

В случае нескольких селекторов, в начале лучше указать жесткое условие (например с "=") с полем из стандартной модели данных (не композитных полей S. или N. и т.д.), а затем условия где используются операторы contains или regex.

Операционные правила должны идти вначале:

Редактирование коррелятора



- Общие
- Глобальные переменные
- Корреляция
- Обогащение
- Реагирование
- Маршрутизация
- Проверка параметров

Корреляция

С помощью правил корреляции задаются условия, по которым анализируются поступающие события и, если выполняются условия правил, создаются алерты. Подробнее см. [в онлайн-справке](#).

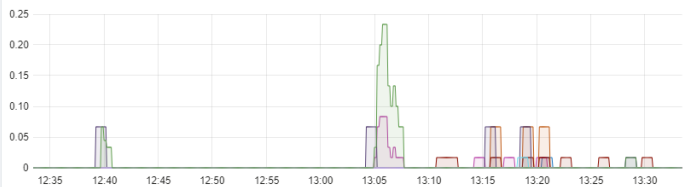
+ Добавить
🔗 Привязать
🗑 Удалить
⬆ Опустить
⬆ Опустить
⋮
Поиск...
🔍

	Правила корреляции	Тип	Действия
<input checked="" type="checkbox"/>	R433_01_Запуск контейнера на неконтейнерной системе	simple	В дальнейшую обработку В коррелятор Обогащение событий
<input checked="" type="checkbox"/>	R230_02_Копирование данных с учетными данными из реестра Windows	simple	В дальнейшую обработку В коррелятор Обогащение событий
<input checked="" type="checkbox"/>	R211_01_Ettercap-аргументы в командной строке (Windows)	simple	В дальнейшую обработку В коррелятор Обогащение событий
<input checked="" type="checkbox"/>	R084_05_Использование ПО для удаленного администрирования (CheckPoint)	simple	В дальнейшую обработку В коррелятор Обогащение событий

Еще, например, есть правило, в котором в переменную кладется значение из активного листа, а затем эта переменная сравнивается в условии. Так вот в этом случае очередность условий имеет большое значение, так как поменяв условия местами и отодвинув проверку по активному листу в конец, в метриках количество OPS с активным листом уменьшилось со 100000 OPS до 1,1 OPS.

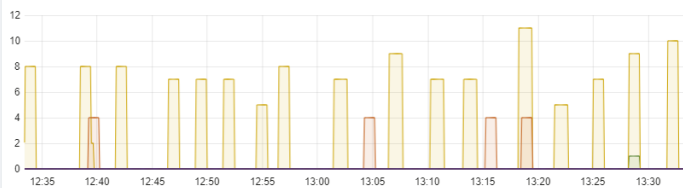
Correlation

EPS



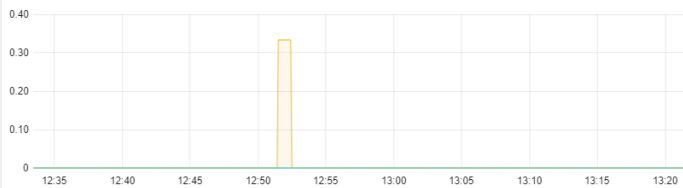
Event Name	max	current
Удален вирус / out Main @ [Example] Correlator @ test-kuma.sales.lab:7249	0.2	0
[test] some dir / out Main @ [Example] Correlator @ test-kuma.sales.lab:7249	0.0	0
[PoC]R202_Обнаружено обращение на подозрительный Domain / out Main @ [Example] Correlator @ test-kuma...	0.1	0
[KATA] Обнаружено вредоносной ссылки в письме / out Main @ [Example] Correlator @ test-kuma.sales.lab:7249	0.0	0
[KATA] Обнаружение вредоносного файла в письме / out Main @ [Example] Correlator @ test-kuma.sales.lab:7249	0.1	0
Vacation additional / out Main @ [Example] Correlator @ test-kuma.sales.lab:7249	0.0	0
Test var timestamp / out Main @ [Example] Correlator @ test-kuma.sales.lab:7249	0.0	0

Buckets



Event Name	max	current
[PoC]R202_Обнаружено обращение на подозрительный Domain Main @ [Example] Correlator @ test-kuma.sale...	4	0
Windows Successful Bruteforce Main @ [Example] Correlator @ test-kuma.sales.lab:7249	11	0
Windows Bruteforce Attempt Main @ [Example] Correlator @ test-kuma.sales.lab:7249	1	0

Rate Limiter Hits



Event Name	max	current
[OP] Add collector to AL Main @ [Example] Correlator @ test-kuma.sales.lab:7249	0.3	0

Active Lists OPS



Event Name	max	current
test_rec_alarm / net Main @ [Example] Correlator @ test-kuma.sales.lab:7249	5.8	1.6

Revision #10

Created 2023-08-09 13:18:42 UTC by Boris RZR

Updated 2026-05-21 08:28:02 UTC by Boris RZR