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

В KUMA во многих местах можно использовать шаблоны для обогащения. Но мало кто знает, что в template можно использовать не только значения полей, например, `{{.DeviceAddress}}`, но и другой функционал шаблонов GO (ссылка).

Ниже приведем несколько полезных лайфхаков, которые сделают ваши события красивыми и упростят обогащение и корреляцию.

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

Обогащать события можно не только классическими полями, например, `{{.DeviceAddress}}`, но и полями Extra, а также переменными.

Шаблон с обычными полем:

```
{{.DeviceAddress}}
```

Шаблон с Extra полем:

```
{{index .Extra "myField"}}
```

Шаблон с переменными (в функциях переменных):

```
template('Значения локальных переменных {{index . 0}} и {{index . 1}} а также {{index . 2}}', $var1, $var2, $var10)
```

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

Чтобы в message вставить текст `"Пользователь user1 на хосте user1-pc.local (10.10.10.10) выполнил команду 'whoami'"`, а hostname и address не всегда могут быть указаны, но хочется красивую надпись без пустых скобок или лишних пробелов, то можно использовать условия:

```
Пользователь {{.DestinationNtDomain}}\{{.DestinationUserName}} на хосте {{if and .DeviceAddress .DeviceHostName}} {{.DeviceHostName}} ({{.DeviceAddress}}) {{else if .DeviceAddress}} {{.DeviceAddress}} {{ else }} {{.DeviceHostName}} {{ end }} выполнил команду "{{.DeviceCustomString4}}"
```

Такой же шаблон можно создать и с Extra-полями. Например, в поле события DeviceProcessName нужно записать значение из Extra-поля myField1, а в случае его отсутствия - myField2:

```
{{if index .Extra "myField1"}}{{index .Extra "myField1"}}{{else}}{{index .Extra "myField2"}}{{end}}
```

Еще пример:

```
{{if eq .DeviceCustomString1 "" }}{{""}}{{else}}{{"vlan"}}{{end}}
```

Также пример с использованием логических операторов `and` и `or`:

```
{{if and (eq .DeviceEventCategory "Application") ((or (eq .DeviceCustomString4 "MSSQL") (eq .DeviceCustomString4 "SQLISPackage")))}}{{.DestinationUserName}}{{end}}
```

Еще пример:

```
{{if and ((eq .DeviceCustomIPv6Address2 "") (not (eq .SourceAddress "")))}}{{.SourceAddress}}{{else}}{{.DeviceCustomIPv6Address2}}{{end}}
```

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

В правилах standard можно в шаблоне указать количество базовых событий, которые попали в окно корреляции:

```
{{ len (.BaseEvents) }}
```

В правилах standard можно в шаблоне перечислить все значения, которые были в базовых событиях:

```
{{range .BaseEvents}} {{.SourceUserName}}{{end}}
```

В правилах standard можно в шаблоне достать значение из конкретного события, используя условия:

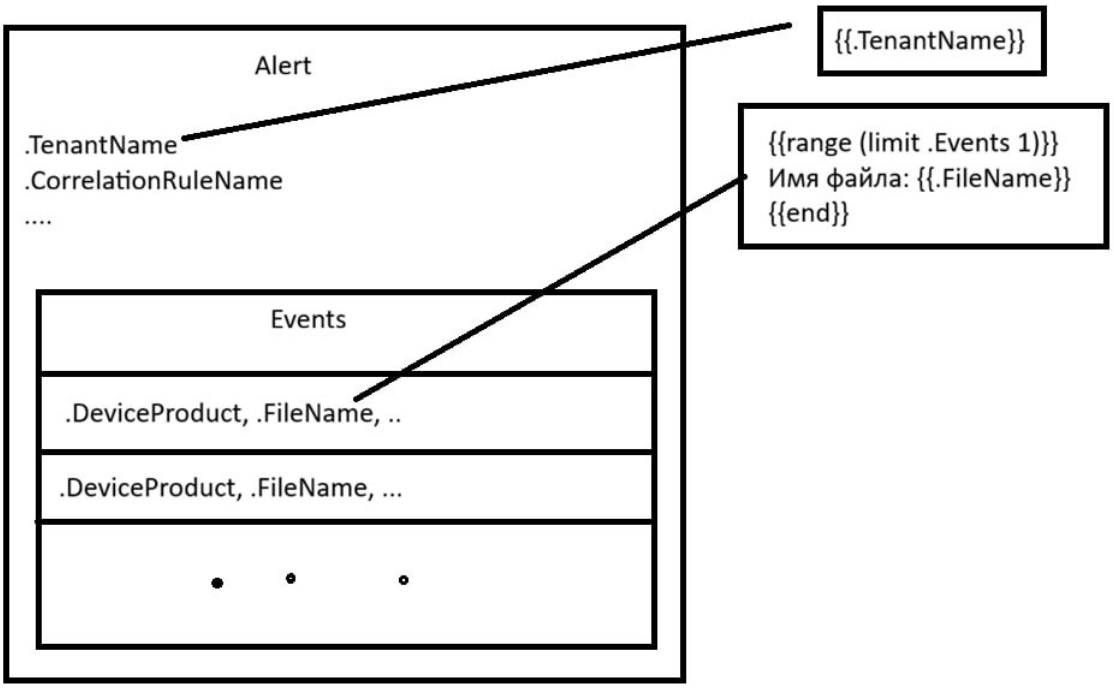
```
{{range .BaseEvents}}{{if eq .DeviceEventClassID "4688"}}{{.DestinationProcessName}}{{end}}{{end}}
```

Также в шаблонах можно использовать переменные, например, можем весь массив сырых событий положить в отдельную переменную $baseEvents и использовать её дальше. Пример ниже сортирует события 4104 по dcn1 и конкатенирует куски ScriptBlockText, чтобы в корреляционном событии получить весь PowerShell скрипт, а не куски из 15,5к символов.

```
{{ $baseEvents := .BaseEvents }}
{{range $index, $element := $baseEvents}}
    {{range $i, $e := $baseEvents}}
        {{if eq $e.DeviceCustomNumber1 (len (printf "a%*s" $index ""))}}
            {{.S.ScriptBlockText}}
        {{end}
    }{{end}}
{{end}}
```

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

В правиле обогащения, когда вы обращаетесь, вы как бы находитесь в событии и можете напрямую обращаться к полям.
Но в шаблоне уведомлений вы находитесь уже в алерте и в нем нет полей события, но сами события есть. Поэтому нужно сначала проитерироваться по Events (корреляционные события) или дополнительно по Events.BaseEvents (базовые события корреляционных) и оттуда достать уже поле, куда вы в правиле корреляции все сложили.



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

Другие варианты работы с шаблонами GO в KUMA:

- https://support.kaspersky.com/kuma/2.1/ru-ru/233508.htm
- https://pkg.go.dev/text/template

Revision #9
Created 2023-08-31 12:38:32 UTC by Koala
Updated 2026-05-27 13:26:57 UTC by Boris Rzr