

# 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 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 KUMA configuration interface for creating an enrichment rule. On the left is a sidebar with a vertical list of steps: 3 Парсинг событий, 4 Фильтрация событий, 5 Агрегация событий, 6 Обогащение событий (highlighted in green), 7 Маршрутизация, and 8 Проверка параметров. The main area contains the configuration form for the enrichment rule.

*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	<table border="1"><thead><tr><th>Поле KUMA</th><th>Индикатор CyberTrace</th></tr></thead><tbody><tr><td>Code</td><td>url</td></tr></tbody></table> <div>+ Добавить сопоставление</div>	Поле KUMA	Индикатор CyberTrace	Code	url
Поле KUMA	Индикатор CyberTrace				
Code	url				
*Отладка	Выключено				
Фильтр	Создать				
	<input type="checkbox"/> 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:

15:33:00

DestinationProcessName

Индикатор TI

Категория индикатора

extralInfo

threat

Extra

Исходное событие

Информация о событии

TenantName

Timestamp

EndTime

DeviceAddress

DeviceReceiptTime

DeviceTimeZone

Service

Code

Type

977

Base

977

MyFeed

KUMA\_THE\_BEST\_SIEM

SOME\_INFO

cmd: arp -a

{"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 18 January 2024 07:29:52 by Boris RZR

Updated 7 July 2024 08:06:29 by Koala