Обогащение произвольного поля с утилитой Tracer

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Утилита (скрипт) была написана для получения возможности обогощать событие по значению поля со сторонних систем с использованием языка программирования Python3. Tracer.py мимикрирует под механизм обогащения аналогично CyberTrace, с обогащенными данными можно работать подобно обогащению Threat Intelligence. Утилита может работать как на Linux (рекомендуется), так и Windows платформах (ОС).

> **Для продвинутых пользователей!** Для работы с Tracer.py требуются навыки программирования Python3

Скрипт можно загрузить по ссылке в Пресейл-Паке контенте.

Необходимые библиотеки для работы Tracer.py:

- import socket
- from select import select
- from signal import signal
- from sys import platform
- from re import match
- from datetime import datetime
- from dateutil.relativedelta import relativedelta

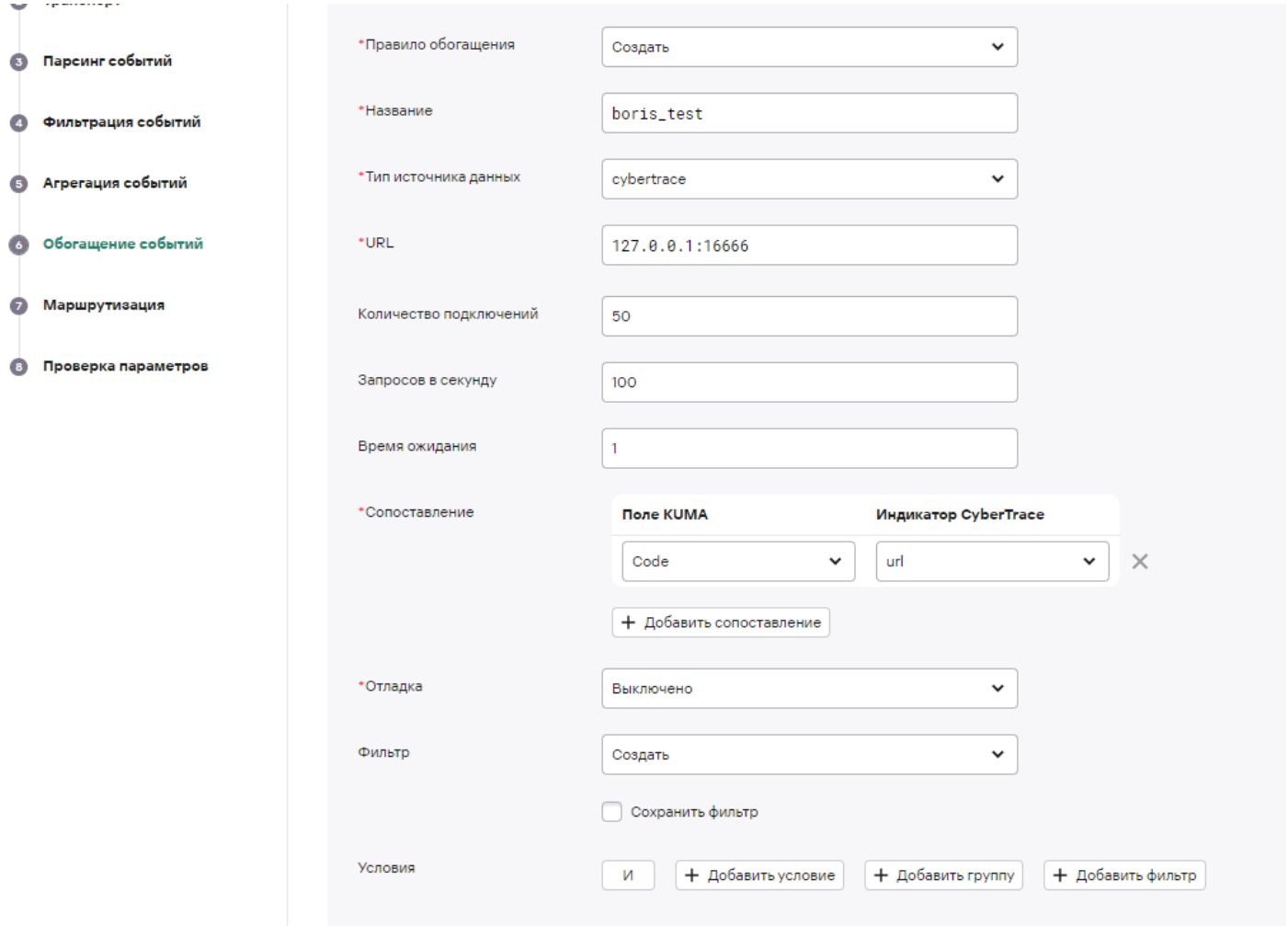
Для использования TCP_FASTOPEN (рекомендуется) на ОС Linux выполните команду ниже:

```
echo 3 > /proc/sys/net/ipv4/tcp_fastopen
```

Предварительные правки для Tracer.py:

- SERVER = "127.0.0.1" (строка кода 14) - укажите IP-адрес для прослушивания
- PORT = 16666 (строка кода 15) - укажите порт для прослушивания
- Обогащение данными производится в строках 72-74, в переменную somedata можно добавить произвольные данные полученные любым способом (из файла, БД, GET запросом и т.д.), таже можно использовать и другие поля (см строку 74 кода - extraInfo=KUMA_THE_BEST_SIEM) с разделитетем "|"

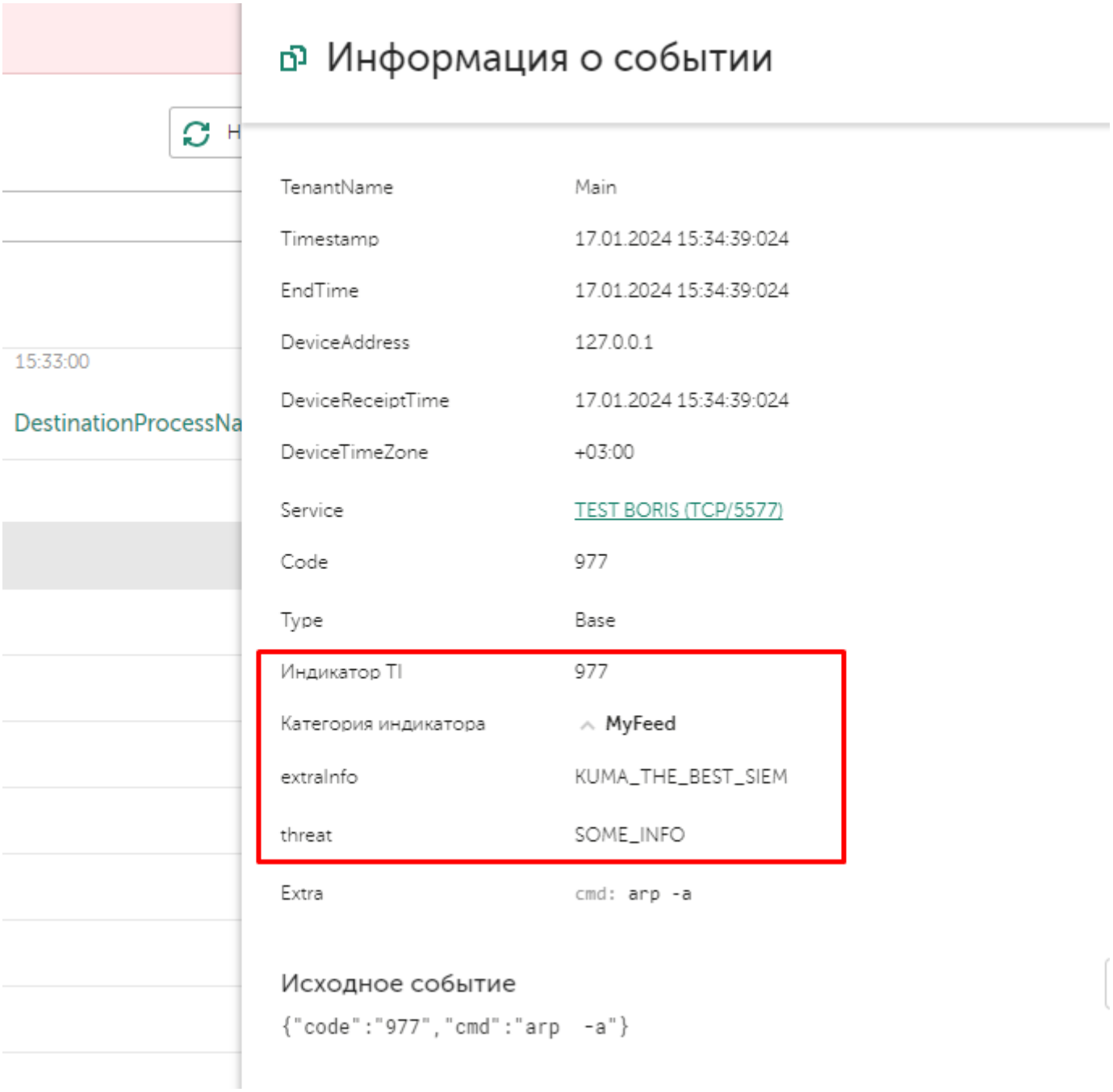
На стороне KUMA нужно прописать следующее обогащение:



По картинке выше, обогащается значение поля Code и сопоставляется с полем Tracer - url. Производительность скрипта состовляет ~ 50 EPS, при рекомендуемой настройке Enrichment: 50 connections и 100 RPS.

> Возможно использовать только поле url в сопоставлении, но туда можно поместить произвольные данные

При обогащении события получаем следующие обогащенные данные:



Так как используется "нелегальный" механизм обогащения в логах коллектора копятся (периодически очищайте) ошибки следующего вида:

```
2024-01-17T15:35:00.340+0300    error   enrichment method 'boris_test'  /opt/tfs-agent/_work/1/s/sdk/enrichment/async_rule_cybertrace.go:165    EOF
kuma/sdk/enrichment.(*asyncRuleCybertrace).worker
        /opt/tfs-agent/_work/1/s/sdk/enrichment/async_rule_cybertrace.go:165
2024-01-17T15:35:00.378+0300    error   enrichment method 'boris_test'  /opt/tfs-agent/_work/1/s/sdk/enrichment/async_rule_cybertrace.go:165    EOF
kuma/sdk/enrichment.(*asyncRuleCybertrace).worker
        /opt/tfs-agent/_work/1/s/sdk/enrichment/async_rule_cybertrace.go:165
2024-01-17T15:35:00.395+0300    error   enrichment method 'boris_test'  /opt/tfs-agent/_work/1/s/sdk/enrichment/async_rule_cybertrace.go:165    EOF
kuma/sdk/enrichment.(*asyncRuleCybertrace).worker
        /opt/tfs-agent/_work/1/s/sdk/enrichment/async_rule_cybertrace.go:165
2024-01-17T15:35:00.415+0300    error   enrichment method 'boris_test'  /opt/tfs-agent/_work/1/s/sdk/enrichment/async_rule_cybertrace.go:165    EOF
kuma/sdk/enrichment.(*asyncRuleCybertrace).worker
```

Revision #4
Created 18 January 2024 07:29:52 by Boris Rzr
Updated 7 July 2024 08:06:29 by Koala