

# 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):

## Работа механизма сегментации алертов

Сервисы Коллекторы Ядро

**События**

- базовые нормализованные (Type = 1)
- агрегированные (Type = 2)
- корреляционные (Type = 3)
- внутреннего аудита (Type = 4)
- политик мониторинга (Type = 5)

Сервис Коррелятор

- Правила корреляции
- Правила обогащения
- Правила реагирования

Корр. сработка по правилу (Type=3)

Сработка может уходить обратно в коррелятор на повторную обработку

### Варианты сегментации:

По группирующим полям

По фильтру

Шаблон именование Алерта

По количеству событий

- Порядок применения правил сегментации соответствует порядку правил сегментации созданным в интерфейсе КУМА (могут применяться и несколько сегментаций, если сработка правила корреляции соответствует нескольким правилам сегментации)
- Одно правило сегментации может быть переиспользовано для множества правил корреляции

В правиле указано "создавать Алерт"?

ДА

НЕТ

Сработка просто сохраняется в хранилище

Проверяется привязано ли к правилу корреляции правило сегментации?

ДА

НЕТ

Уже есть открытый сегментированный Алерт с такими же значениями условий сегментации

ДА

НЕТ

Сегментированный Алерт переполнен?

НЕТ

ДА

Новая сработка добавляется к существующему сегментированному Алерту по данному правилу

Сработка просто сохраняется в хранилище, не попадая в сегментированный Алерт

Создается новый сегментированный Алерт

Уже есть открытый Алерт по данному правилу

ДА

НЕТ

Создается новый Алерт

Алерт переполнен?

ДА

НЕТ

Новая сработка добавляется к существующему Алерту по данному правилу

Сработка просто сохраняется в хранилище

Дальнейшие возможные действия с Алертами:

### Автоматические

Обрабатывает правило уведомлений, отправляется Email с информацией о новом Алерте

Новый Алерт уходит в IRP/SOAR

IRP/SOAR запрашивает новые добавленные к Алерту корреляционные сработки по API

### Ручные

Аналитик SOC берёт новый Алерт в работу, проверяет достаточность данных и выполняет проверку на False Positive. По итогам проверки:

Закрывает Алерт как FP

Создаёт на основе Алерта новый Инцидент

Связывает Алерт с существующим Инцидентом

Пример работы, есть правило корреляции, которое срабатывает на событие с полем Code равное "777" с разными значениями SourceUserName, все сработки правила складываются в один Алерт, мы хотим создать отдельные алерты для отдельных пользователей:

### 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	<a href="#">SegRule</a>
Идентификатор алерта		
e9b1bc30-3831-40fa-9746-0036831702c7		

### Связанные события

<div></div> Время ↓	Информация о событии
<div>✓</div> <div></div> 15.09.2023 14:59:15	Code: 777 , SourceUserName: <div>alice</div>
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
<a href="#">Найти в событиях: 1</a>	
<div>&gt;</div> <div></div> 15.09.2023 14:59:10	Code: 777 , SourceUserName: <div>jack</div>
<div>&gt;</div> <div></div> 15.09.2023 14:59:05	Code: 777 , SourceUserName: <div>bob</div>

Для этог онужно создать правило сегментации ипривязать 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

Сегментация по SourceUserName

\*Тенант

Main

\*Тип

По группирующим полям

\*Группирующие поля правила корреляции

\*Шаблон именования алертов

По фильтру

По группирующим полям

По количеству событий

Описание

Указываем свой шаблон именования 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	<div><div>+ Добавить поле</div><div>SourceUserName <div>×</div></div><div><div>×</div> Сбросить</div></div> <div>?</div>
*Шаблон именования алертов	<div><div>{{.SourceUserName}}</div><div>?</div></div>
Описание	<div></div>

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