

Сегментация правил корреляции

По умолчанию, если в корреляторе какое-то правило корреляции сработает несколько раз, все созданные в результате этого корреляционные события будут присоединены к одному алерту. Правила сегментации алертов дают возможность определить условия, при которых на основе таких однотипных корреляционных событий будут создаваться разные алерты.

Порядок применения правил сегментации соответствует порядку правил сегментации созданным в интерфейсе KUMA (могут примениться и несколько сегментаций, если сработка правила корреляции соответствует нескольким правилам сегментации)

Блок-схема работы сегментации (спасибо за наработку интегратору):

Уровень важности: Низкий Назначить: Не назначено Закорить алертСоздать инцидентПривязать

Информация об алерте

Уровень важности правила корреляции	Первое появление	Тенант
Низкий	15.09.2023 14:59:05	Main
Наивысшая важность категории активов	Последнее появление	Правило корреляции
Нет значения	15.09.2023 14:59:15	SegRule
Идентификатор алерта		
e9b1bc30-3831-40fa-9746-0036831702c7		

Связанные события

 Время ↓	Информация о событии
  15.09.2023 14:59:15	Code: 777 , SourceUserName: alice
15.09.2023 14:59:13	EndTime: 15.09.2023 14:59:13 , DeviceAddress: 127.0.0.1 , DeviceReceiptTime: 15.09.2023 14:59:13 , DeviceTimeZone: +03:00 , SourceUserName: alice , Code: 777 , Type: Base
Найти в событиях: 1	
  15.09.2023 14:59:10	Code: 777 , SourceUserName: jack
  15.09.2023 14:59:05	Code: 777 , SourceUserName: bob

Для этого нужно создать правило сегментации и привязать его к правилу корреляции. Перейдите в **Ресурсы - Правила сегментации** и нажмите на кнопку **Добавить правило сегментации**. В нашем случае подойдет тип **По группирующим полям**:

Создание правила сегментации

*Название	<input type="text" value="Сегментация по SourceUserName"/>
*Тенант	<input type="text" value="Main"/>
*Тип	<input type="text" value="По группирующим полям"/>
*Группирующие поля правила корреляции	<ul style="list-style-type: none">По фильтруПо группирующим полямПо количеству событий
*Шаблон именованя алертов	<input type="text"/>
Описание	<input type="text"/>

Указываем свой шаблон именованя и группирующее поле - используем поля имени пользователя и **Сохраняем**:

Создание правила сегментации

*Название	<input type="text" value="Сегментация по SourceUserName"/>
*Тенант	<input type="text" value="Main"/>
*Тип	<input type="text" value="По группирующим полям"/>
*Группирующие поля правила корреляции	<input type="button" value="+ Добавить поле"/> <input type="text" value="SourceUserName"/> <input type="button" value="x"/> <input type="button" value="?"/> <input type="button" value="x Сбросить"/>
*Шаблон именованя алертов	<input type="text" value="{{SourceUserName}}"/> <input type="button" value="?"/> <small>Red squiggly underline under SourceUserName</small>
Описание	<input type="text"/>

Далее необходимо привязать правило сегментации к нашему правилу корреляции. Это делается в **Параметры - Алерты - вкладка Сегментация**. Выбираем необходимый тенант, нажимаем кнопку Добавить, Указываем название, Выбираем правило корреляции и добавлем правило сегментации, затем на каждом шаге все **Сохраняем**.

Создать связь правила сегментации



Выключено

*Название

Сегментация по сорсЮзерНейм

*Тенанты и правила корреляции

Общий

BEL

Boris TEST

SegRule

[Siemens] Industry Mall - Failed login

[PoC]R202_Обнаружено обращение на подозрительный Domain

Main

*Правило сегментации



Правило сегментации

Main

sim - Timestamp

Сегментация по SourceUserName

Общий



По итогу, при появлении событий удовлетворяющих правилу корреляции мы получим отдельные алерты на основе SourceUserName.

Алерты

<input type="checkbox"/>		Название	Статус	Назначен
<input type="checkbox"/>		SegRule (jack)	Новый	
<input type="checkbox"/>		SegRule (bob)	Новый	
<input type="checkbox"/>		SegRule (alice)	Новый	
<input type="checkbox"/>		[KUMA] Нет событий от коллектора	Новый	
<input type="checkbox"/>		SegRule	Новый	

Аналогичным образом можно использовать и другие типы правил сегментации.

Revision #6

Created 15 September 2023 11:46:11 by Boris RZR

Updated 7 July 2024 08:24:17 by Koala