

# ???????????????????????????????? ????? ? ?????????????? 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 обогащать 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.), также можно использовать и другие поля (см строку 74 кода - extraInfo=KUMA\_THE\_BEST\_SIEM) с разделителем "|"

На стороне KUMA нужно прописать следующее обогащение:

The screenshot shows the configuration interface for creating an enrichment rule in KUMA. The sidebar on the left lists the following steps:

- 3 Парсинг событий
- 4 Фильтрация событий
- 5 Агрегация событий
- 6 Обогащение событий
- 7 Маршрутизация
- 8 Проверка параметров

The main configuration form includes the following fields and options:

- \*Правило обогащения:** Создать
- \*Название:** boris\_test
- \*Тип источника данных:** cybertrace
- \*URL:** 127.0.0.1:16666
- Количество подключений:** 50
- Запросов в секунду:** 100
- Время ожидания:** 1
- \*Сопоставление:**
  - Поле KUMA: Code
  - Индикатор CyberTrace: url
  - + Добавить сопоставление
- \*Отладка:** Выключено
- Фильтр:** Создать
- Сохранить фильтр
- Условия:** И, + Добавить условие, + Добавить группу, + Добавить фильтр

По картинке выше, обогащается значение поля Code и сопоставляется с полем Tracer - url. Производительность скрипта составляет ~ 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:

## Информация о событии



TenantName	Main
Timestamp	17.01.2024 15:34:39:024
EndTime	17.01.2024 15:34:39:024
DeviceAddress	127.0.0.1
DeviceReceiptTime	17.01.2024 15:34:39:024
DeviceTimeZone	+03:00
Service	<a href="#">TEST BORIS (TCP/5577)</a>
Code	977
Type	Base
Индикатор TI	977
Категория индикатора	^ MyFeed
extralInfo	KUMA_THE_BEST_SIEM
threat	SOME_INFO
Extra	cmd: arp -a

### Исходное событие

```
{"code": "977", "cmd": "arp -a"}
```

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

```
/opt/tfs-agent/_work/1/s/sdk/enrichment/async_rule_cybertrace.go:165
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