Стандартное правило (standard)

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

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

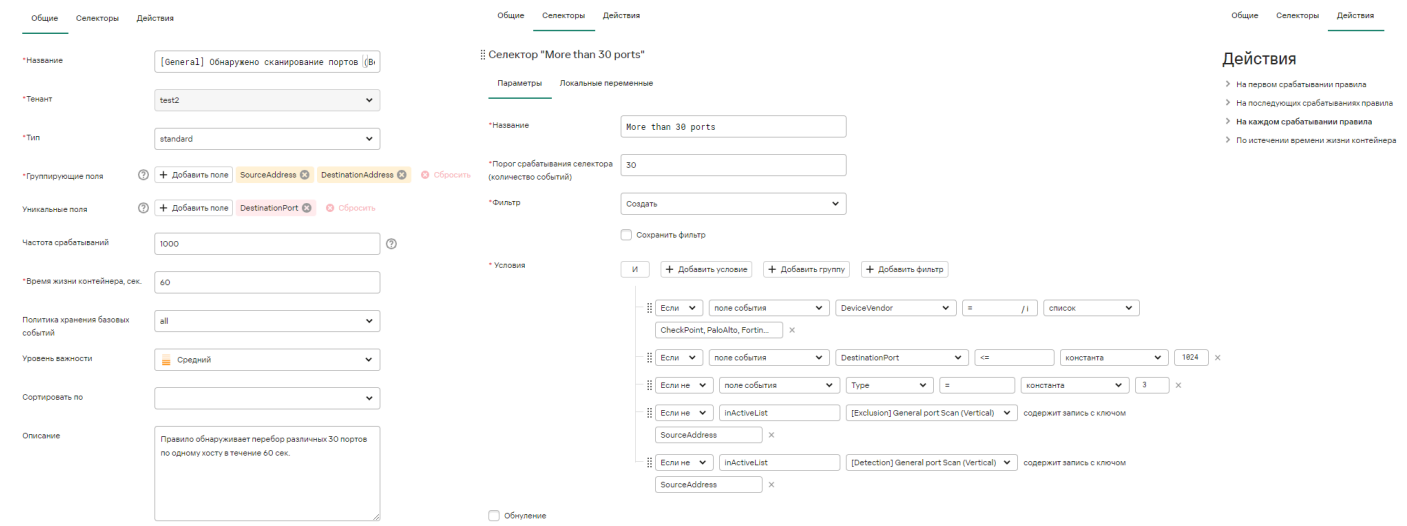
Стандартное правило (standard) — срабатывает при достижении определенного порогового значения группы событий, которые удовлетворяют условиям селектора, полей группировки событий (на основе значений поля создается группа) и времени жизни контейнера для группы.

Если частота срабатывания (Rate limiting) явна не указана, то устанавливается лимит умолчанию - 100 срабатываний в секунду. При превышении лимита правило ничего не делает.

Политика хранения базовых событий (Base events keep policy) - указание, какие из базовых событий должны сохраняться в корреляционном. Возможно указать одно из значений:

- first (по умолчанию) - сохранять только первое базовое событие от каждого селектора в корреляционном событии
- last - сохранять только последнее базовое событие от каждого селектора в корреляционном событии
- all - сохранять все базовые события в корреляционном событии

Типовой пример правила:



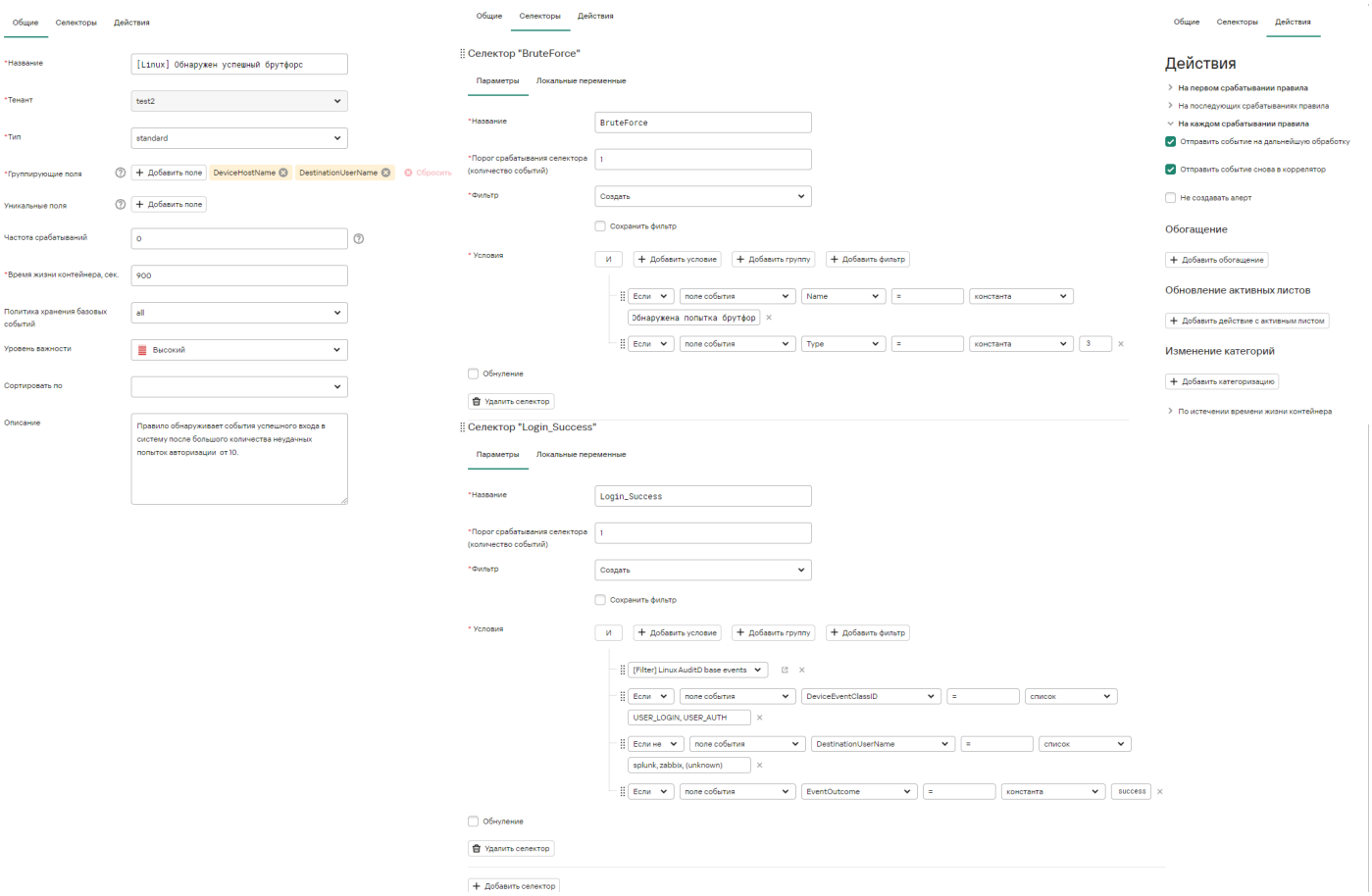
Возможные действия (допускается указать одно или более) правила:

- On first threshold — создавать корреляционное событие только после первого превышения порога, а двукратное, трехкратное и т.д. превышение порога за время жизни группы игнорировать.
- On every threshold — создавать корреляционное событие после каждого превышения порога за время жизни группы.
- On subsequent threshold — создавать корреляционные событие при всех превышениях порога, кроме первого.
- On timeout — в стандартных правилах есть еще возможность настройки действий по окончании времени жизни группы. Это действие используется в связке с опцией Recovery (Обнуление) в настройках селектора, в каких случаях это уместно и как именно это работает рассматривается ниже.

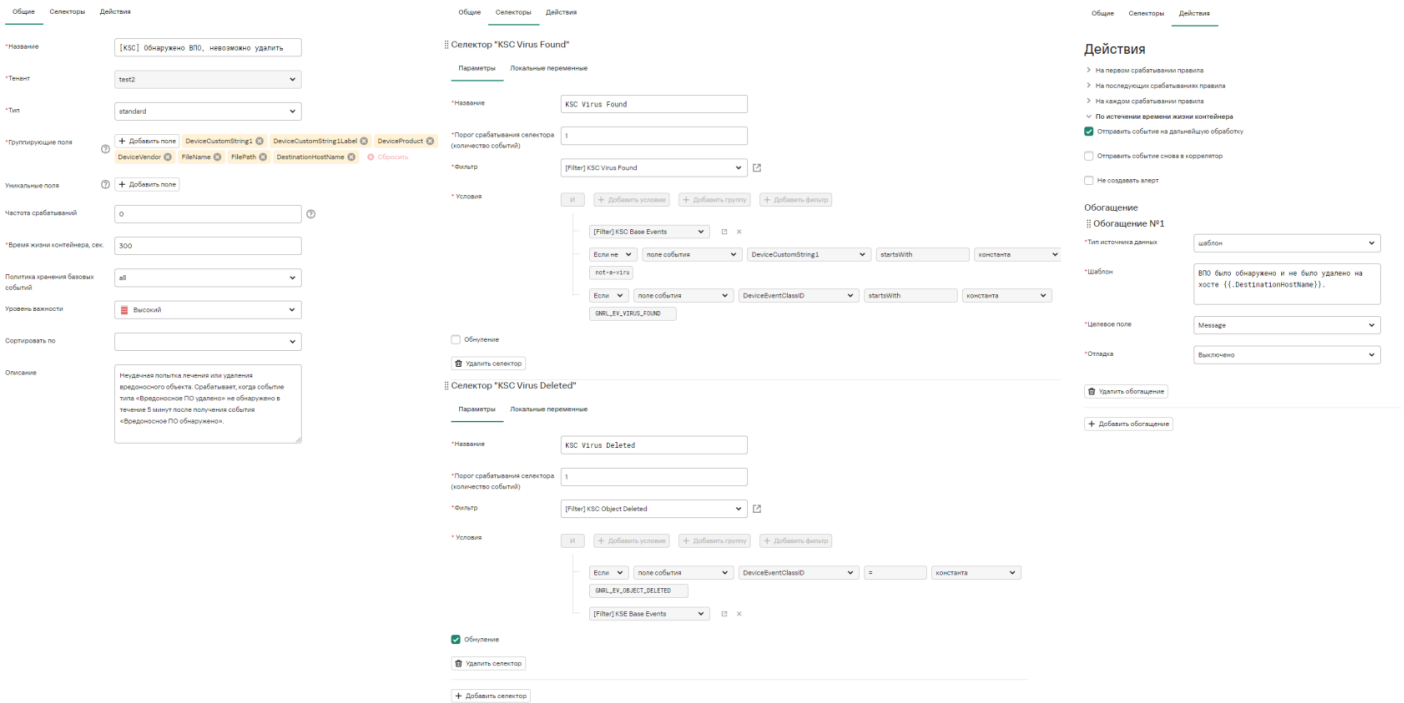
> Необходимо указывать все поля и переменные участвующие в селекторах в группирующих/уникальных полях.

Можно также использовать **несколько селекторов**. Например, несколько неудачных попыток брутфорса (ловится на основе сработки другого правила корреляции) и успешный вход.

Пример правила с несколькими селекторами:



Можно также **рекавери правило**. Например, когда событие типа «Вредоносное ПО удалено» не обнаружено в течение 5 минут после получения события «Вредоносное ПО обнаружено».



Бакет (Окно корреляции)

1. Бакет открывается на событие из любого селектора, не важно в каком они порядке в правиле, порядок проверяется после наполнения бакета!
2. Для каждого набора Identical Fields создается свой бакет.
3. Когда событие подпадает под селектор, коррелятор смотрит, есть ли уже бакет с нужным набором полей Identical Fields, если нет - создает, если есть - событие отправляется в существующий.
4. Когда под селектор с Unique fields подпадает событие, то проверяется, есть ли уже в бакете события с таким же набором значений для Unique Fields, если есть, то событие не учитывается.

Recovery селектор (Обнуление)

1. Бакет открывается только на событие из обычного селектора, на событие из recovery-селектора бакет не открывается никогда!
2. Место нахождения селектора с recovery не имеет значения, как только в бакет попадут все нужные recovery-события бакет будет закрыт!
3. На recovery-селектор не влияет настройка фильтра Order By.
4. Если нужно, чтобы произошло событие А, и не произошло событие Б, при этом событие Б может произойти раньше А, нужно использовать активные листы, т.к. с помощью recovery-селектора такой логики не достичь (см п.1).

Revision #7
Created 9 August 2023 12:44:28 by Boris Rzr
Updated 7 July 2024 08:21:47 by Koala