

Тестирование правил корреляции

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, заполнятся листы, если это есть в действиях правила корреляции. Также можно включить опцию запуска реагирования.

Events

No refresh

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

DeviceProduct	Timestamp ↓	Name	TenantID	DeviceVendor	DestinationAddress	DestinationUserNa...
audit	2023-03-22 12:11:11		Main	Unix		unset
audit	2023-03-22 12:11:11		Main	Unix		unset
audit	2023-03-22 12:11:11		Main	Unix		unset
audit	2023-03-22 12:11:11		Main	Unix		unset
audit	2023-03-22 12:11:11		Main	Unix		unset

Retroscan

*Correlator

[Example] Correlator

Correlation rules

[KATA] Внедрение в процесс

Execute responses

Create alerts

ыыаыа