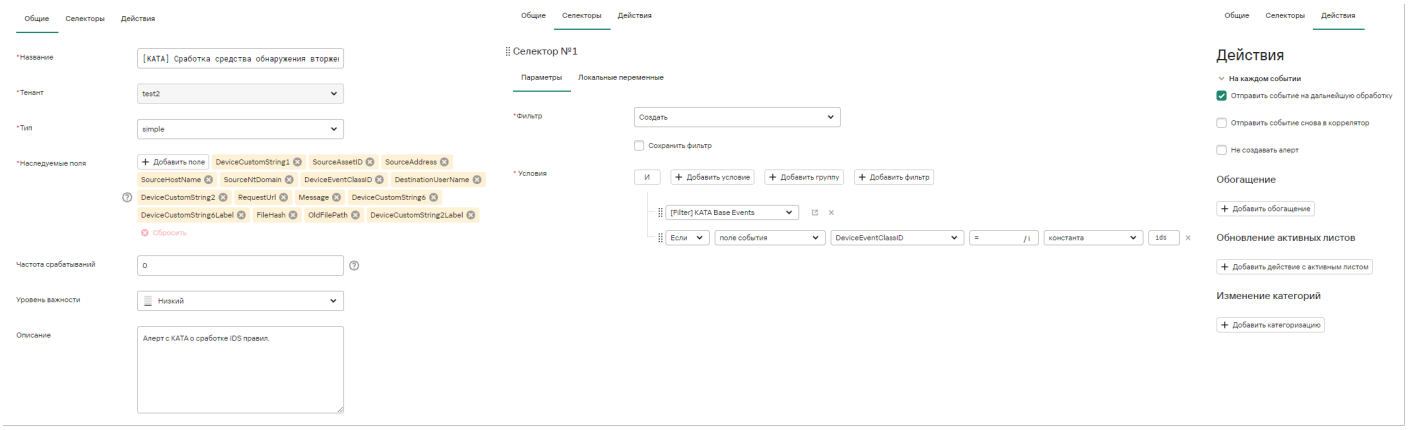
??????? ??????? (simple)

> **"Обновить параметры"** нужно делать в коррелляторе, когда какое-либо правило меняется, чтобы подтянулись актуальные изменения в правилах в коррелятор.

Простое правило (simple) — срабатывает при обнаружении каждого события, удовлетворяющего условиям в одном селекторе.

Типовой пример правила:



Параметр **Наследуемые поля (Identical fields)** имеет разный смысл, в зависимости от типа правила. В простом правиле он просто перечисляет, какие поля базового события коррелятор скопирует в корреляционное событие при срабатывании правила. Этот параметр обязательный, поэтому хотя бы одно такое поле нужно задать.

Например, если простое правило срабатывает на события о сетевых атаках, в идентичных полях уместно будет перечислить поля с информацией, характеризующие атаку: адрес злоумышленника, адрес жертвы, тип атаки. Аналитику следует посмотреть, в каких полях базовых событий содержится эта информация и перечислить эти поля в Наследуемых полях.

Если аналитик планирует создавать другие правила корреляции, которые реагируют не только на базовые, но и на корреляционные события, то от того, какие поля будут скопированы в корреляционное событие, будет зависеть, какие условия аналитик сможет использовать для такого события.

Простое правило используется, когда нужно создать алерт при обнаружении любого события, которое соответствует определенным условиям. В этом правиле есть только один **селектор**, который определяет эти условия.

Селектор работает как фильтр. В настройках селектора можно выбрать фильтр из существующих ресурсов или создать новый прямо в этом правиле. Также, как и в других фильтрах, можно использовать ссылки на другие фильтры в более сложных условиях.

Например, можно задать условие: "Если поле события равно X" или "Если выполняются условия фильтра Y".

При срабатывании правила аналитик может настроить одно или несколько из следующих **действий**:

- output — создать корреляционное событие, которое будет передано в настроенные точки назначения (обычно это хранилище), и по которому будет создано (или дополнен) алерт
- loop — переслать корреляционное событие на вход этого же коррелятора для рекурсивной обработки
- пополнить активные списки — добавить в активный список (или удалить из списка) запись на основании содержимого полей события
- обогатить корреляционное событие по словарю, по данным исходного события, константой или по шаблону, без запросов во внешние системы (т.е. такое же обогащение как в нормализаторе на коллекторе). Обогащение правилами можно задать в корреляторе отдельно, точно так же как в коллекторе

> Необходимо указывать все поля и переменные участвующие в селекторах в наследуемых полях.

???????? ??????? ?????????? ???? Simple

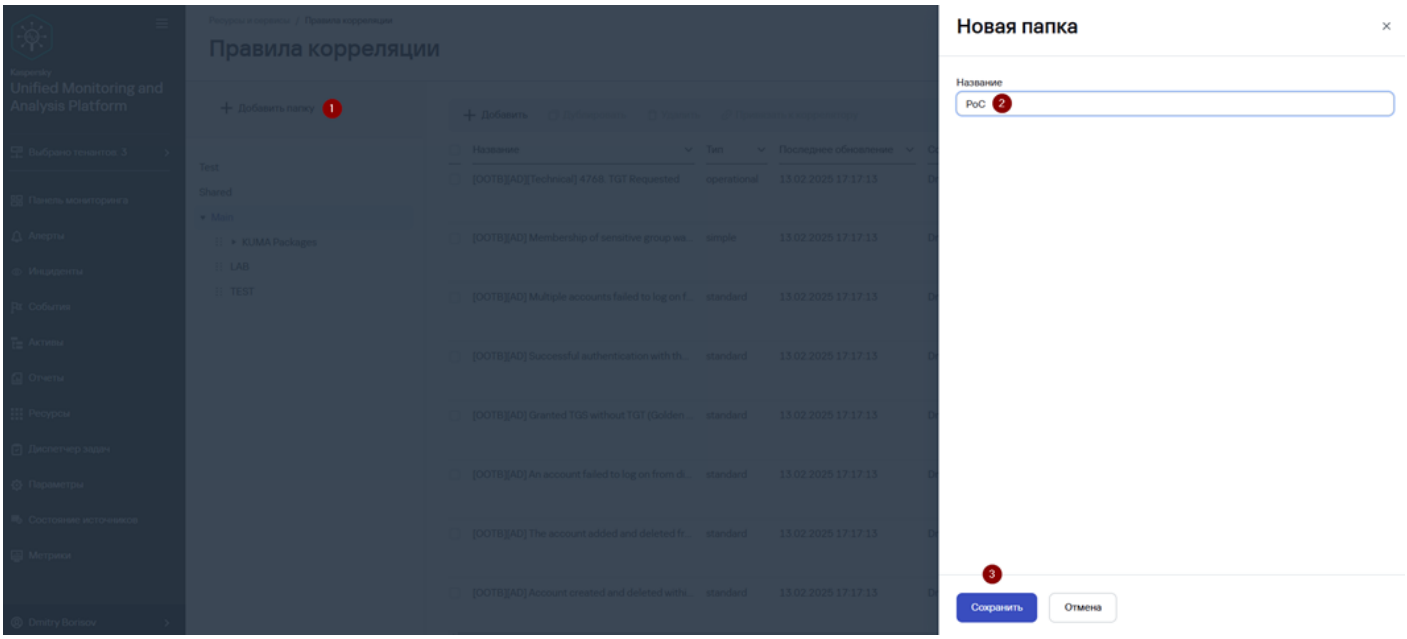
В качестве примера создадим простое правило корреляции для обнаружения неудачной попытки входа в веб-интерфейс KUMA.

Чтобы настроить правило корреляции типа Simple:

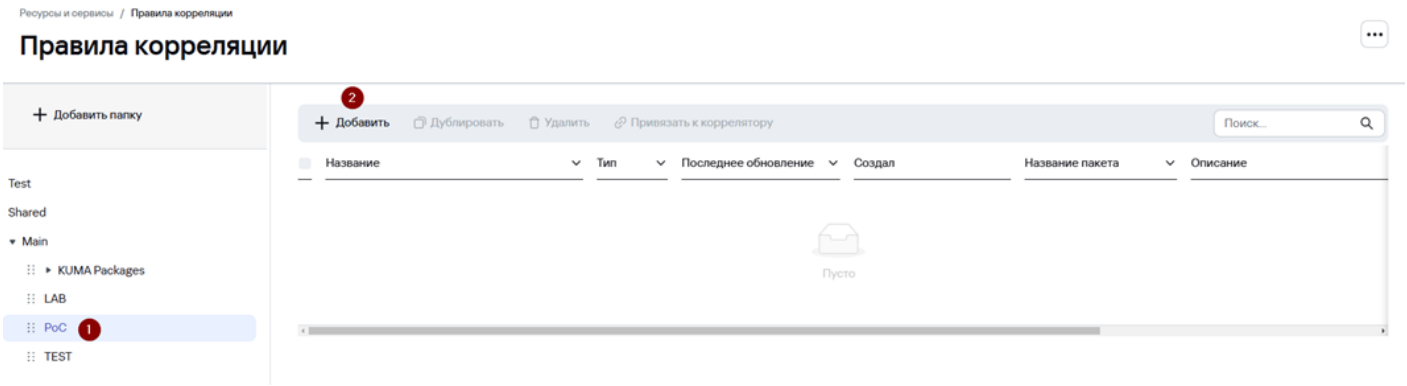
1. Перейдите в раздел **Ресурсы ? Правила корреляции.**

2. Опционально слева нажмите **Добавить папку** для создания отдельной папки под пользовательские правила.

3. В окне **Новая папка** укажите **Название** и нажмите **Сохранить**.



4. В панели слева выберите созданную папку и далее нажмите **Добавить.**



5. В появившемся окне **Создание правила корреляции** на вкладке **Общие** укажите:

- **Название** правила корреляции
- **Тенант**
- **Тип** (в нашем примере **simple**)
- **Наследуемые поля** (в нашем примере это поля DeviceAction, SourceAddress, SourceUserName и EventOutcome).

Наследуемые поля – это поля базового события, которые коррелятор скопирует в корреляционное событие при срабатывании правила.

Например, если простое правило срабатывает на событие неудачного входа в веб-интерфейс в наследуемых полях уместно будет перечислить поля с информацией под какой учетной записью и с какого адреса была выполнена неудачная попытка входа.

Какие поля с полезной информацией необходимо добавить в наследуемые можно «подсмотреть» в примере события, на которое Вы планируете, чтобы срабатывало правило корреляции и создавался алерт.

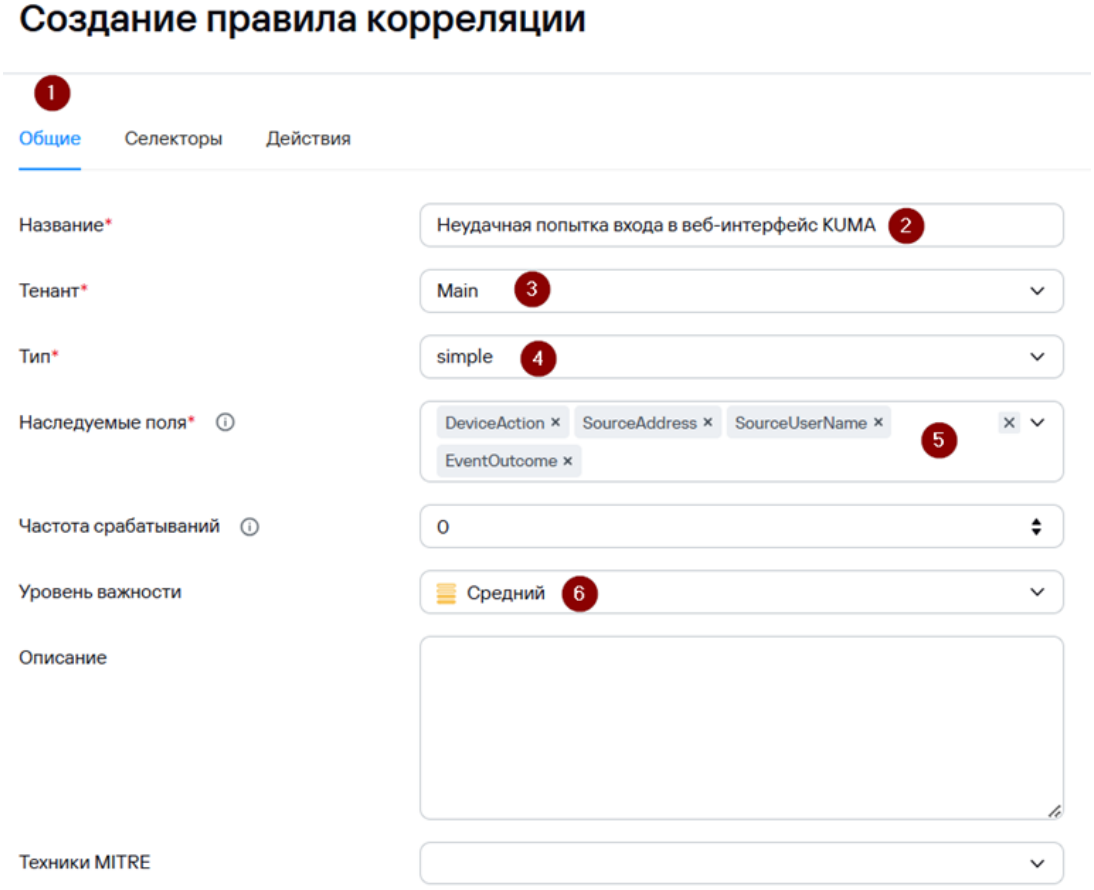
- Уровень важности (в нашем примере **Средний**)
- Опционально **Описание**

Информация о событии

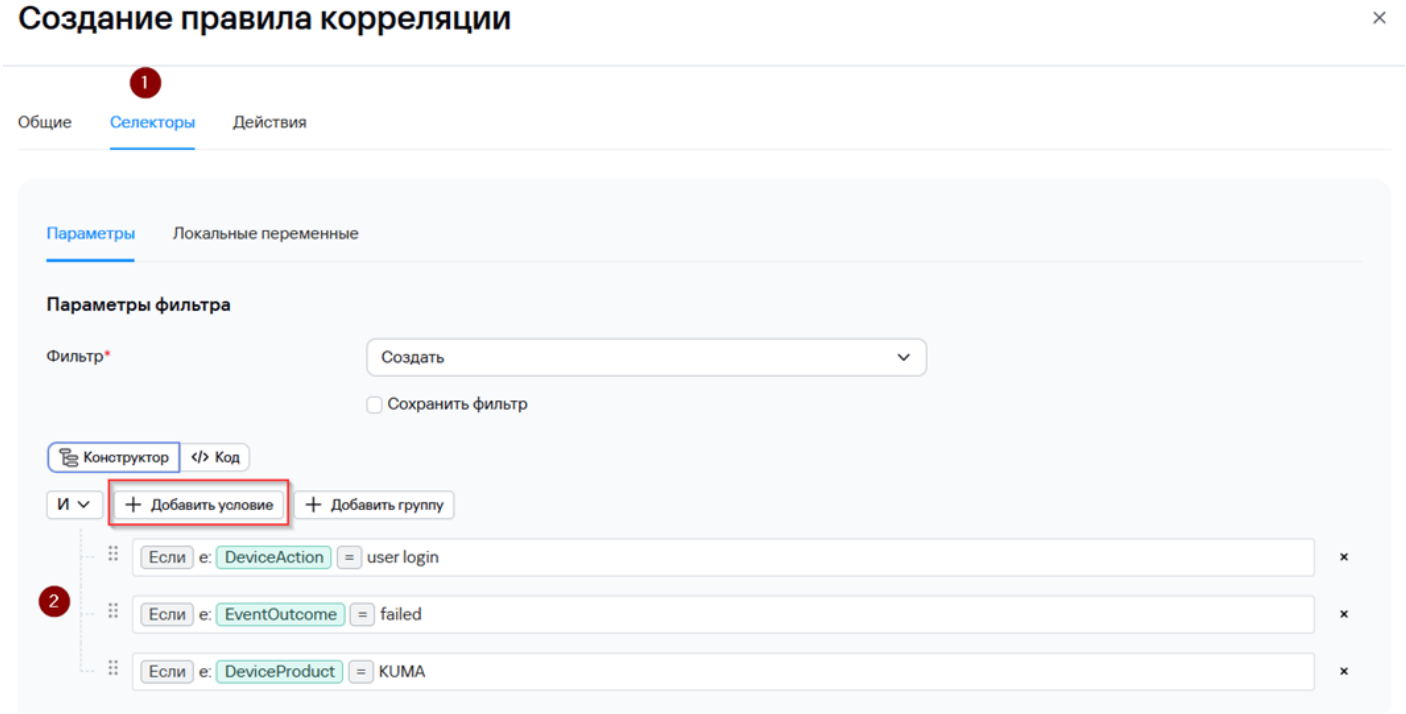
Копировать

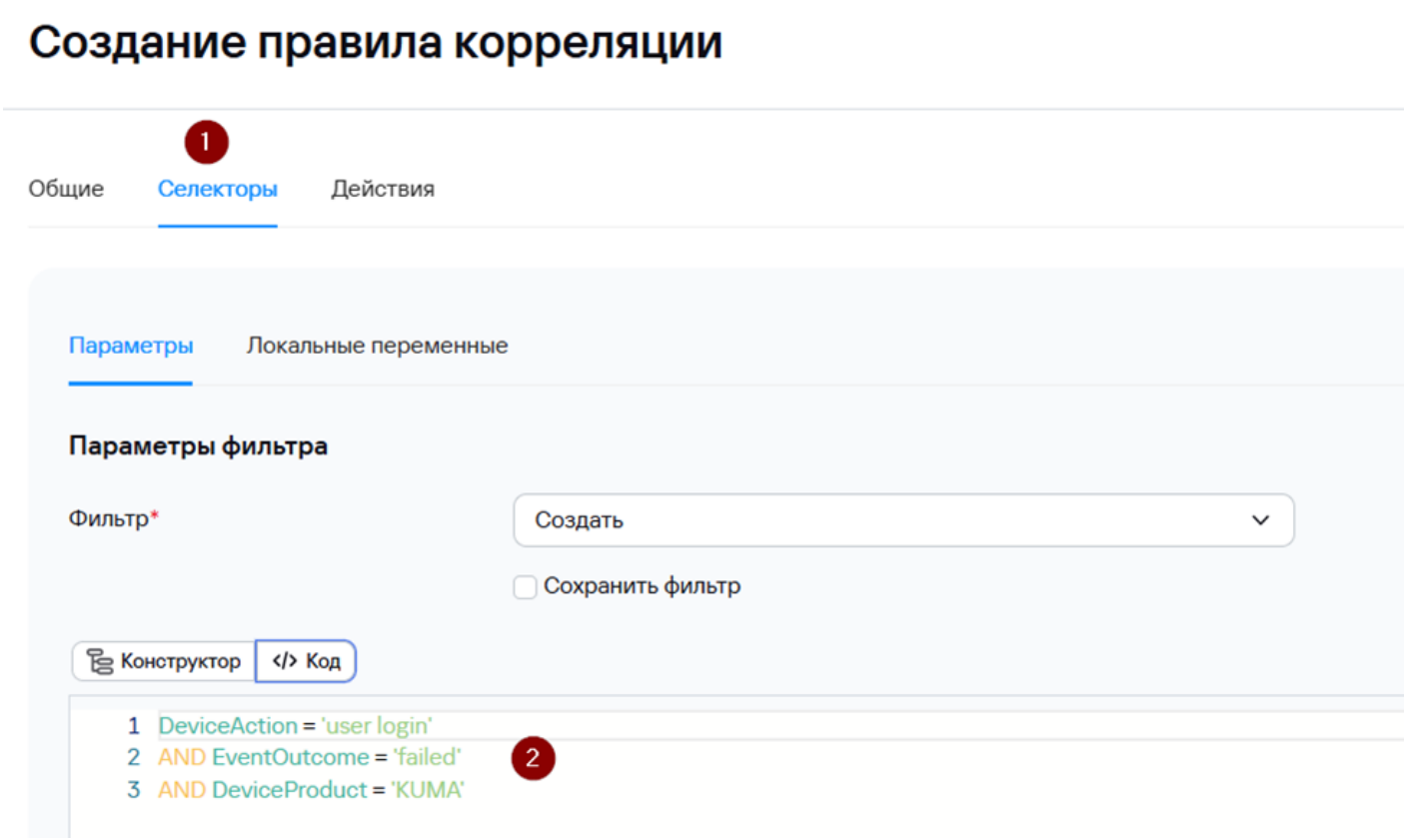
TenantID	Main
Timestamp	26.02.2025 14:28:02:473
EndTime	26.02.2025 14:28:02:473
Message	Invalid credentials
DeviceAction	user login
DeviceHostName	kuma-aio.truecompany.local
DeviceProduct	KUMA
DeviceTimeZone	+03:00
DeviceVendor	Kaspersky
SourceAddress	10.68.85.93
SourcePort	62967
SourceUserName	admin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

- Уровень важности (в нашем примере **Средний**)
- Опционально **Описание**



6. Перейдите на вкладку **Селекторы** и добавьте условия (**Добавить условие**) согласно скриншоту ниже. На вкладке **Селекторы** определяются условия, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции.





Условия можно задавать как в виде **конструктора**, так и в виде **кода**.

Какие поля и их значения необходимо использовать в качестве условий **Селектора** можно «подсмотреть» в примере события, на которое Вы планируете, чтобы срабатывало правило корреляции и создавался алерт.

Для повышения производительности более специфичные условия рекомендуется размещать выше, например, условие DeviceAction = ‘user login’ является более специфичным, чем условие DeviceProduct = ‘KUMA’.

7. Перейдите на вкладку **Действия** и установите флажок возле параметра **В дальнейшую обработку** для отправки корреляционного события, создаваемого в результате срабатывания правила корреляции, на хранение в Хранилище**.**

8. Добавьте обогащение, нажав **Добавить обогащение:**

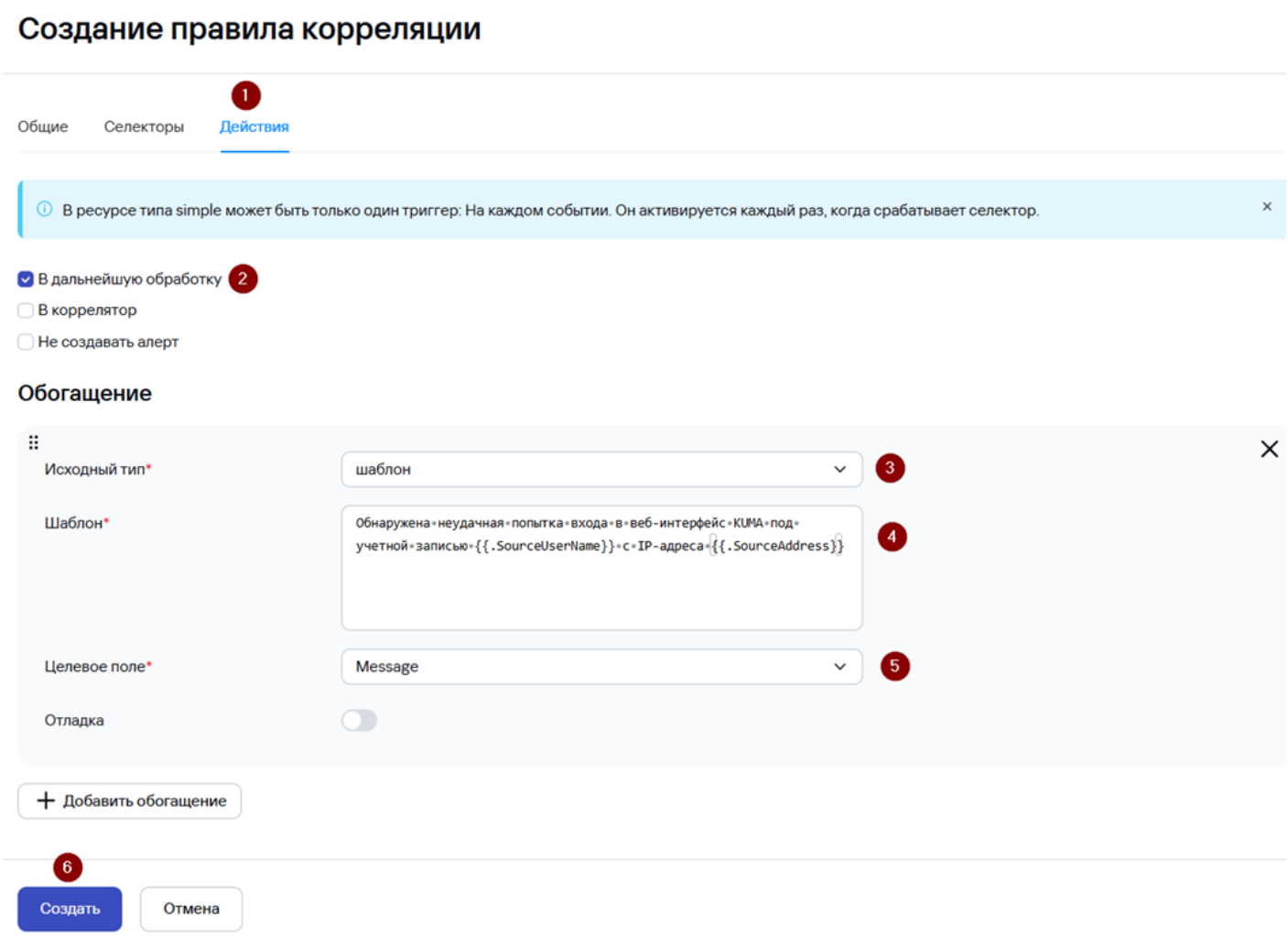
- Укажите **Исходный тип** – **Шаблон**
- В поле **Шаблон** добавьте следующий текст:

Обнаружена неудачная попытка входа в веб-интерфейс KUMA под учетной записью {{.SourceUserName}} с IP-адреса {{.SourceAddress}}

- В поле **Целевое поле** укажите **Message**

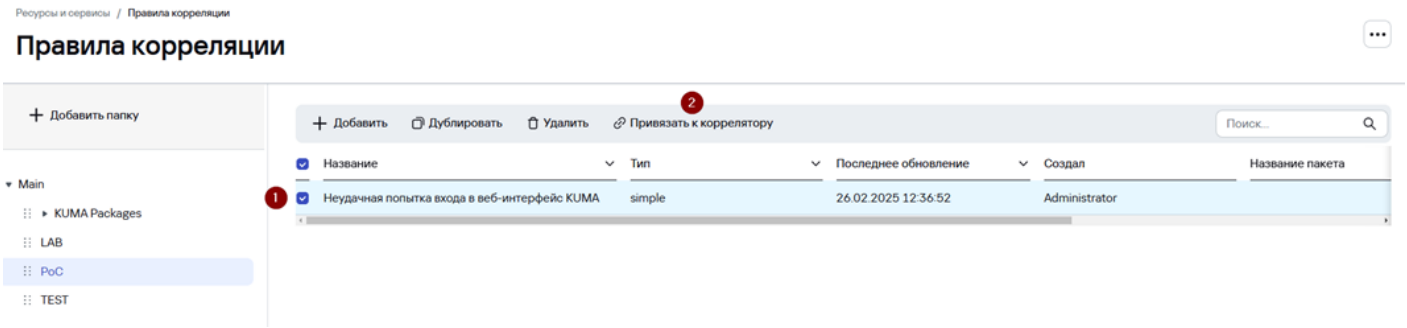
Данное обогащение является опциональным и используется для информирования аналитика какое потенциально вредоносное действие было совершено.

9. Нажмите **Создать**.

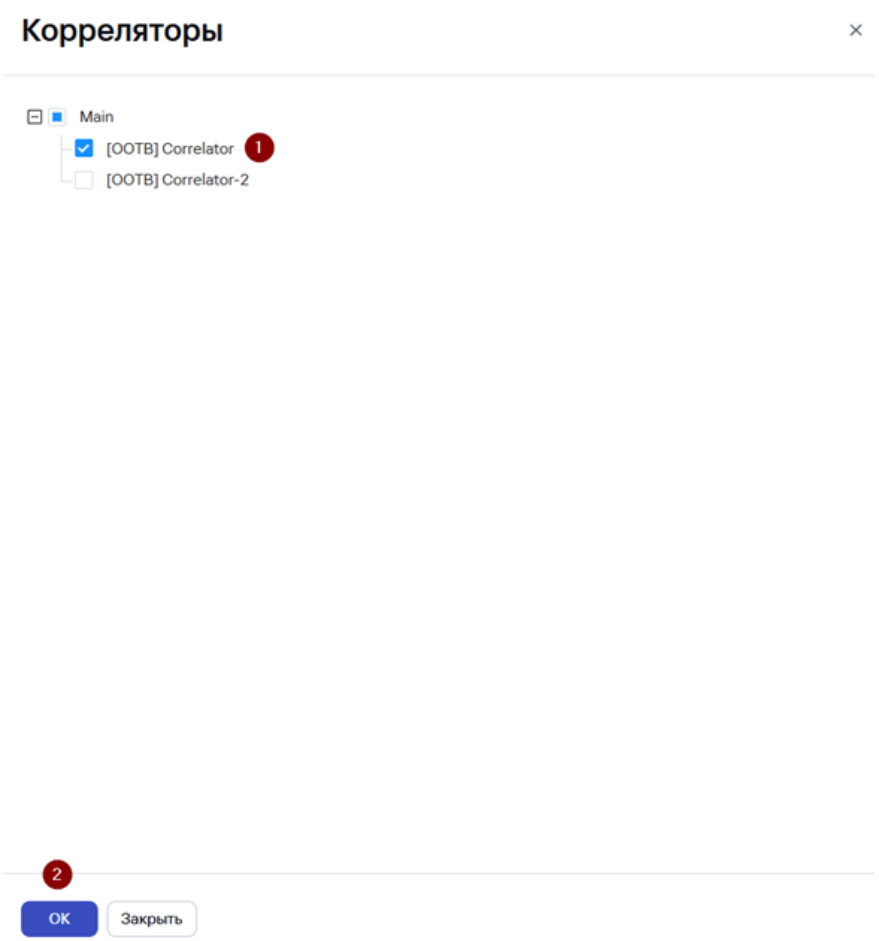


После создания правила корреляции необходимо выполнить его привязку к коррелятору:

1. Выберите созданное правило корреляции и нажмите **Привязать к коррелятору**.



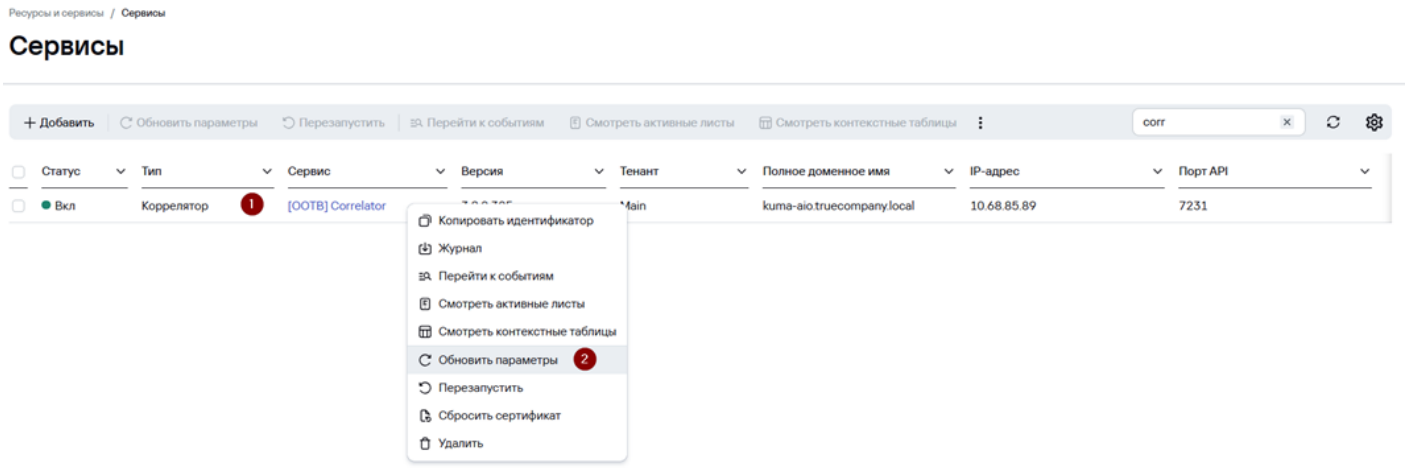
2. В окне **Корреляторы** выберите сервис Коррелятора, к которому будет привязано правило и нажмите **OK**.



Чтобы коррелятор применил изменения конфигурации необходимо обновить параметры сервиса:

3. Перейдите в **Ресурсы ? Активные сервисы**.

4. Нажмите **ПКМ** на сервис Коррелятора и выберите **Обновить параметры**.

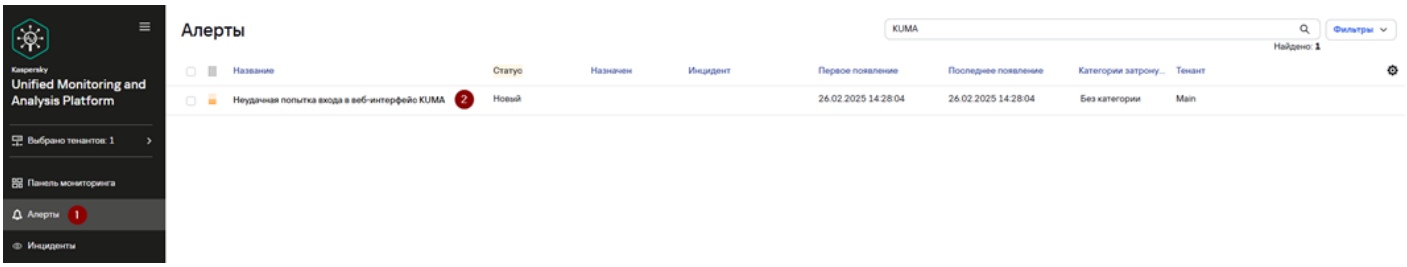


Чтобы проверить корректность работы созданного правила корреляции выполните неудачную попытку входа в веб-интерфейс KUMA.

Для проверки, что созданное правило сработало:

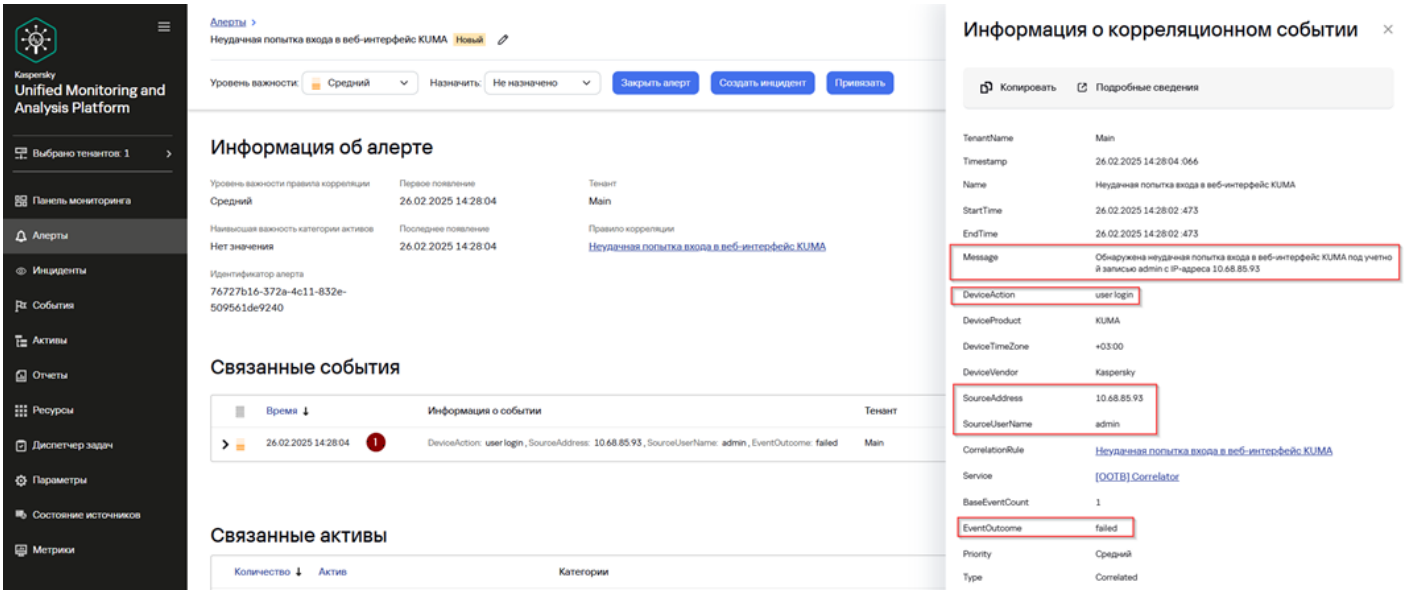
1. Перейдите в **Алерты.**

2. Убедитесь, что в списке алертов присутствует алерт **Неудачная попытка входа в веб-интерфейс KUMA**



3. Откройте карточку алерта, нажав на алерт.

4. В карточке алерта в секции **Связанные события** нажмите на созданное корреляционное событие.



5. Убедитесь, что в окне **Информация о корреляционном событии** присутствуют поля, которые при создании правила корреляции были добавлены в **Наследуемые поля:**

- DeviceAction
- SourceAddress
- SourceUserName
- EventOutcome

6. Убедитесь, что в окне **Информация о корреляционном событии** в поле **Message** добавлен текст согласно ранее настроенному обогащению для информирования аналитика какое потенциально вредоносное действие было совершено.

Revision #10
Created 2023-08-09 12:40:46 UTC by Boris Rzr
Updated 2026-06-16 10:56:13 UTC by lerat