# misp-grafana


Luciano Righetti

a real-time Grafana dashboard using MISP ZeroMQ message queue and InfluxDB

https://github.com/MISP/misp-grafana

## _grafana

*"The open and composable observability and data visualization platform. Visualize metrics, logs, and traces from multiple sources like Prometheus, Loki, Elasticsearch, InfluxDB, Postgres and many more."*

source:
*https://github.com/grafana/grafana*

# _setup_1

1. git clone https://github.com/MISP/misp-grafana & cd docker/
2. docker-compose up -d
3. cd ../src/
4. pip install -r requirements.txt
5. python3 src/push_zmq_to_influxdb.py
6. configure ZeroMQ plugin in your MISP settings

```
[INFO] [2022-03-31 17:32:51,602] - Subscribed to ZMQ
[INFO] [2022-03-31 17:32:56,945] - Received message from topic: misp_json_self
[INFO] [2022-03-31 17:32:56,945] - ZMQ status pushed to InfluxDB
...
```

# _pushing_web_logs

A *Telegraf** agent is used to parse MISP logs and push them to InfluxDB

- http requests response times
- http status codes
- MISP error logs

* https://www.influxdata.com/time-series-platform/telegraf/

## Logins


## Latests Events

| Time | Title | Owner |
|---|---|---|
| 2022-03-30 16:50:16.3... | OSINT Potao Express samples from contagiodump | |
| 2022-03-30 16:33:15.4... | OSINT ShellShock scanning IPs from OpenDNS | CthulhuSPRL.be |
| 2022-03-30 15:57:05.8... | adasdas | HOST |

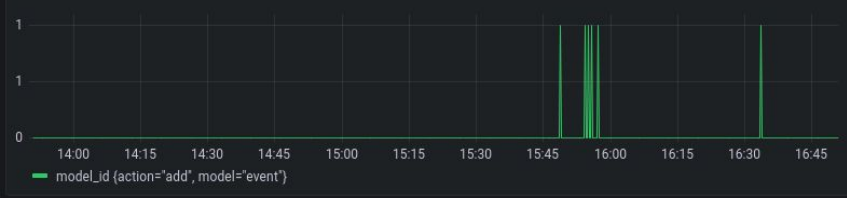
## Logins Today

7

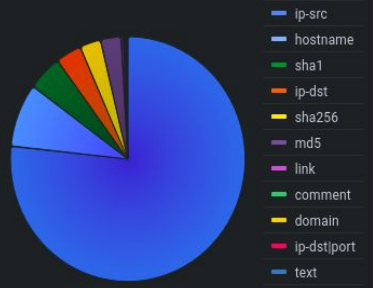
## New Events Today

8

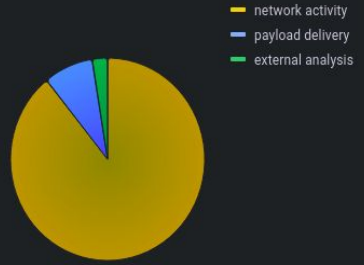
## Events




## Attribute Types




## Attribute Categories




## New Attributes Today

1 K

## Emails sent Today

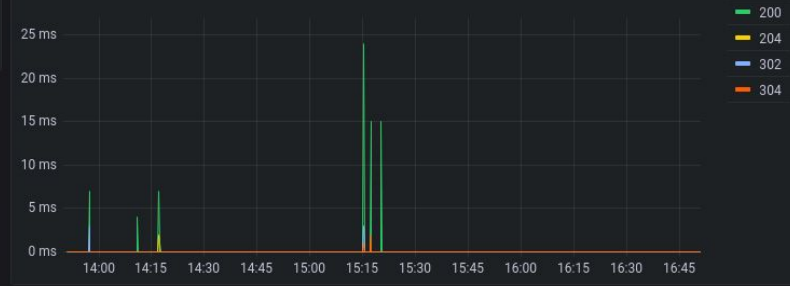
15

## New Object/Attributes


## Avg. Response Time

2.37 s

## HTTP requests




## Max. Response Time

1.57 min

## Error log

| | | |
|---|---|---|
| 2022-03-30 16:46:30 | Error | Could not add event '2017b845-f06b-48e4-b8a2-17d1fbd3dbb1' from feed 2. |
| 2022-03-30 16:46:23 | Error | Could not add event '54e1a7eb-4190-424f-bb4a-4d65950d210b' from feed 3. |
| 2022-03-30 16:50:51 | Warning | Could not add event '560994d3-73e8-4ae1-80e7-4c0c950d210b' from feed 3: 3 |
| 2022-03-30 16:50:50 | Warning | Could not add event '56095579-6aa0-403c-8ac3-409b950d210b' from feed 3: 3 |
| 2022-03-30 16:50:50 | Warning | Could not add event '56095160-7848-4ce6-b0d4-4d2b950d210b' from feed 3: 3 |
| 2022-03-30 16:50:49 | Warning | Could not add event '56056045-6158-4b49-8a23-cfaf950d210b' from feed 3: 3 |
| 2022-03-30 16:50:48 | Warning | Could not add event '560460c7-a840-4949-a92e-3c09950d210b' from feed 3: 3 |

## Errors Today

9