Лайфхаки для шаблонов

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.

Простое обогащение

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)
```

Обогащение с условиями

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}}
```

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

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

Полезные ссылки

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 #4
Created 31 August 2023 12:38:32 by Koala
Updated 24 October 2023 11:50:12 by Koala