Создание TAA-алертов в KUMA с KATA

Введение

При отправке событий из KATA в KUMA есть известная проблема: KATA отправляет сообщение о TAA-сработке только при первой сработке на хосте, а само Syslog сообщение не содержит достаточной информации. События из телеметрии KEDR в свою очередь не содержат идентификатора алерта в KATA в связи с чем отсутствует возможность создания ссылки на карточку алерта в KATA.

В этой статье представлен вариант решения этой проблемы, который позволяет создавать алерт в KUMA идентичный TAA-алерту в KATA, со всеми связанными событиями телеметрии.

Требования

Для работы метода требуется установленная KUMA версии 2.1 или выше, а также KATA версии 5.0 или выше.

На KUMA должна быть настроены коллекторы для приема Syslog сообщений от KATA **и** телеметрии от KEDR. Информацию по настройке данных источников можно найти в соответствующих статьях (ссылки приведены для последних версий).

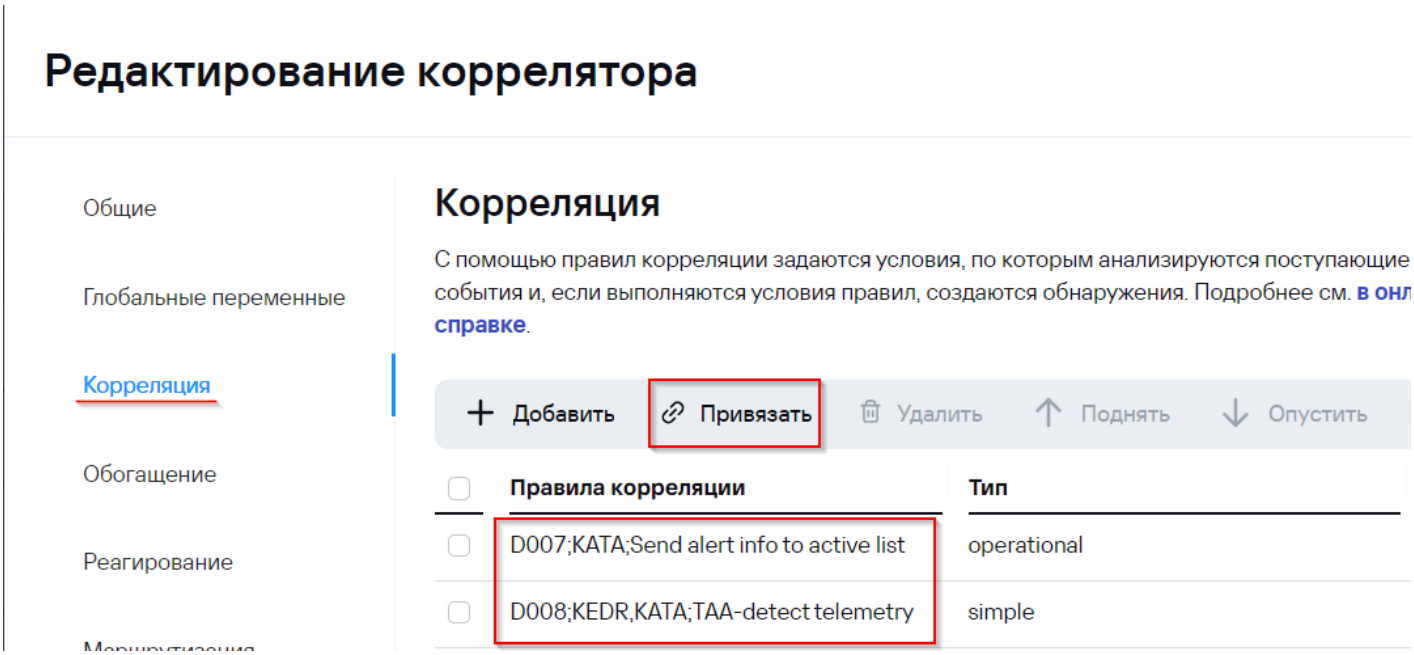
Оба коллектора должны отправлять события в коррелятор.

Реализация

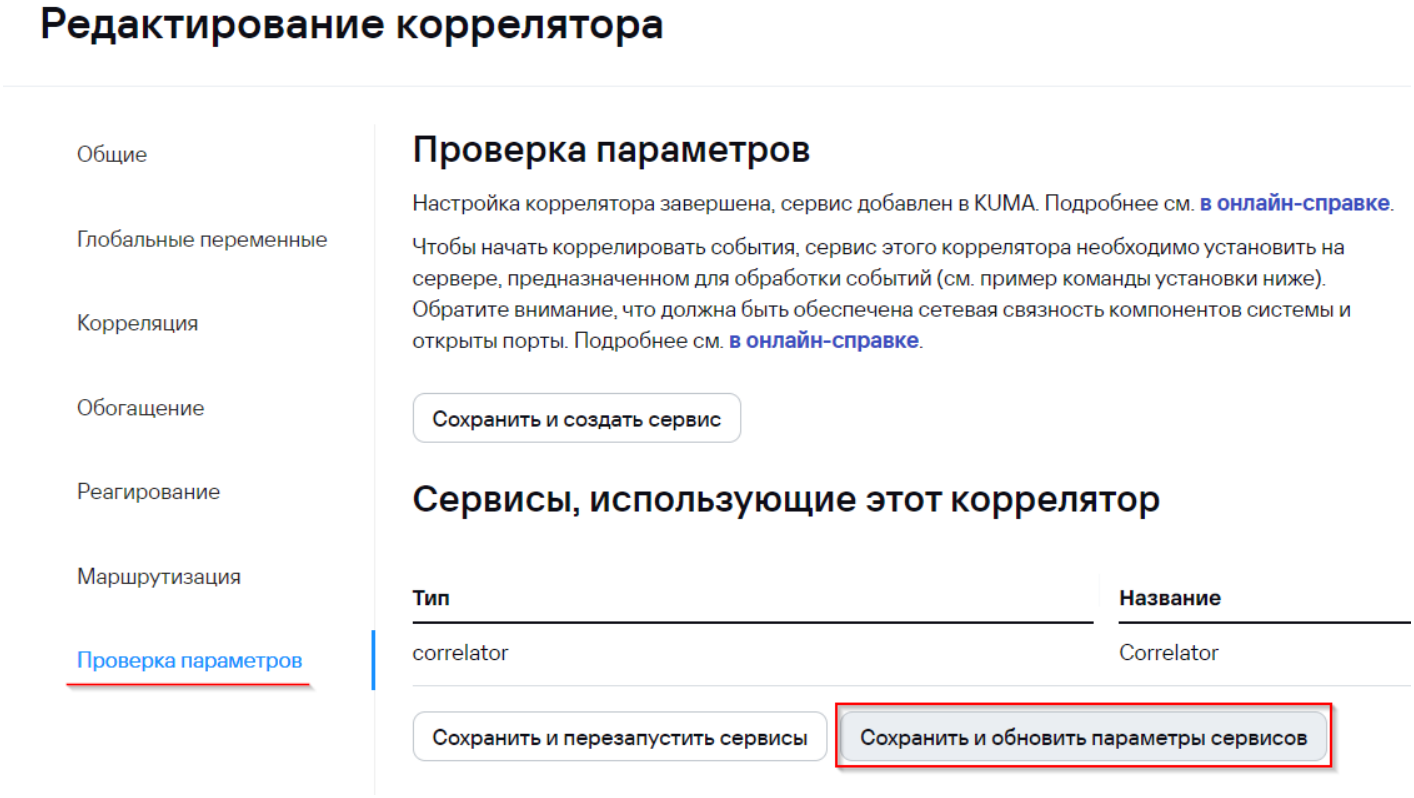
1. Загрузить пакет ресурсов по ссылке: https://github.com/KUMA-Community/kuma_taa_alert

2. Импортировать все ресурсы из пакета в KUMA.

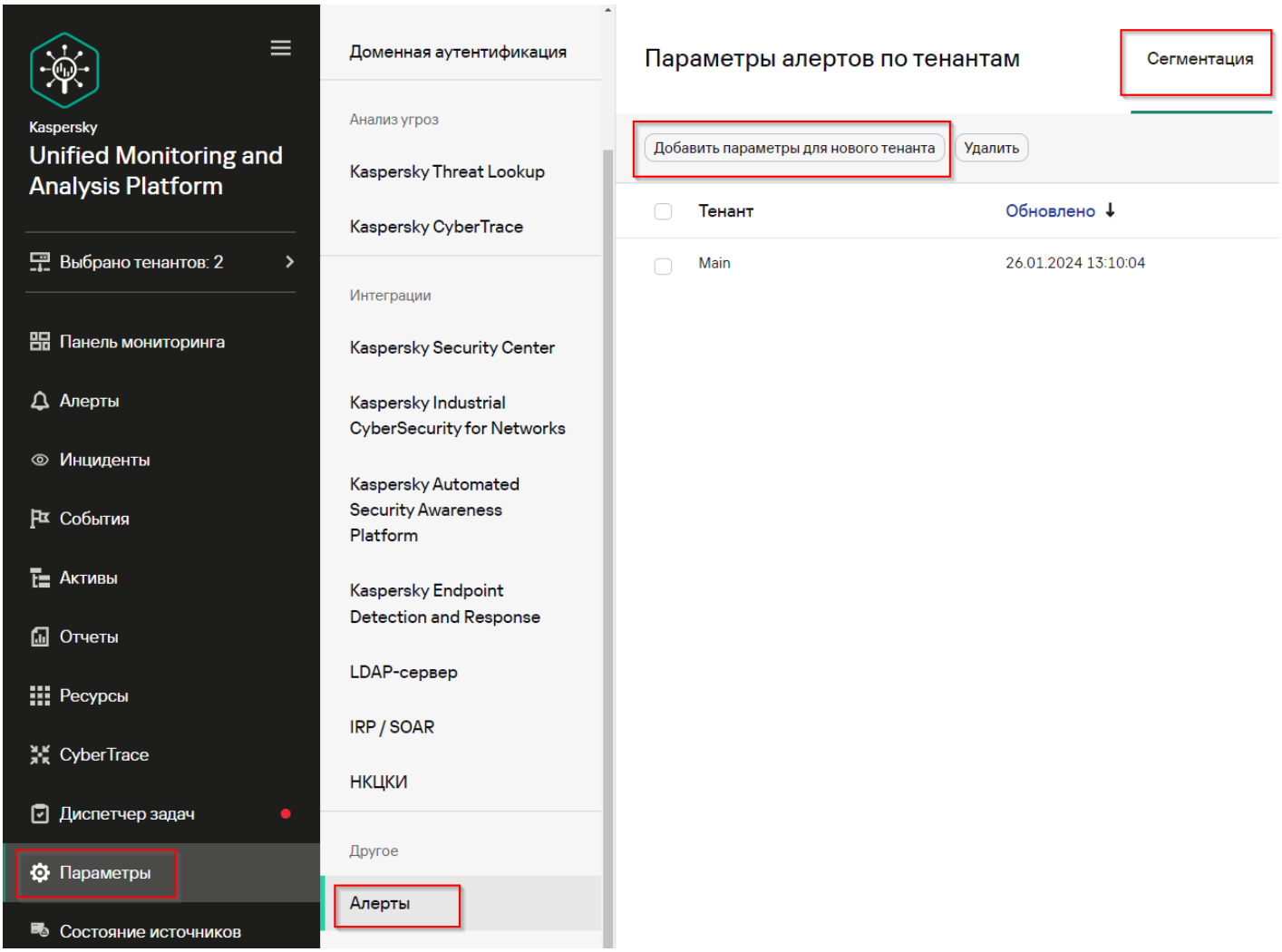
3. Перейти в Коррелятор, перейти на шаг Корреляция и привязать правила корреляции D007 и D008



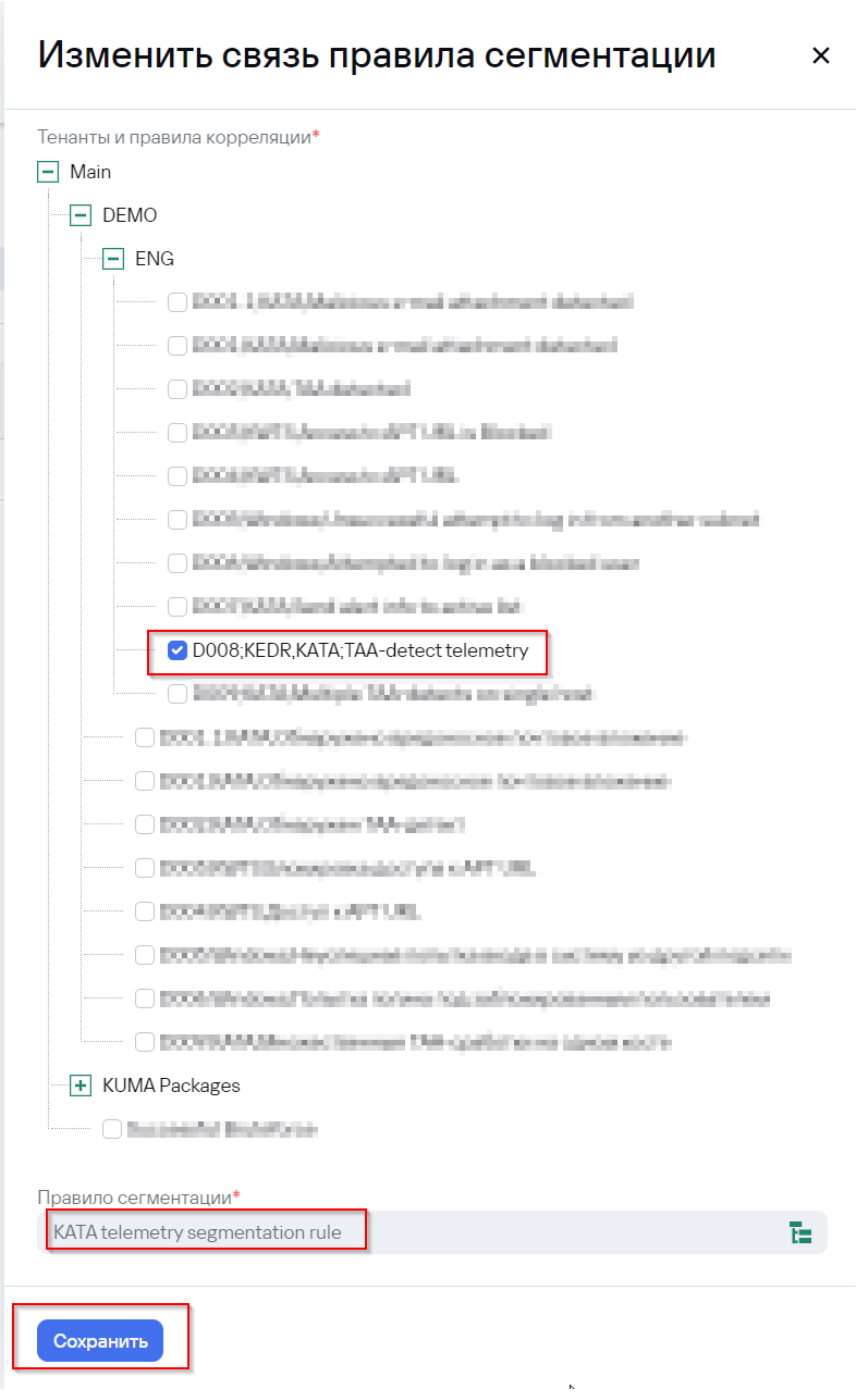
4. Перейти на шаг Проверка параметров и обновить параметры сервиса коррелятора



5. Перейти в веб-интферфейсе в Параметры -> Алерты -> Сегментация и нажать Добавить параметры для нового тенанта (если в KUMA не настроены никакие правила сегментации), либо нажать на соответствующий тенант в списке (если в KUMA уже настроены какие-либо правила сегментации).



6. Создайте связь правила корреляции и правила сегментации как на рисунке ниже:



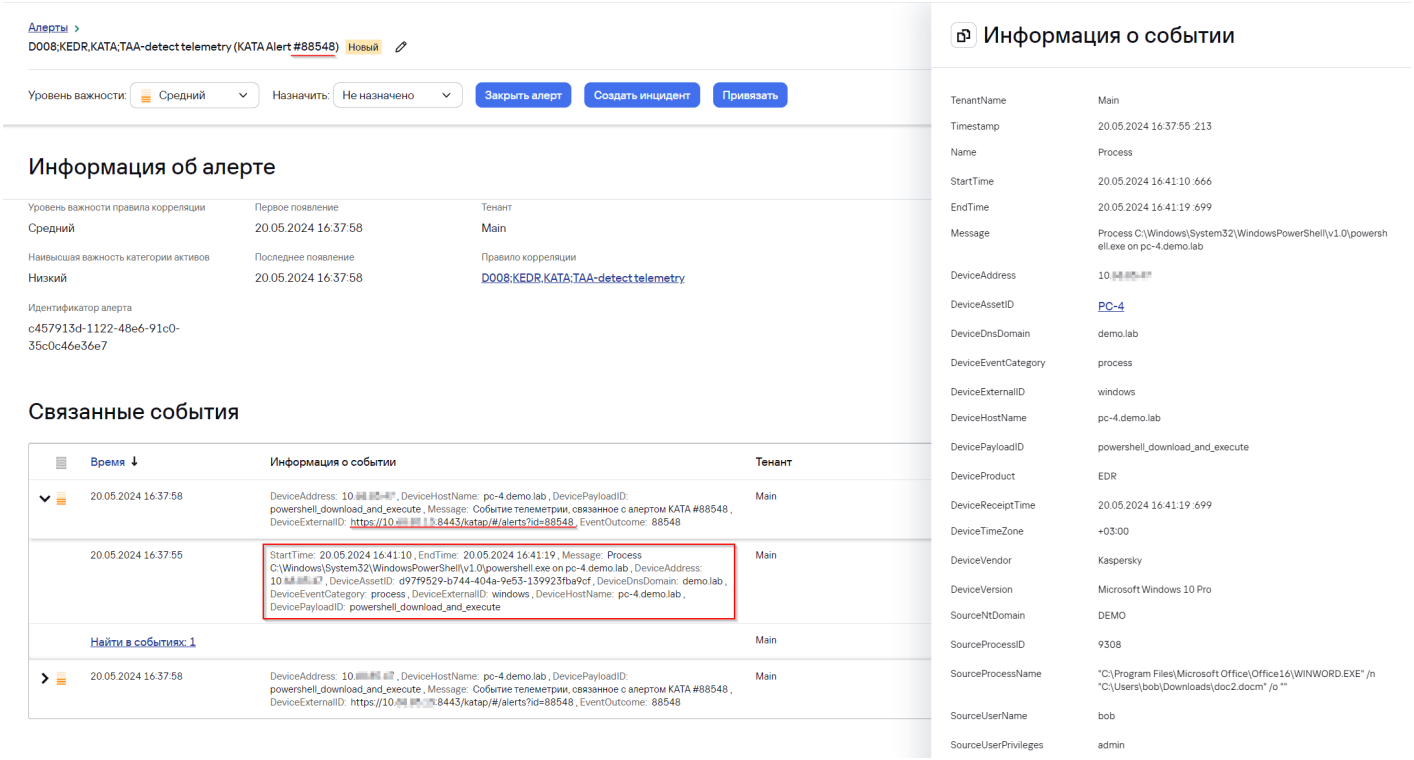
7. Сохраните все внесенные изменения.

На этом настройка завершена.

Результат

В результате проделанных манипуляций в KUMA на каждую TAA сработку будет возводиться алерт, в который согласно правилу сегментации будут добавляться все события телеметрии связанные с данной сработкой. Сам алерт будет содержать ID алерта KATA, ссылку на алерт KATA (для этого необходимо на коллекторе для сбора Syslog с KATA добавить обогащение **[OOTB] KATA alert**), а также связанные события телеметрии от KEDR.

Ниже представлен скриншот алерта в KUMA



А также соответствующий алерт в KATA

И связанные с ним события телеметрии

Threat Hunting

```
IOAId = "b85fdcf0-69a9-0a64-4daa-3d5dfbbc70ea" AND Host = "pc-4.demo.lab"
```

Refresh

All events (2 events)

Event time ↑	Event type	Host name	Details
2024-05-20 16:41:25.150	Process started	pc-4.demo.lab	File: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Importance: High Hash: SHA256 MD5
2024-05-20 16:41:10.667	Process started	pc-4.demo.lab	File: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Importance: High Hash: SHA256 MD5

Revision #3
Created 30 May 2024 11:18:01 by Koala
Updated 19 July 2024 14:37:44 by Koala