Обогащение произвольного поля с утилитой Tracer

?????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? **НЕ** ???????? ??????????? ????????????? ???????.



??????? (??????) ???? ???????? ??? ????????? ??????????? ????????? ??????? ?? ???????? ???? ?? ????????? ?????? ? ????????????? ????? ???????????????? Python3. Tracer.py ??????????? ??? ???????? ?????????? ?????????? CyberTrace, ? ??????????? ??????? ????? ???????? ??????? ?????????? Threat Intelligence. ??????? ????? ???????? ??? ?? Linux (?????????????), ??? ? Windows ?????????? (??).

Для продвинутых пользователей! ??? ?????? ? Tracer.py ????????? ?????? ???????????????? Python3

?????? ????? ????????? ?? ?????? ? ???????-???? ????????.

??????????? ?????????? ??? ?????? 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

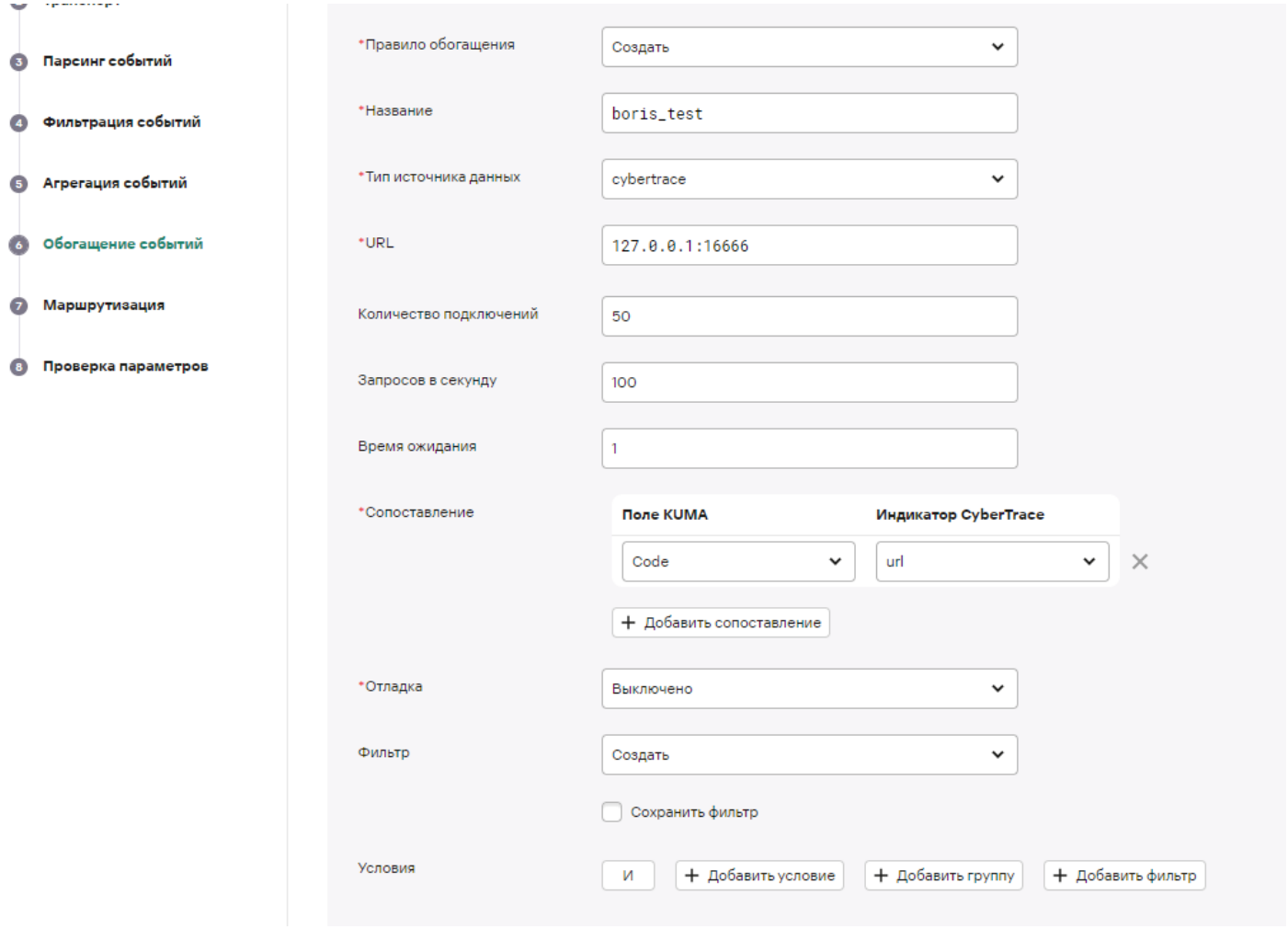
??? ????????????? TCP_FASTOPEN (?????????????) ?? ?? Linux ????????? ??????? ????:

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

????????????????? ?????? ??? Tracer.py:

- SERVER = "127.0.0.1" (?????? ???? 14) - ??????? IP-????? ??? ?????????????
- PORT = 16666 (?????? ???? 15) - ??????? ???? ??? ?????????????
- ?????????? ??????? ???????????? ? ??????? 72-74, ? ?????????? somedata ????? ???????? ???????????? ?????? ?????????? ????? ???????? (?? ?????, ??, GET ???????? ? ?.?.), ???? ????? ???????????? ? ?????? ???? (?? ?????? 74 ???? - extraInfo=KUMA_THE_BEST_SIEM) ? ???????????? "|"

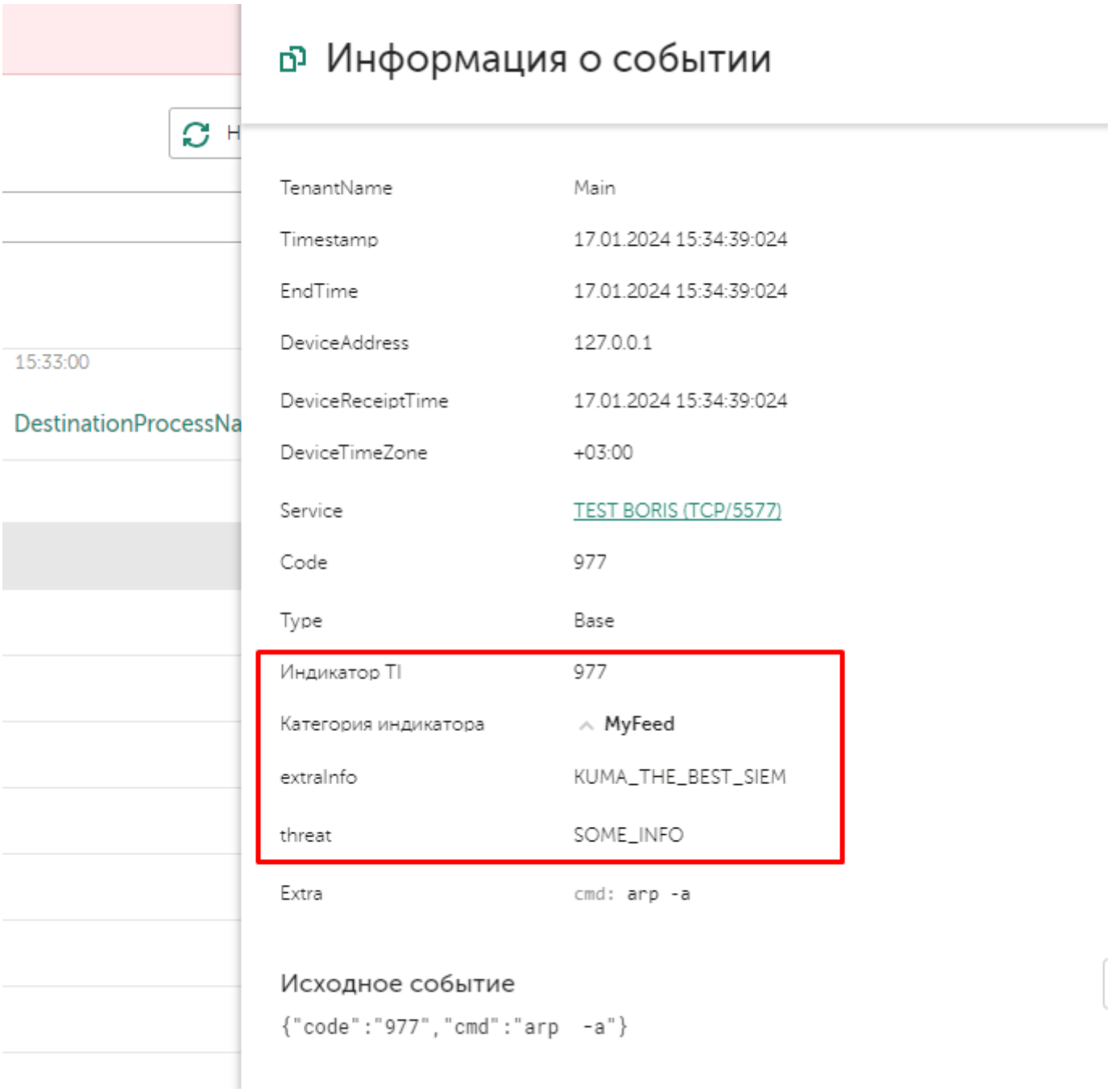
?? ??????? KUMA ????? ????????? ????????? ??????????:



?? ???????? ????, ??????????? ???????? ???? Code ? ????????????? ? ????? Tracer - url. ????????????????? ??????? ?????????? ~ 50 EPS, ??? ???????????? ????????? Enrichment: 50 connections ? 100 RPS.

> ???????? ???????????? ?????? ???? url ? ?????????????, ?? ???? ????? ????????? ???????????? ??????

??? ?????????? ??????? ???????? ????????? ??????????? ??????:



??? ??? ???????????? "????????????" ???????? ?????????? ? ????? ?????????? ??????? (???????????? ????????) ?????? ?????????? ????:

```
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 2024-01-18 07:29:52 UTC by Boris Rzr
Updated 2024-07-07 08:06:29 UTC by Koala