

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) — наполняет активные листы без создания корреляционного события, механика работы аналогична простому правилу корреляции. С помощью списков можно отслеживать закономерности на длительных промежутках времени. Активный список хранится в памяти коррелятора (и кешируется на диск), так что состояние списка не теряется при перезагрузке службы или сбое.

Наполнять список могут любые правила. Но простые и стандартные правила всегда создают корреляционные события и предупреждения. Чтобы просто наполнять список и не создавать предупреждений, предусмотрены операционные правила.

В операционном правиле доступны только две операции над списком: set и del. Операция get не имеет смысла, поскольку она призвана обогащать корреляционное событие, а операционное правило не создает таких событий.

Пример правила:

The screenshot displays the configuration interface for an operational rule, divided into three main sections: **Общие** (General), **Селекторы** (Selectors), and **Действия** (Actions).

- Общие:** Includes fields for **Название** (Name) set to "[Ngate] Вход на VPN одним пользователем и", **Тип** (Type) set to "test2", and **Частота срабатываний** (Frequency) set to "0".
- Селекторы:** Shows a selector named "Селектор №1" with a **Локальное переименование** (Local rename) field. Below it, there are options for **Фильтр** (Filter) and **Условия** (Conditions). The conditions section includes a logical operator "И" (AND) and a list of conditions: "[PBase] Ngate Base Events", "Если поле события SourceProcessName * константа", "Create session", and "Если не isActiveList Ngate VPN diff srcPa содержит запись с ключом SourceUserName".
- Действия:** Shows the **Действия** (Actions) section with a dropdown for **Название** (Name) set to "Ngate VPN diff srcPa", an **Операция** (Operation) set to "Установить" (Set), and a list of **Ключевые поля** (Key fields) including "SourceUserName", "SourceAddress", and "SourceUserName".

Если при выполнении операции set окажется, что запись с таким же ключом уже есть в списке, она будет перезаписана новым значением на основании полей нового события.

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* сравнивать с этим впоследствии можно будет только с целым ключом, а не с какой-то его частью.

Атрибуты записей из активного списка можно использовать для обогащения корреляционных событий. Для этого его нужно сохранить в виде атрибута записи в активном списке операционным правилом. А затем в корреляционном правиле в разделе действий нужно будет выполнить операцию `get` над активным списком и записать в какое-нибудь поле корреляционного события содержимое атрибута записи из активного списка.

Если есть несколько служб коррелятора, использующих один и тот же ресурс списка, у каждой будет свое состояние этого списка.

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).

Аналитик может экспортировать и импортировать, а также очистить содержимое списка. Аналитик также может отобразить содержимое списка, увидеть, какие в нем есть записи, когда они были созданы или обновлены, и когда у них истекает время жизни, если для списка настроено время жизни. Аналитик может вручную удалять (но не редактировать) записи.

Каждую запись можно открыть и изучить ее дополнительные атрибуты.

Revision #4

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

Updated 24 December 2024 09:46:57 by Boris RZR