MISP Dashboard

MISP DASHBOARD

9, 2024



MISP DASHBOARD

REAL-TIME OVERVIEW OF THREAT INTELLIGENCE FROM

CIRCL / TEAM MISP PROJECT

INFO@CIRCL.LU

JULY 8, 2024



MISP ZEROMQ

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

 \rightarrow Operates at global level in MISP

MISP Dashboard

MISP ZeroMQ

MISP ZeroMQ

MISP ZeroMQ

MISP ZeroMQ

A Description of the MISP zeroside to allow and discrete integration of the MISP zeroside.

A Description of the MISP zeroside or resonal

Solid Spling

Control of the MISP zeroside or resonal

Operates at global level in MISP

MISP ZEROMQ

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

MISP Dashboard

MISP ZeroMQ

MISP ZeroMQ

MISP ZeroMQ

MISP ZeroMQ

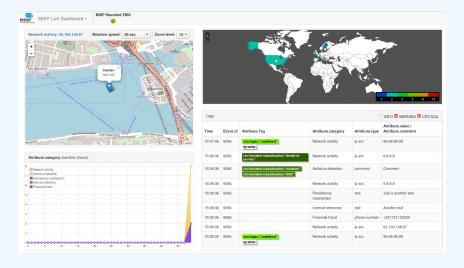
Cathorise south of the cathorise model of integration or to cented first fluctionalities.

Integration or to cented

¹Security Information & Event Management

MISP-DASHBOARD: AN INTRODUCTION

MISP-DASHBOARD - REALTIME ACTIVITIES AND THREAT INTELLIGENCE



MISP Dashboard
—MISP-Dashboard: An introduction

–MISP-Dashboard - Realtime activities and threat intelligence

POSSIBILIZATION ACTIVITIES AND THEIR

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

MISP-Dashboard: An introduction

└─MISP-Dashboard - Features

a Subscribe to multiple 200 WSF instances
Provides historia geolocalized information
Present an experimental Gamilication of the platform
Subsess when an MM MIP is used

1/2

-MISP-Dashboard: Architecture and development

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:
 - ► ./zmg dispatcher.py
- 6. Start the Flask server:
 - ► ./server.py
- 7. Access the interface at http://localhost:8001/

MISP Dashboard

MISP-Dashboard: Architecture and development

-Setting up the dashboard

1. Be som to have a running redis server e.g.

* redis*-server*-p 6556

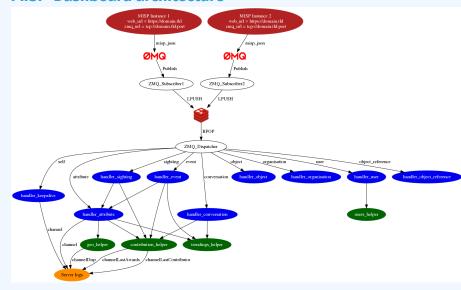
2. Update your configuration in config.cfg

3. Architecture (JASSER MARCHAELER)

* JASSER MARCHAELER

* Satt the fast server.

MISP-Dashboard architecture



14

MISP Dashboard

MISP-Dashboard: Architecture and development

MISP-Deabloard architecture

WRITING YOUR HANDLER

```
1 # Register your handler
2 dico_action = {
                                        handler_dispatcher,
          "misp_json":
          "misp_json_event":
                                        handler_event,
          "misp json self":
                                        handler keepalive,
          "misp json attribute":
                                        handler attribute,
          "misp json object":
                                        handler object,
          "misp json sighting":
                                        YOUR CUSTOM SIGHTINGS HANDLER,
          "misp json organisation":
                                        handler log,
          "misp json user":
                                        handler user,
          "misp json conversation":
                                        handler conversation,
          "misp json object reference": handler log,
```

MISP Dashboard

MISP-Dashboard: Architecture and development

Writing your handler

Magnitus records monitors

Magnitus para basilies

Mag

1/

```
1 # Implement your handler
3 # e.g. user handler
4 def handler user(zmg name, jsondata):
      # json action performed by the user
     action = jsondata['action']
      # user json data
      json user = jsondata['User']
      # organisation json data
      json org = jsondata['Organisation']
      # organisation name
      org = json_org['name']
      # only consider user login
     if action == 'login':
          timestamp = time.time()
          # users_helper is a class to interact with the DB
         users_helper.add_user_login(timestamp, org)
```

MISP Dashboard —MISP-Dashboard: Architecture and development

It implement poor bondars

2. 6. 6. south bunders

2. 6. south bunders

2. south bunders

3. south bunders

4. south bunders

4. south bunders

4. south bunders

5. south bun

RECENT CHANGES IN THE MISP-DASHBOARD

- 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

MISP Dashboard

MISP-Dashboard: Architecture and development

Recent changes in the misp-dashboard

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to to day upon to the first adult of the misp-dashboard **

**Siff section to day upon to the first adult of the misp-dashboard **

**Siff section to day upon to the first adult of the misp-dashboard **

**Siff section to day upon to the first adult of the misp-dashboard **

**Siff section to day upon to the first adult of the misp-dashboard **

**Siff section to day upon to the first adult of the misp-dashboard **

**Siff section to day upon to the first adult of the misp-dashboard **

**Siff section to day upon to the first adult of the misp-dashboard **

**Siff section to day upon to the first adult of the misp-dashboard **

**Siff section to day upon to the first adult of the misp-dashboard **

**Siff section to day upon to the first adult of the misp-dashboard **

**Siff section to day upon to the misp-dashboard **

**Siff section to day upon to the misp-dashboard **

**Siff section to day upon to the misp-dashboard **

**Siff section to day upon to the misp-dashboard **

**Siff section to day upon to the misp-

FUTURE DEVELOPMENT

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

—MISP-Dashboard: Architecture and development

—Future development

Optimizing contribution scoring and model to smorauge sharing and contributions enrichment increasing geolocation coverage clobal filtering capabilities - desocation Showing sustate attribute or only on specific growth of the contribution of the contribution of the property of the contribution of the contribution of the Tighter integration with MISCS - Features in 1979 by dargate.

CONCLUSION

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

MISP Dashboard

MISP-Dashboard: Architecture and development

Conclusion

LUSION

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

Historical geolocalised information

Geospatial information from specific regions

The most active events, categories, tags, attributes,
 The most active events, categories at the other state.

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