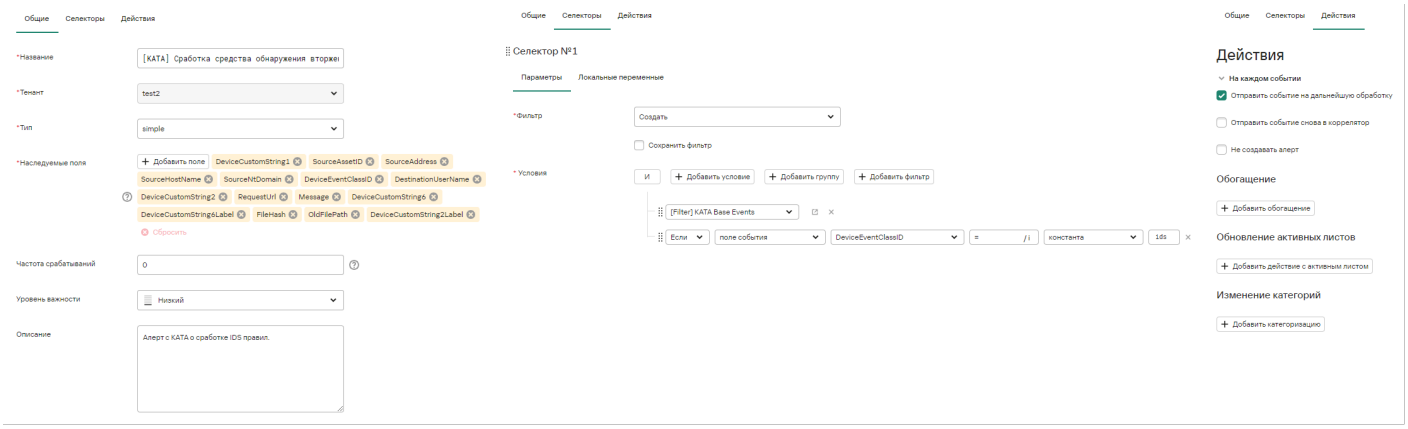
Простое правило (simple)

> **"Обновить параметры"** нужно делать в коррелляторе, когда какое-либо правило меняется, чтобы подтянулись актуальные изменения в правилах в коррелятор.

Простое правило (simple) — срабатывает при обнаружении каждого события, удовлетворяющего условиям в одном селекторе.

Типовой пример правила:



Параметр **Наследуемые поля (Identical fields)** имеет разный смысл, в зависимости от типа правила. В простом правиле он просто перечисляет, какие поля базового события коррелятор скопирует в корреляционное событие при срабатывании правила. Этот параметр обязательный, поэтому хотя бы одно такое поле нужно задать.

Например, если простое правило срабатывает на события о сетевых атаках, в идентичных полях уместно будет перечислить поля с информацией, характеризующие атаку: адрес злоумышленника, адрес жертвы, тип атаки. Аналитику следует посмотреть, в каких полях базовых событий содержится эта информация и перечислить эти поля в Наследуемых полях.

Если аналитик планирует создавать другие правила корреляции, которые реагируют не только на базовые, но и на корреляционные события, то от того, какие поля будут скопированы в корреляционное событие, будет зависеть, какие условия аналитик сможет использовать для такого события.

Простое правило используется, когда нужно создать алерт при обнаружении любого события, которое соответствует определенным условиям. В этом правиле есть только один **селектор**, который определяет эти условия.

Селектор работает как фильтр. В настройках селектора можно выбрать фильтр из существующих ресурсов или создать новый прямо в этом правиле. Также, как и в других

фильтрах, можно использовать ссылки на другие фильтры в более сложных условиях. Например, можно задать условие: "Если поле события равно X" или "Если выполняются условия фильтра Y".

При срабатывании правила аналитик может настроить одно или несколько из следующих **действий**:

- output — создать корреляционное событие, которое будет передано в настроенные точки назначения (обычно это хранилище), и по которому будет создано (или дополнен) алерт
- loop — переслать корреляционное событие на вход этого же коррелятора для рекурсивной обработки
- пополнить активные списки — добавить в активный список (или удалить из списка) запись на основании содержимого полей события
- обогатить корреляционное событие по словарю, по данным исходного события, константой или по шаблону, без запросов во внешние системы (т.е. такое же обогащение как в нормализаторе на коллекторе). Обогащение правилами можно задать в корреляторе отдельно, точно так же как в коллекторе

> Необходимо указывать все поля и переменные участвующие в селекторах в наследуемых полях.

Revision #8
Created 9 August 2023 12:40:46 by Boris Rzr
Updated 24 December 2024 08:12:29 by Boris Rzr