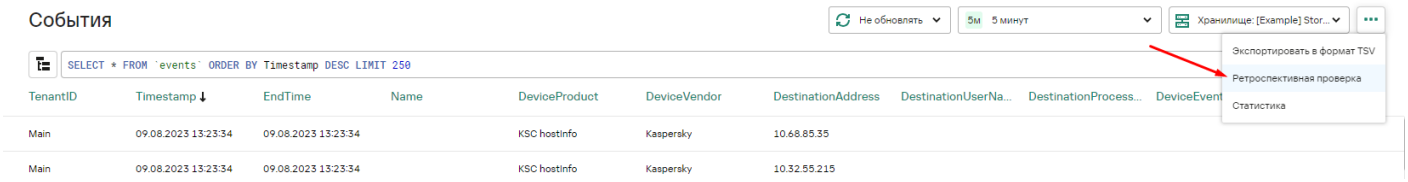
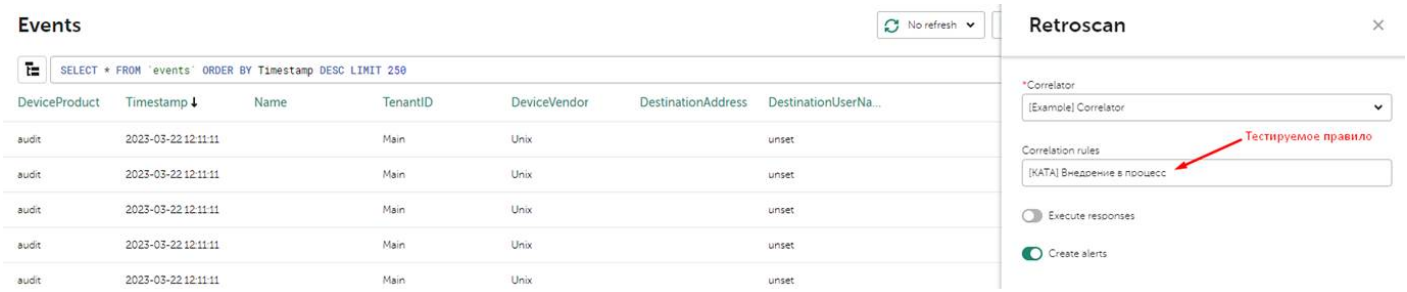
?????????? ?????? ?????????? (??????????)

Для тестирования правил можно использовать ретроскан (из раздела “События”), предварительно это правило нужно добавить в коррелятор и осуществить выборку интересующих событий запросом (выбрать временной диапазон):



В нашем случае, если правило сработает создастся алерт (можно отключить его создание по необходимости), заполнятся листы, если это есть в действиях правила корреляции. Также можно включить опцию запуска реагирования.



> В случае отсутствия сработки попробуйте убрать LIMIT в SQL запросе при ретроскане

Revision #4
Created 2023-08-09 13:17:37 UTC by Boris Rzr
Updated 2026-05-15 11:50:03 UTC by Boris Rzr