

??????? ? ??????????

?????????????

??????????? ? ??????????????

AND + Add condition + Add group + Add filter x

- If event field DeviceVendor = constant Microsoft x
- If event field DeviceProduct = constant Windows x

??????????? ? ?????????/??????????

Аналогично =константе **ИЛИ** =константе

AND + Add condition + Add group + Add filter x

If event field Type = list 1, 2

Base events x

- 1
- 2

AND + Add condition + Add group + Add filter x

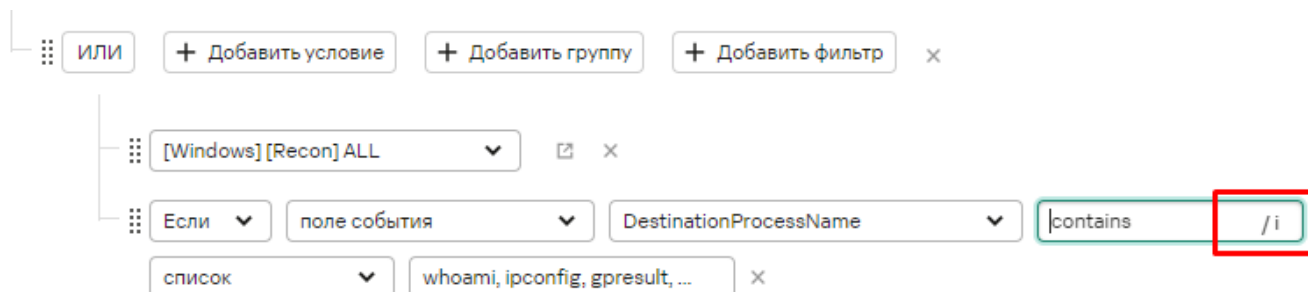
??????????

???????

??????????

????????????????????????????

Ищется заданная подстрока "whoami" или "ipconfig" и др в значении поля DestinationProcessName

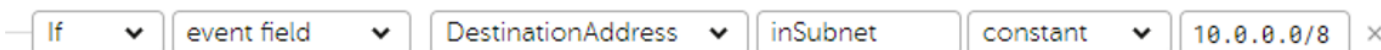


????????????????? ?????????????????? ??????????????????
(REGEX)

Должно быть условие регулярного выражения в формате RE2



????????? ? ??????????????????



????????????? ??????? ?????????????? (?? ??????????)



????????????? ?????????? / ??????

????????????? ?????? ?????????????? ??????

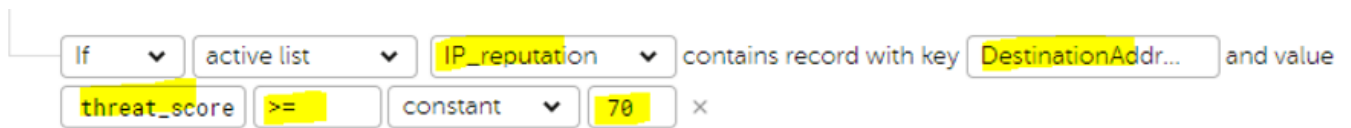
Ключ листа должен совпадать со значением поля *Message*



?????????? ?? ??????? ??????? ? ?????????? ?????? (??????????????
?????)

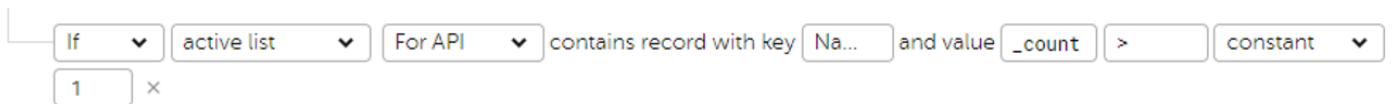
В актуальных версиях, используйте комбинацию Ctrl+Enter для прододжения наполнения условия в конструкторе

Где *threat_score* > 70



??????? ?? ?????????????? ?????????? ?? ?????? ? ??????????? ??????

Где количество записей > 1, используется служебная переменная *_count*



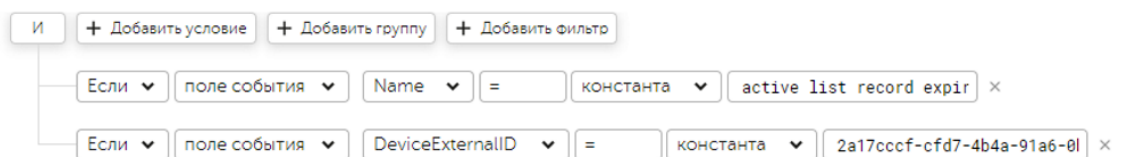
Другие служебные поля активных листов:

- *_count* (счетчик количества записей)
- *_created* (время создания записи UnixTime, в наносекундах)
- *_updated* (время обновления записи UnixTime, в наносекундах)
- *_expires* (время окончания жизни записи UnixTime, в наносекундах)
- *_key* (значение ключевой записи)

????????? ?????????????? ?????????? ?????? ? ??????????? ??????

Возникает служебное событие *active list record expired*, помимо этого необходимо указать UUID активного листа в поле *DeviceExternalID*

* Условия



Значение ключевого поля передается в *DevicePayloadID* служебного события.

?????? ? ?????????? ??????? ?? ?? ??? ID

Если указывать ID листа неудобно (а это обычно так), то можно в ключевое поле писать уникальный префикс типа "failed login attempts|username|1.1.1.1" и в события ловить по полю *devicePayloadID* функцией *startsWith* "failed login attempts" такой вариант реализации правила не зависит от инсталляции.

Такие события существуют только в рамках коррелятора (служебные события) и не сохраняются в сторадже, их можно поймать только правилом корреляции.

????????????? ?????????????? ? ??????????????
?????????????

Из строки с REGEX вырезается число и кладется его в переменную, например, для получения SID пользователя из "SID: 1-21-1231-500", получаем "500", кладем в переменную \$temp, чтобы сделать сравнение необходимо \$temp привести к числовому типу это можно сделать новой переменной `$usersid = $temp + 0` и далее сравнивать, например, `$usersid > 1000`

????????? ? ?????? TI, ?????????????? ? ??????????????????

The screenshot shows a rule configuration interface with the following elements:

- Logic operators: AND, + Add condition, + Add group, + Add filter
- Condition 1: If [dropdown] TI [dropdown] feed KL_IP_Reputation contains record found by DestinationAddress [dropdown] with field category [dropdown]. Sub-condition: contains [dropdown] constant [dropdown] vpn [input type="checkbox"]
- Condition 2: OR [dropdown] + Add condition, + Add group, + Add filter [input type="checkbox"]
- Condition 3: If [dropdown] TIDetect [input type="text"] feed feed contains record found by DestinationAddress [dropdown] [input type="checkbox"]
- Condition 4: If [dropdown] inActiveList [input type="text"] IP blacklist [dropdown] contains record with key DestinationAddress [input type="text"] [input type="checkbox"]

Значение feed это именование фидов из CyberTrace, например для фидов Kaspersky бывают такие значения (зависит какие фиды приобретены/подключены):

Indicators Add Mark as false positive Delete

ioc_value: 192.0.2.* OR (ioc_type: md5 AND ioc_updated_date: >=01.01.2020)

Indicators selected: 0 of 2417532

Type	Value	Added	Changed	Tag	Total tag weight	Suppliers
URL	*.0077x24hr.com	2021-11-24 20:28:08	2023-12-07 09:59:48	No tags	-	Botnet_CnC_URL_Data_Feed
URL	*.1s2.in.ua	2021-11-24 20:28:08	2023-12-07 09:59:48	No tags	-	Botnet_CnC_URL_Data_Feed
URL	*.2023.ebeenj.co...	2023-09-21 14:30:20	2023-12-07 10:00:26	No tags	-	Botnet_CnC_URL_Data_Feed, Malicious_URL_Data_Feed
URL	*.22a.chengxinw...	2021-11-24 20:28:08	2023-12-07 09:59:48	No tags	-	Botnet_CnC_URL_Data_Feed
URL	*.2atbw3gw5r.co...	2022-08-18 22:30:08	2022-12-01 03:30:34	No tags	-	Malicious_URL_Data_Feed
URL	*.2ra8le.com	2023-09-06 20:02:52	2023-12-07 10:00:26	No tags	-	Malicious_URL_Data_Feed

?????? ? ?????????? AD

Необходимо указывать полный DN, пример:

Distinguished name
 cn=administrator,cn=users,dc=soc,dc=env

User logon name
 administrator

Member Of
 { cn=administrators,cn=builtin,dc=soc,dc=env, cn=domain admins,cn=users,dc=soc,dc=env, cn=enterprise admins,cn=users,dc=soc,dc=env, cn=group policy creator owners,cn=users,dc=soc,dc=env, cn=schema admins,cn=users,dc=soc,dc=env }

Условие фильтра:

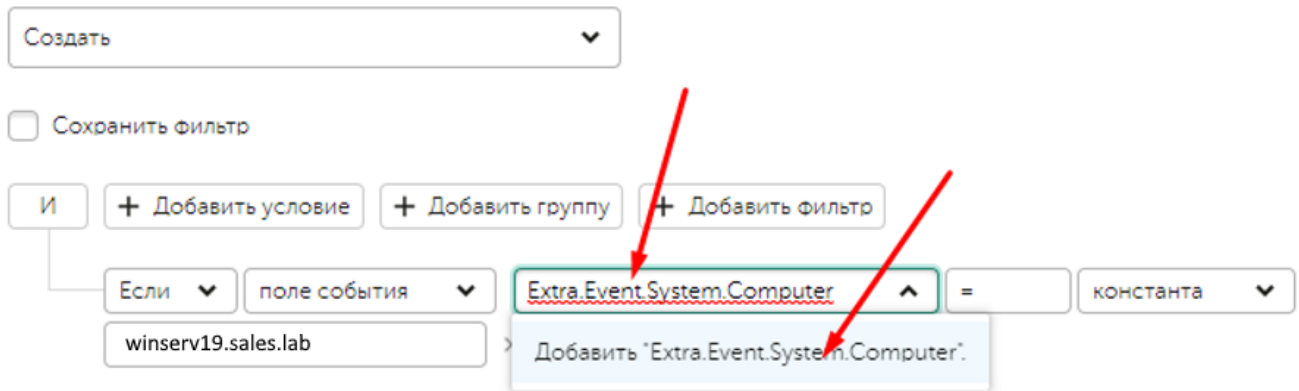
OR + Add condition + Add group + Add filter

If event field DestinationAccountID inActiveDirectoryGroup constant

cn=domain admins,cn=users

????? ?????????? ? ?????????????????? ??????????????

?????? ? ?????? Extra ? ???????????



?????? ? ??????? ????? SA (?????? ??????)
KUMA 3.0+

При операции **match** к полям типа SA применяется как к строке, т.е. массив представляется в виде строки ["a1", "b2", "c3"] и т.д. Т.е. ко всему массиву сразу, а не к отдельным его элементам по очереди.

При операции **contains** применяется именно к элементам массива. Т.е. **contains** [для массива вернет false, как и **contains** " или '. Но при этом же, если в массиве есть элемент abc, то contains abc вернет true и contains ab тоже вернет true

?????? ? ????????????????? (KUMA 2.1+)

???? ? ?????????? ??????

[Документация](#) по функциям переменных (локальные переменные).

Сначала извлекается час из таймштемпа, с помощью функции: `extract_from_timestamp(Timestamp, 'h', 'Europe/Moscow')`

Variable	Value
hour	<code>extract_from_timestamp(Timestamp, 'h', 'Europe/Moscow')</code>

+ Add variable

Условие в селекторе:

AND + Add condition + Add group + Add filter

- If event field Type = list 1,2
- If event field DeviceVendor = constant Microsoft
- If event field DeviceProduct = constant Windows
- If event field DeviceEventClassID = constant 4720

OR + Add condition + Add group + Add filter

- If event field \$hour >= constant 19
- If event field \$hour < constant 8

Переменные необходимо указывать в группирующих полях:

*Наследуемые поля

+ Добавить поле DeviceHostName SourceUserName DestinationUserName \$hour

Сбросить

?????? ? Extra

Здесь вместо `Event.System.Channel` нужно указать интересующее вас поле экстра.

Регулярка: `."Event\.System\.Channel":"([^\"]+)"`

Variable	Value
asd	<code>regex_capture(Extra, '.*"Event\.System\.Channel":"([^\"]+)"')</code>

В некоторых случаях производительней использовать не регулярки, а функции:

- \$firstIndex=index_of('(', fieldName)
- \$lastIndex=index_of('.', fieldName)
- \$getSubstring=substring(fieldName, \$firstIndex, \$lastIndex)

?????? ? ?????????????? ?????????? (KUMA 3.0+)

Исходная задача: Необходимо отслеживать, на каких отличных друг от друга устройствах производится вход одной УЗ. (активный лист будет менее удобен т.к. различных устройств может быть > 1)

Пример Контекстной таблицы:

Редактирование контекстной таблицы ×

Название*

pc-user

Тенант*

Shared ▼

Срок жизни ⓘ

0 ↕

Описание

Схема

+ Добавить
Удалить

	Название	Тип	Ключево...
<input type="checkbox"/>	user	Строка ▼	<input checked="" type="checkbox"/>
<input type="checkbox"/>	pc	Массив строк ▼	<input type="checkbox"/>

Примеры переменных:

Извлечение содержимого поля с массивом `pc` из контекстной таблицы в тенанте `Shared` (только для этого тенанта нужно в переменной это указывать) по ключевому полю `user` и его значением `DestinationUserName`, назовем переменную `ct_value`:

```
context_table('pc-user@Shared', 'pc', 'user', DestinationUserName)
```

В событии выглядит это так:

FlexString1

['zpc1']

Получение индекса (номер символа) по содержимому поля массива `pc` по значению поля `DestinationHostName` из контекстной таблицы в тенанте Shared (только для этого тенанта нужно в переменной это указывать) по ключевому полю `user` и его значением `DestinationUserName`, назовем переменную `ct_contains`:

```
index_of(DestinationHostName, $ct_value)
```

Возвращает первую позицию символа или подстроки в строке, расчет индекса начинается с 0. Если в результате работы функции подстрока не была найдена, функция вернёт значение -9223372036854775808

Вот как выглядит это в событии, значение `ct_contains` в поле FlexNumber1.

FlexNumber1	2
FlexNumber2	1
FlexString1	['zpc1']

Номер символа: 012

Получение количества элементов в поле с массивом `pc` из контекстной таблицы (пример в событии на рисунке выше в поле FlexNumber2), назовем переменную `ct_len`:

```
len($ct_value)
```

Если в содержимом поля с массивом `pc` из контекстной таблицы есть подстрока см. выше описание переменной `ct_contains`, то вернуть `true` назовем переменную `ct_item_exist`:

```
conditional(`$ct_contains LIKE '-.*'`, 'false', 'true')
```

Вот как выглядит это в событии, значение `ct_item_exist` в поле FlexString2.

FlexString1	['zpc1']
FlexString2	true

??? ?????????? ?????????? ?? ??????????????
????????? ? ?????? ?????? ? ?????????? ??????????????
????? Standard

В обогащении можно написать шаблон, в котором можно пройтись по всем подсобытиям и получить список всех полей. Дальше уже с помощью функционала Go template можете сделать что хотите. Для правильной работы метода keep event policy в правиле корреляции должна иметь значение all.

В данном примере можно получить в строку все значения SourceAddress из базовых событий через ";" в корреляционном событии.

Source kind* template

Template*

```
{{ .range .BaseEvents }}{{ .SourceAddress }}; - {{ .end }}
```

Target field* Message

Debug

На выходе получается примерно следующее

EndTime	2024-10-21 10:48:28:274
Message	head; sleep; tail; df; who;
DeviceAddress	192.168.1.171

Revision #21

Created 2023-08-09 13:06:47 UTC by Boris RZR

Updated 2025-08-14 11:20:19 UTC by Boris RZR