

Приемы в правилах корреляции

Сравнение с константой

AND + Add condition + Add group + Add filter x

If event field DeviceVendor = constant Microsoft x

If event field DeviceProduct = constant Windows x

Сравнение с листом/списком

Аналогично =константе **ИЛИ** =константе

AND + Add condition + Add group + Add filter x

If event field Type = list 1, 2

Base events x

AND + Add condition + Add group + Add filter x

1

2

Содержит список констант

регистронезависимый

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

The screenshot shows a query builder interface. At the top, there are buttons: "ИЛИ" (OR), "+ Добавить условие" (Add condition), "+ Добавить группу" (Add group), "+ Добавить фильтр" (Add filter), and a close button "x". Below these, a filter is configured: a dropdown menu shows "[Windows][Recon] ALL", followed by a checkbox and a close button. The main filter is set to "Если" (If) with a dropdown arrow, "поле события" (event field) with a dropdown arrow, "DestinationProcessName" with a dropdown arrow, and the operator "contains". The value field contains "whoami, ipconfig, gresult, ..." with a close button. A red box highlights the "/i" flag at the end of the value field.

Соответствие регулярному выражению (REGEX)

Должно быть условие регулярного выражения в формате RE2

The screenshot shows a query builder interface. The filter is configured as follows: "If" with a dropdown arrow, "event field" with a dropdown arrow, "RequestUrl" with a dropdown arrow, the operator "match", "constant" with a dropdown arrow, and the value "[\\-\\p{L}\\p{N}]+\\. [\\-\\p{L}]" with a close button.

Работа с подсетями

The screenshot shows a query builder interface. The filter is configured as follows: "If" with a dropdown arrow, "event field" with a dropdown arrow, "DestinationAddress" with a dropdown arrow, the operator "inSubnet", "constant" with a dropdown arrow, and the value "10.0.0.0/8" with a close button.

Содержит любое значение (не пустое)

The screenshot shows a query builder interface. The filter is configured as follows: "If not" with a dropdown arrow, "event field" with a dropdown arrow, "TI" with a dropdown arrow, the operator "=", "constant" with a dropdown arrow, and the value "value" with a close button.

Активный лист содержит ключ

Ключ листа должен совпадать со значением поля *Message*

— If ▼ inActiveList ▼ For API ▼ contains record with key Mess... x

Сравнение по экстра данным в активном листе (неключевому полю)

Где *threat_score* > 70

— If ▼ active list ▼ IP_reputation ▼ contains record with key DestinationAddr... and value
threat_score >= constant ▼ 70 x

Сравнение переменной с числовым значением

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`

Условие с полем TI, сравнение с категорией

AND + Add condition + Add group + Add filter

If TI feed KL_IP_Reputation contains record found by DestinationAddress with field category


contains constant vpn x

OR + Add condition + Add group + Add filter x

If TIDetect feed feed contains record found by DestinationAddress x

If inActiveList IP blacklist contains record with key DestinationAddress x

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

 Kaspersky CyberTrace admin Timezone: UTC+3

Dashboard Search Retroscan Indicators Detections Graph Tasks 231 Settings Help

Indicators Add Mark as false positive Delete

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

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	*.2reale.com	2023-09-06 20:02:52	2023-12-07 10:00:26	No tags	-	Malicious_URL_Data_Feed

Фильтр по количеству записей по ключу в активном листе

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

If active list For API contains record with key Na... and value _count > constant

1 x

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)

Событие истечения времени жизни в активном листе

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

* Условия

И
+ Добавить условие
+ Добавить группу
+ Добавить фильтр

Если
поле события
Name
=
константа
active list record expir
×

Если
поле события
DeviceExternalID
=
константа
2a17cccf-cfd7-4b4a-91a6-0l
×

Значение ключевого поля передатся в *DevicePayloadID* служебного события.

Работа с активным листом не по его 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.

Работа с группами 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 x

Актив находится в определенной категории

If event field SourceAssetID inCategory constant HQ/Categorized assets/ x

Работа с полем Extra в селекторе

Создать

☐ Сохранить фильтр

И + Добавить условие + Добавить группу + Добавить фильтр

Если поле события Extra.Event.System.Computer = константа

winserv19.sales.lab

Добавить "Extra.Event.System.Computer".

Работа с полями типа SA (массив строк) 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

Работа с переменными (KUMA 2.1+)

Вход в рабочее время

Документация по функциям переменных.

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

Settings Local variables

Variable	Value
<input type="text" value="hour"/>	<input type="text" value="extract_from_timestamp(Timestamp, 'h', 'Europe/Moscow')"/>

+ Add variable

Условие в селекторе:

AND + Add condition + Add group + Add filter

If event field Type = list 1, 2 x

If event field DeviceVendor = constant Microsoft x

If event field DeviceProduct = constant Windows x

If event field DeviceEventClassID = constant 4720 x

OR + Add condition + Add group + Add filter x

If event field \$hour >= constant 19 x

If event field \$hour < constant 8 x

Переменные необходимо указывать в группирующих полях:

*Наследуемые поля

+ Добавить поле DeviceHostName x SourceUserName x DestinationUserName x \$hour x

Сбросить

Работа с 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>

Работа с контекстной таблицей (КУМА 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*	<input type="text" value="pc-user"/>
Тенант*	<div>Shared</div>
Срок жизни ⓘ	<div>0</div>
Описание	<div></div>

Схема

+ Добавить Удалить

<input type="checkbox"/>	Название	Тип	Ключево...
<input type="checkbox"/>	<input type="text" value="user"/>	<div>Строка</div>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="text" value="pc"/>	<div>Массив строк</div>	<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 -922337203685477580

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

Как записать значение из нескольких событий в одно поле в правиле корреляции типа Standard

В обогащении можно написать шаблон, в котором можно пройти 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 #16

Created 9 August 2023 13:06:47 by Boris RZR

Updated 3 December 2024 08:54:55 by Boris RZR