

MISP DASHBOARD

REAL-TIME OVERVIEW OF THREAT INTELLIGENCE FROM

CIRCL / TEAM MISPPROJECT

INFO@CIRCL.LU

SEPTEMBER 16, 2022



MISP
Threat Sharing

MISP ZEROMQ

MISP includes a flexible publish-subscribe model to allow real-time integration of the MISP activities:

- Event publication
- Attribute creation or removal
- Sighting
- User login

→ Operates at global level in MISP

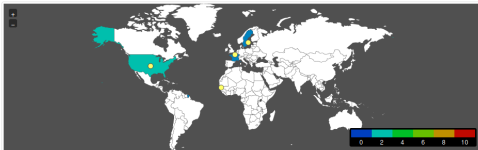
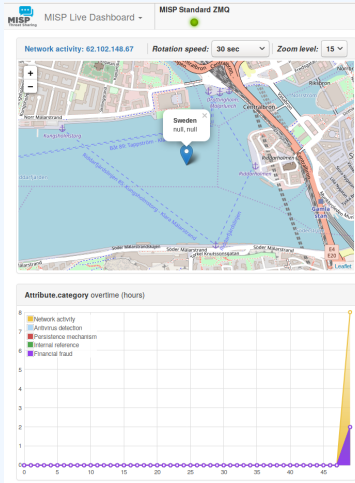
MISP ZeroMQ functionality can be used for various model of integration or to extend MISP functionalities:

- Real-time search of indicators into a SIEM¹
- Dashboard activities
- Logging mechanisms
- Continuous indexing
- Custom software or scripting

¹Security Information & Event Management

MISP-DASHBOARD: AN INTRODUCTION

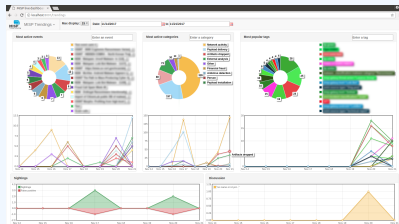
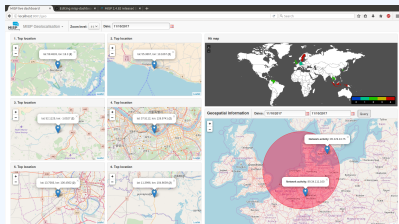
MISP-DASHBOARD - REALTIME ACTIVITIES AND THREAT INTELLIGENCE



Logs INFO WARNING CRITICAL

| Time | Event.id | Attribute.Tag | Attribute.category | Attribute.type | Attribute.value Attribute.comment |
|----------|----------|--|-----------------------|----------------|-------------------------------------|
| 15:07:46 | 9356 | ctrl:topic="undefined" ip:white | Network activity | ip-src | 99.99.99.99 |
| 15:08:36 | 9356 | ctrl:incident-classification="denial-of-service" | Network activity | ip-src | 8.8.8.8 |
| 15:08:36 | 9356 | ctrl:incident-classification="malware" ctrl:incident-classification="XSS" | Antivirus detection | comment | Comment |
| 15:08:36 | 9356 | | Network activity | ip-src | 9.9.9.9 |
| 15:08:36 | 9356 | | Persistence mechanism | text | Just a another text |
| 15:08:36 | 9356 | | Internal reference | text | Another text |
| 15:08:36 | 9356 | | Financial fraud | phone-number | +221721120220 |
| 15:08:36 | 9356 | | Network activity | ip-src | 62.102.148.67 |
| 15:08:36 | 9356 | ctrl:topic="undefined" ip:white | Network activity | ip-src | 99.99.99.99 |

MISP-DASHBOARD - FEATURES



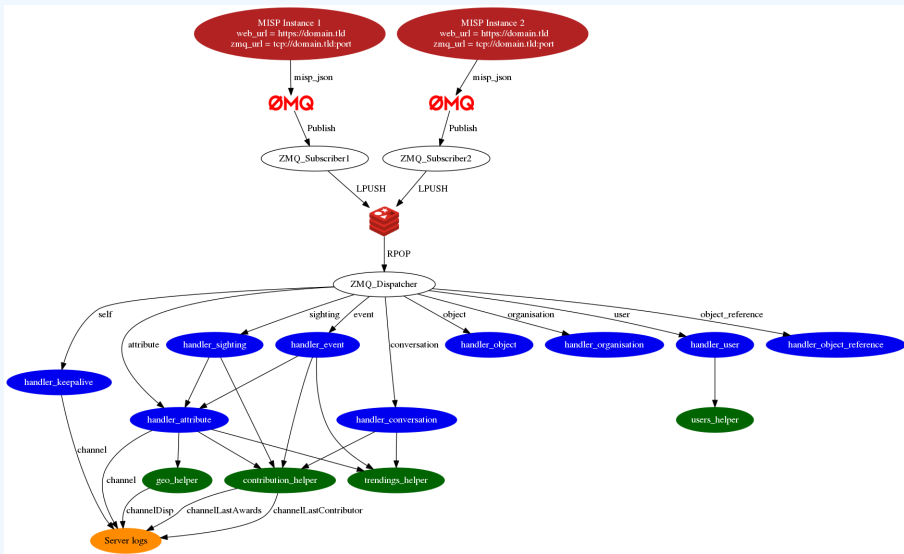
- Subscribe to multiple **ZMQ** MISP instances
- Provides historical geolocalised information
- Present an experimental **Gamification of the platform**
- Shows when and how MISP is used
- Provides real time information showing current threats and activity

MISP-DASHBOARD: ARCHITECTURE AND DEVELOPMENT

SETTING UP THE DASHBOARD

1. Be sure to have a running redis server: e.g.
 - ▶ `redis-server -p 6250`
2. Update your configuration in `config.cfg`
3. Activate your virtualenv:
 - ▶ `. ./DASHENV/bin/activate`
4. Listen to the MISP feed by starting the `zmq_subscriber`:
 - ▶ `./zmq_subscriber.py`
5. Start the dispatcher to process received messages:
 - ▶ `./zmq_dispatcher.py`
6. Start the Flask server:
 - ▶ `./server.py`
7. Access the interface at `http://localhost:8001/`

MISP-Dashboard architecture



WRITING YOUR HANDLER

```
1 # Register your handler
2 dico_action = {
3     "misp_json":             handler_dispatcher,
4     "misp_json_event":      handler_event,
5     "misp_json_self":       handler_keepalive,
6     "misp_json_attribute":  handler_attribute,
7     "misp_json_object":     handler_object,
8     "misp_json_sighting":   YOUR_CUSTOM_SIGHTINGS_HANDLER,
9     "misp_json_organisation": handler_log,
10    "misp_json_user":        handler_user,
11    "misp_json_conversation": handler_conversation,
12    "misp_json_object_reference": handler_log,
13 }
14
```

```
1 # Implement your handler
2
3 # e.g. user handler
4 def handler_user(zmq_name, jsondata):
5     # json action performed by the user
6     action = jsondata['action']
7     # user json data
8     json_user = jsondata['User']
9     # organisation json data
10    json_org = jsondata['Organisation']
11    # organisation name
12    org = json_org['name']
13    # only consider user login
14    if action == 'login':
15        timestamp = time.time()
16        # users_helper is a class to interact with the DB
17        users_helper.add_user_login(timestamp, org)
18
```

- MISP authentication can now be used in the misp-dashboard
- Improved TLS/SSL support in the default misp-dashboard
- Self-test tool to debug and test ZMQ connectivity



Optimizing contribution scoring and model to encourage sharing and contributions enrichment



Increasing geolocation coverage



Global filtering capabilities

- Geolocation: Showing wanted attribute or only on specific region
- Trendings: Showing only specified taxonomies



Tighter integration with MISP

- Present in MISP by default
- ACL enabled version

MISP-Dashboard can provides realtime information to support security teams, CSIRTs or SOC showing current threats and activity by providing:

- Historical geolocalised information
- Geospatial information from specific regions
- The most active events, categories, tags, attributes, ...

It also propose a prototype of gamification of the platform providing incentive to share and contribute to the community