

# Операционное правило (operational)

**“Обновить параметры”** нужно делать в корреляторе, когда какое-либо правило меняется, чтобы подтянулись актуальные изменения в правилах в коррелятор.

<https://www.youtube.com/embed/TauttDGugBc?si=jw05NxFfgxOuyioY>

**Операционное правило (operational)** — наполняют активные листы без создания корреляционного события, механика работы аналогична простому правилу корреляции. Чтобы просмотреть содержимое списка нужно открыть список активных сервисов (Active services), выбрать службу типа Correlator (поставить галочку слева) и у нее появится активная кнопка Go to active lists (Перейти в активные листы).

Общие Селекторы Действия

Название [NGate] Вход на VPN одним пользователем и

Тег test2

Тип operational

Частота срабатываний 0

Описание

Селектор №1

Локальное переименование

Фильтр

Создать

Сохранить фильтр

И + Добавить условие + Добавить группу + Добавить фильтр

Если [FRM] Ngate Base Events поле событие SourceProcessName \* константа

Create session

Если не inActiveList Ngate VPN diff accPs содержит запись с ключом SourceUserName

Действия

На каждом событии

Обновление активных листов

Активный лист #1

Название Ngate VPN diff accPs

Операция Установить

Ключевые поля SourceUserName

Сопоставление SourceAddress SourceAddress / Константа SourceUserName SourceUserName / Константа

Удалить действие с активным листом

Добавить действие с активным листом

При записи в активный лист, в качестве ключевого поля могут быть несколько значений полей события, для составления комбинированного ключа, при этом в значении ключа это будет выглядеть так: *поле1|поле2|поле3*

Revision #3

Created 9 August 2023 12:53:29 by Boris RZR

Updated 7 July 2024 08:22:02 by Koala