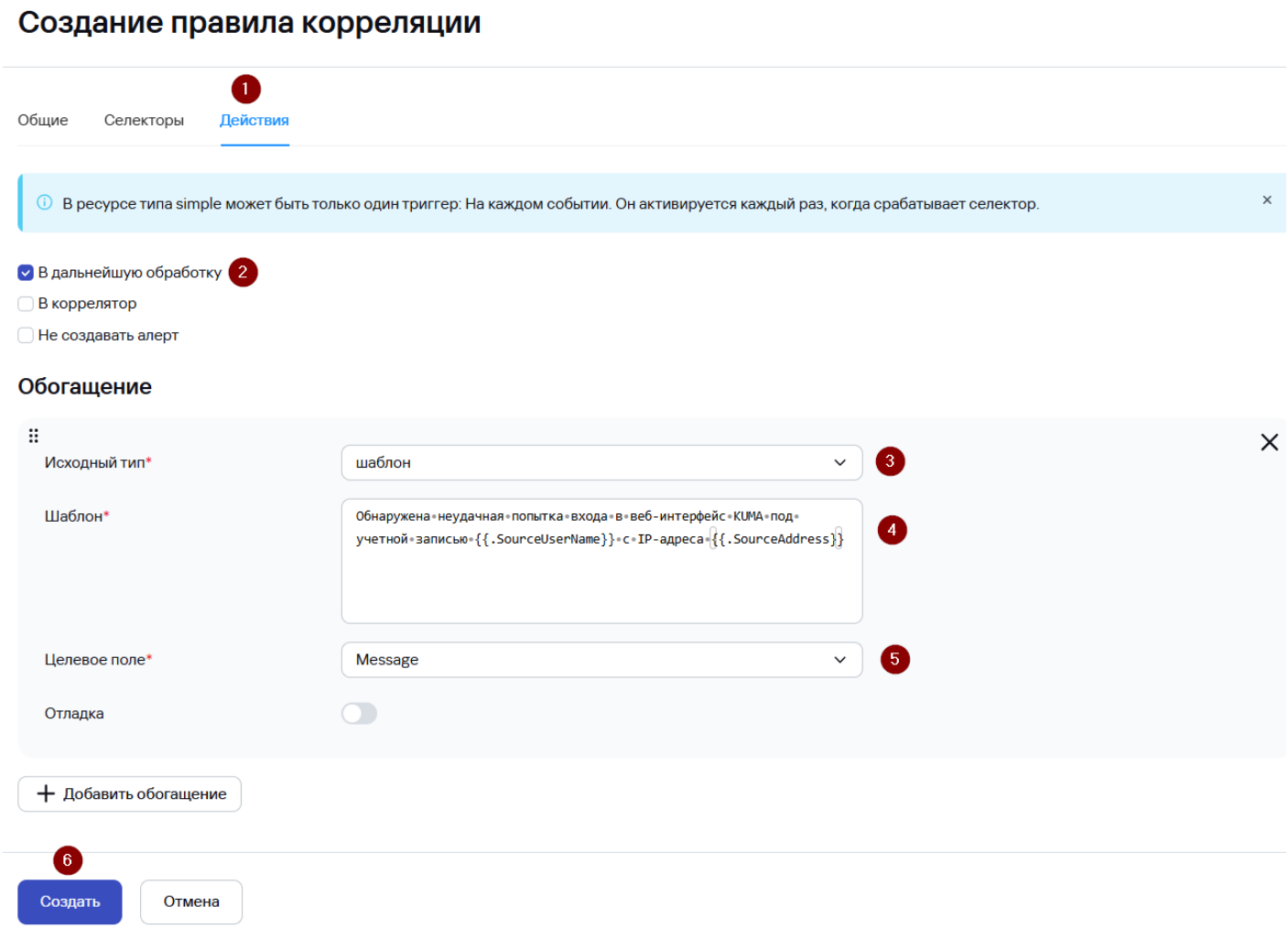
- ????????? ?? ??????? **Действия** ? ?????????? ?????? ????? ????????? **В дальнейшую обработку** ??? ???????? ???????????????? ???????, ???????????? ? ?????????? ???????????? ??????? ??????????, ?? ???????? ? ?????????**.**
- ???????? ??????????, ????? **Добавить обогащение:**
  - ??????? **Исходный тип** – **Шаблон**
  - ? ???? **Шаблон** ???????? ????????? ?????:

```
?????????? ????????? ??????? ????? ? ???-????????? KUMA ??? ??????? ???????
{{.SourceUserName}} c IP-?????? {{.SourceAddress}}
```

  - ? ???? **Целевое поле** ??????? **Message**

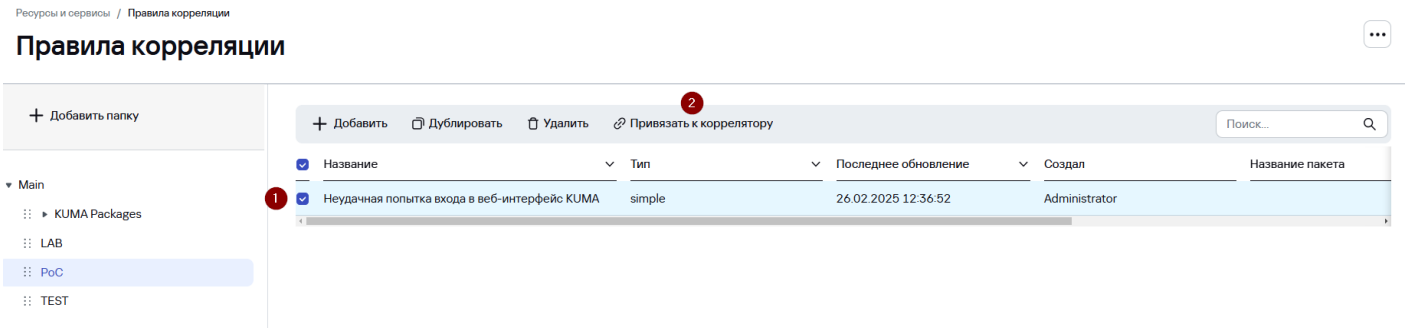
  ?????? ?????????? ???????? ???????????? ? ???????????? ??? ????????????? ????????? ????? ???????????? ?????????? ???????? ???? ?????????.

- ??????? **Создать**.

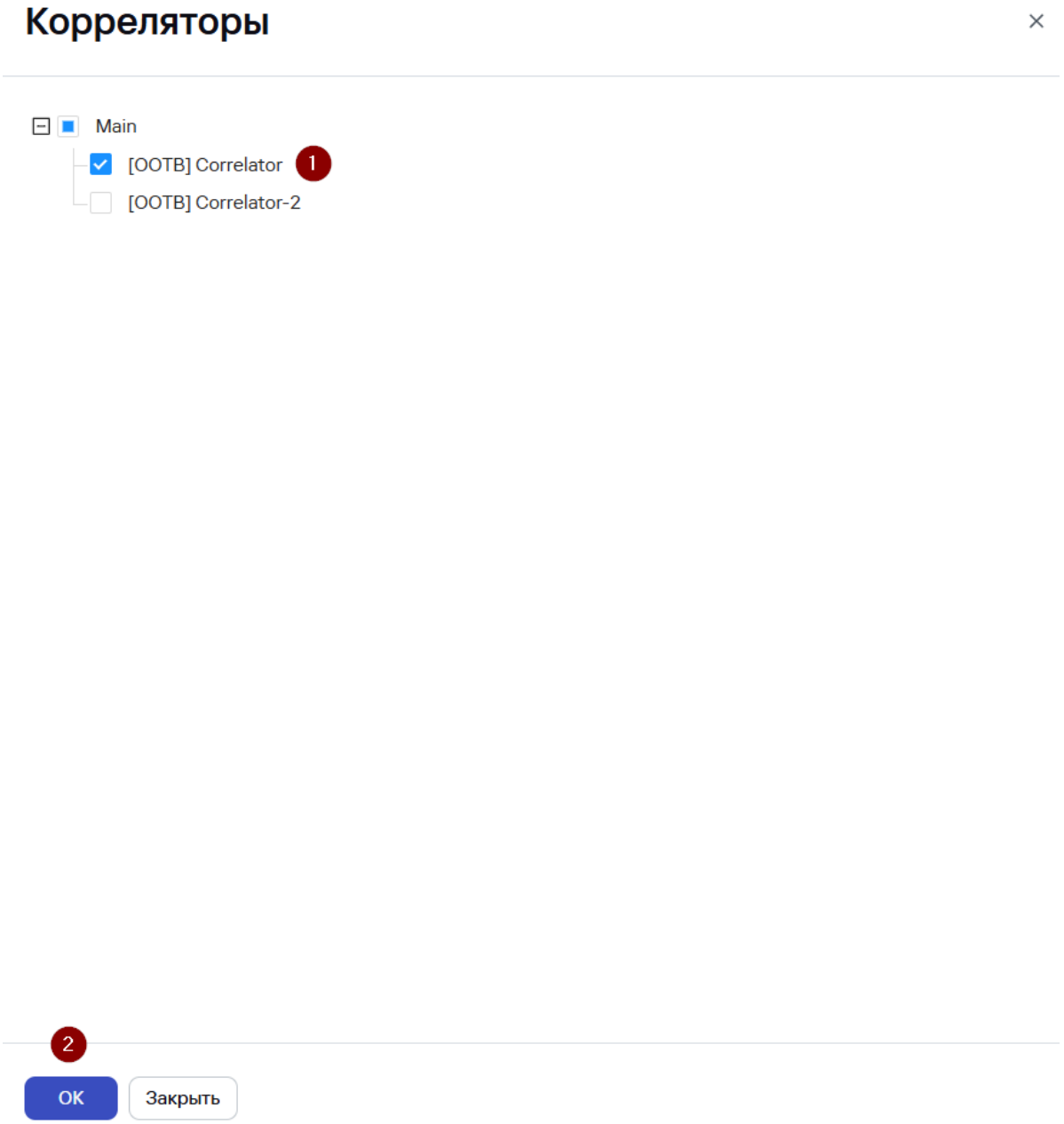


????? ???????? ??????? ?????????? ?????????? ????????? ??? ???????? ? ???????????:

- ???????? ????????? ??????? ?????????? ? ??????? **Привязать к коррелятору**.

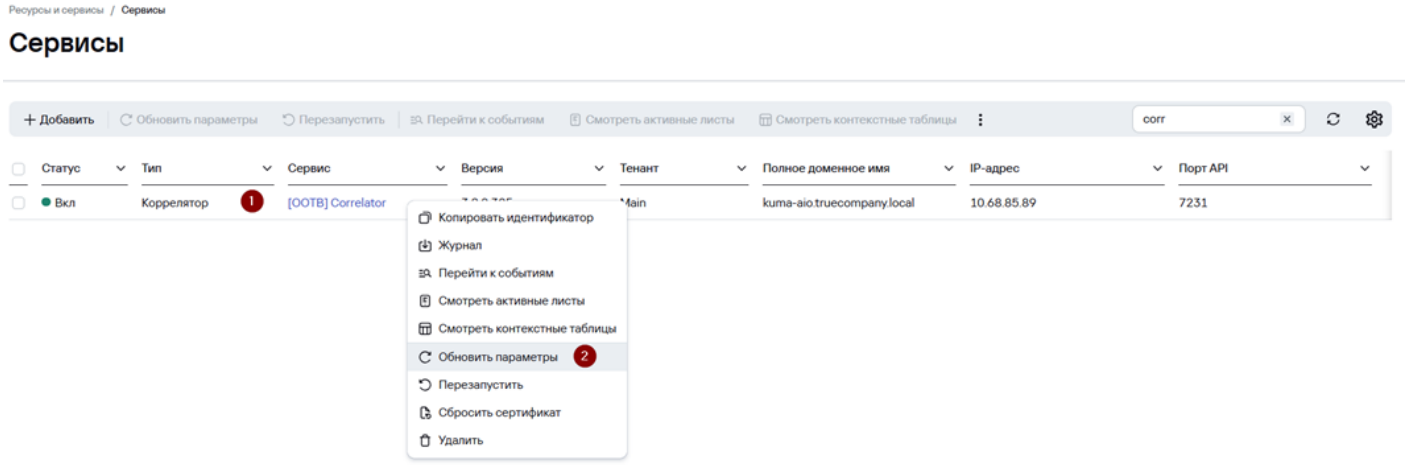


- ? ???? **Корреляторы** ???????? ?????? ???????????, ? ???????? ????? ????????? ??????? ? ??????? **OK**.



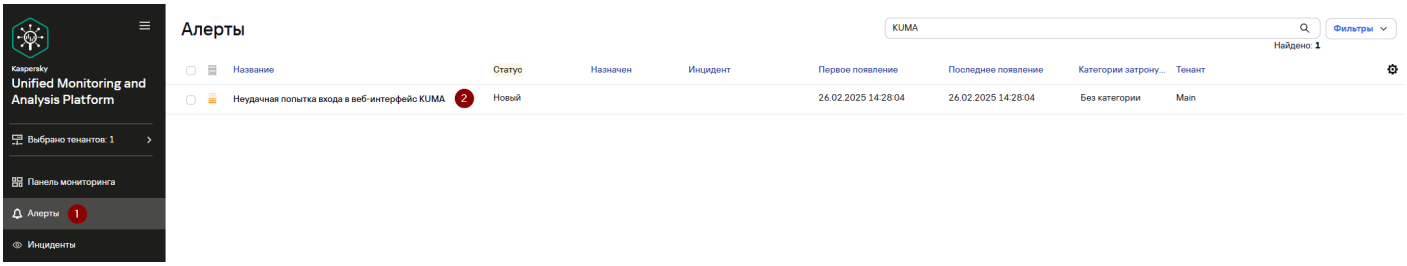
????? ?????????? ???????? ????????? ???????????? ?????????? ???????? ????????? ???????:

- ????????? ? **Ресурсы → Активные сервисы**.
- ??????? **ПКМ** ?? ?????? ??????????? ? ???????? **Обновить параметры**.

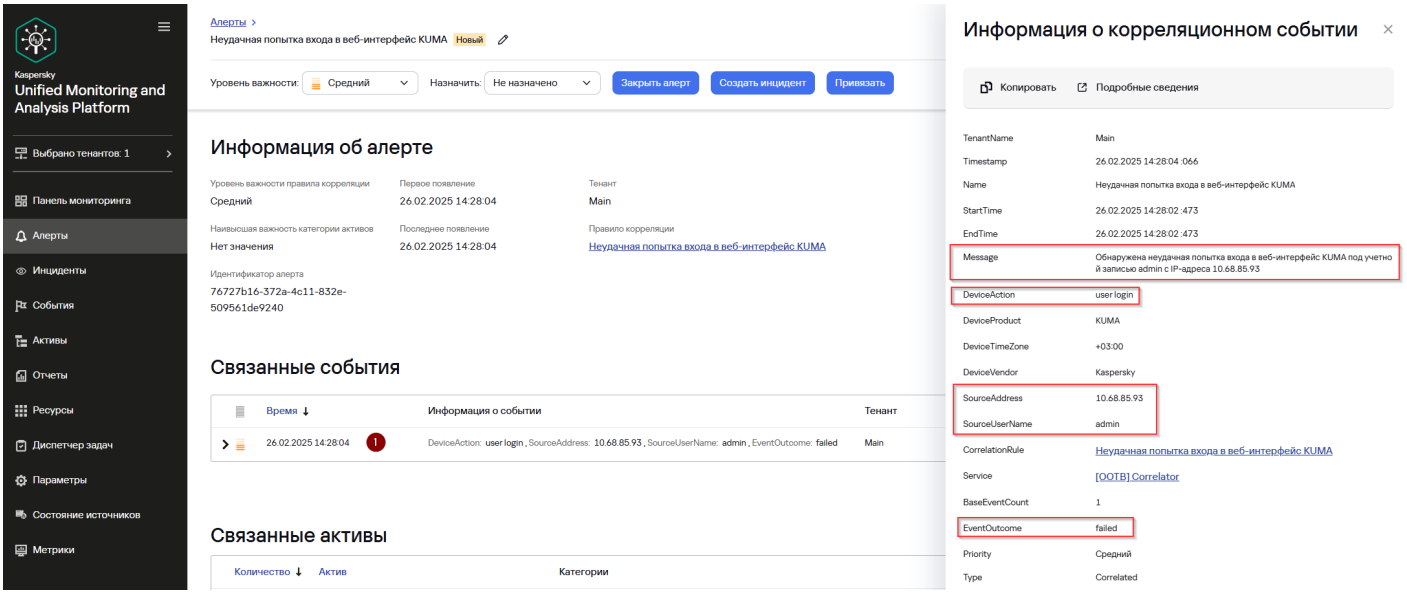


????? ????????? ???????????? ?????? ?????????? ??????? ?????????? ????????? ????????? ??????? ????? ? ???-????????? KUMA. ??? ????????, ??? ????????? ??????? ?????????:

- ????????? ? **Алерты.**
- ?????????, ??? ? ?????? ??????? ???????????? ????? **Неудачная попытка входа в веб-интерфейс KUMA**



- ???????? ???????? ??????, ????? ?? ?????.
- ? ???????? ?????? ? ?????? **Связанные события** ??????? ?? ????????? ?????????????? ???????.



- ?????????, ??? ? ???? **Информация о корреляционном событии** ???????????? ????, ??????? ??? ???????? ??????? ?????????? ???? ????????? ? **Наследуемые поля:**
  - DeviceAction
  - SourceAddress
  - SourceUserName
  - EventOutcome
- ?????????, ??? ? ???? **Информация о корреляционном событии** ? ???? **Message** ???????? ????? ???????? ????? ???????????? ?????????? ??? ????????????? ????????? ????? ???????????? ?????????? ???????? ???? ?????????.

Revision #14
Created 2023-08-09 12:40:46 UTC by Boris Rzr
Updated 2026-08-10 12:15:43 UTC by Dmitry Borisov