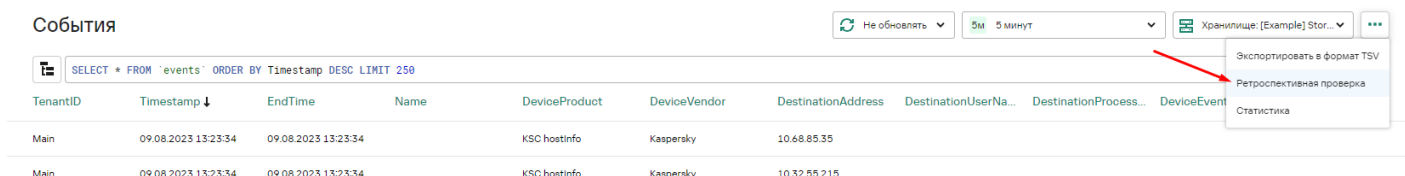


???????????????? ????  
???????????? (?????????)

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):



События

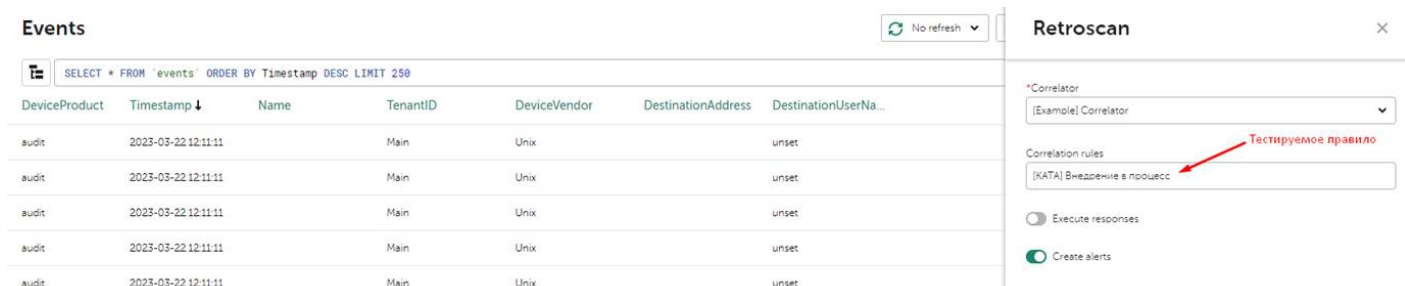
Не обновлять 5м 5 минут Хранилище: [Example] Stor...

SELECT \* FROM 'events' ORDER BY Timestamp DESC LIMIT 250

TenantID	Timestamp ↓	EndTime	Name	DeviceProduct	DeviceVendor	DestinationAddress	DestinationUserNa...	DestinationProcess...	DeviceEvent
Main	09.08.2023 13:23:34	09.08.2023 13:23:34		KSC hostinfo	Kaspersky	10.68.85.35			
Main	09.08.2023 13:23:34	09.08.2023 13:23:34		KSC hostinfo	Kaspersky	10.32.55.215			

Экспортировать в формат TSV  
Ретроспективная проверка  
Статистика

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.



Events

No refresh

Retroscan

\*Correlator  
[Example] Correlator

Correlation rules  
[KATA] Введение в процесс

Execute responses

Create alerts

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