

Modern MISP

Filter My Organization My Events 0 selected select all Delete event Export							
ID	Description	Organizations	Tags	Clusters	Distribution	# Attr.	Dates
	This is a test	ghost_org ghost_org	misp-galaxy:disarm-techniques="Action/Attitude"	Techniques	☒ Your organization only	# 0	created 2025-05-13 modified 2025-05-14 published 2025-05-15
	International Workers Day Attacks	ghost_org ghost_org			☒ All communities	# 1	created 2025-05-01 modified 2025-05-13 published 2025-05-15

Modern MISP

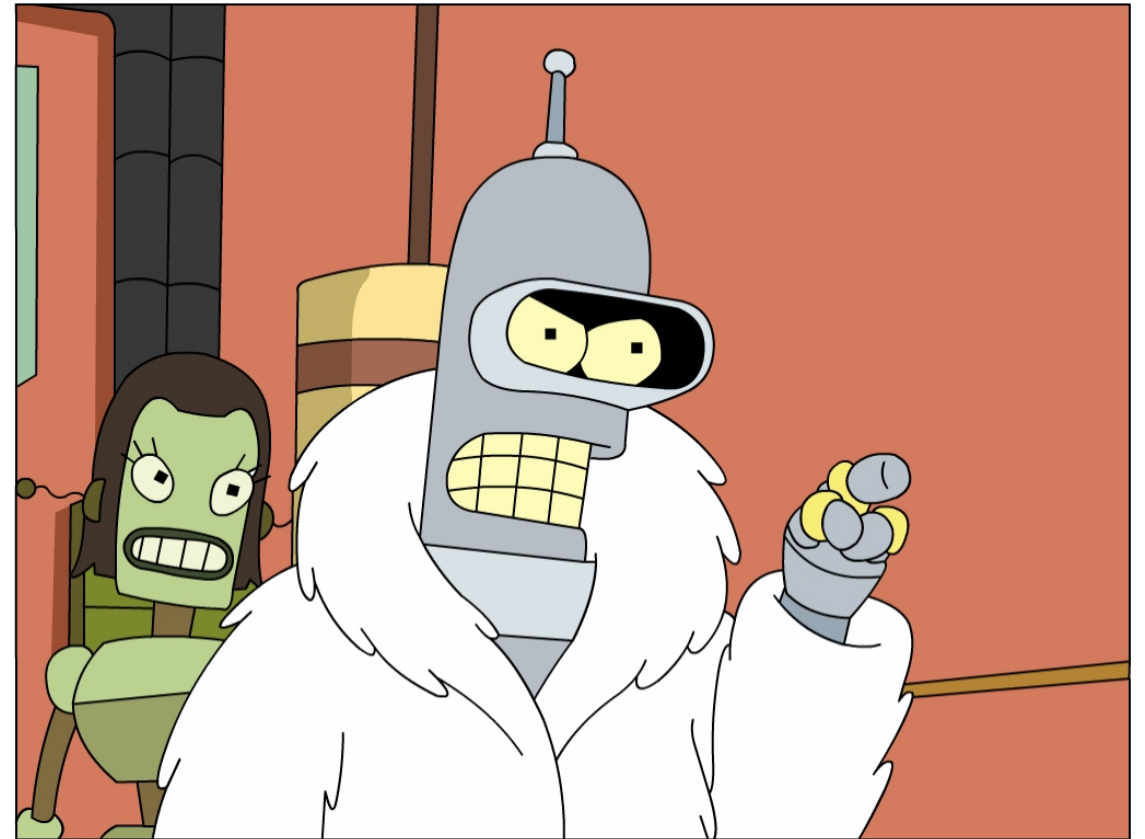
- a reimplementation of MISP
 - drop-in replacement
 - compatible API
 - using the same database schema
- API first approach
 - webfrontend using API, not server side generated

Why?

- We (KIT-CERT) wanted to use MISP, but ...
 - use a Postgres DB
 - had trouble installing
- Talked to people
 - operating seemed troublesome

*"I'm going to build my own MISP with
FastAPI and SQLAlchemy"*

How hard can it be?



KIT is a university

Computer Science Students have to complete a software development internship

- one semester long
- groups of five

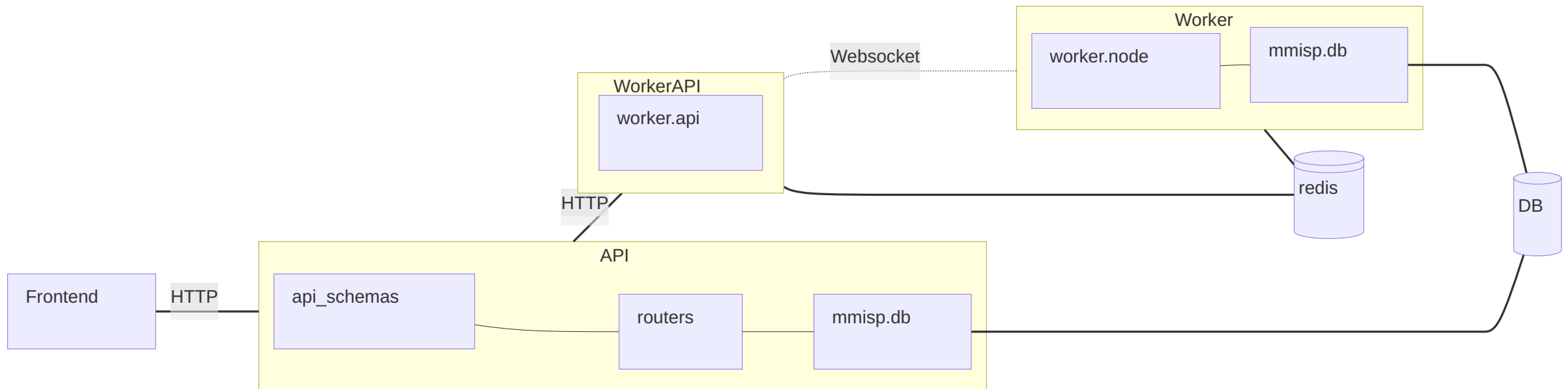
Initial thought (on May 2023):

"lets put two groups on it, one backend one frontend and we're done"

Student projects

- First term: 3 groups each 5 persons
 - Frontend
 - API
 - Worker
- Second term: 2 groups
 - Commandline client, Frontend, Login, ...
 - MISP Workflows
- Third term: 2 groups
 - Import Galaxies, Taxonomies, Object Templates
 - Access System: Permissions

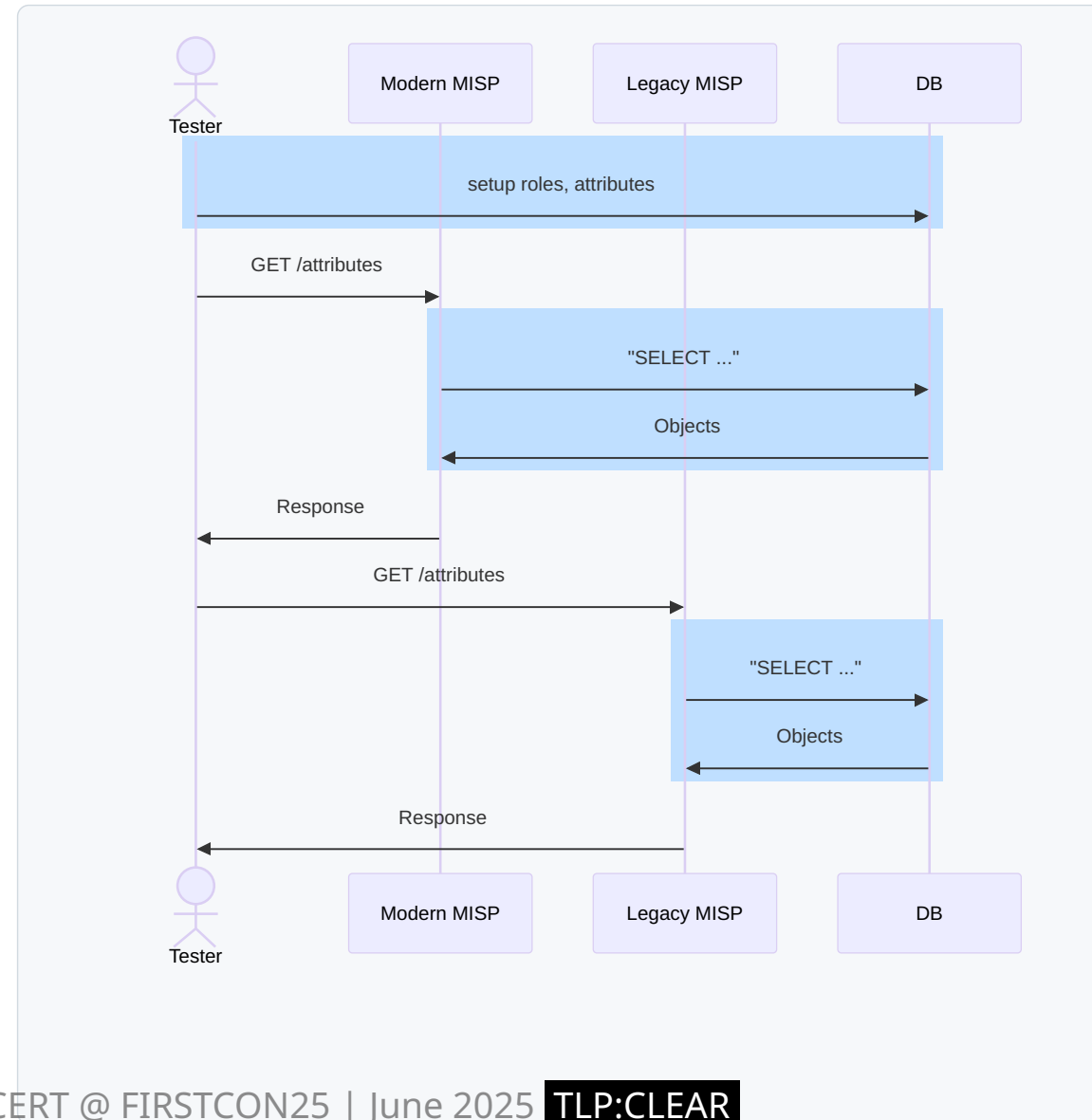
Modern MISP Architecture



Architecture

- scalable
 - using multiple worker nodes
 - load balancers for api
- distributable
- small setups also possible:
 - e.g. no worker, for workshops

Compatibility Tests



■ Blackbox Testing

■ Ensuring same response

■ Paths:

- `/events`
- `/events/view/{event.id}`
- `/attributes`
- `/attributes/{attribute_id}`
- `/attributes/describeTypes`
- `/sharing_groups/view/{sg_id}`
- `/sharing_groups/index`
- `/galaxy_clusters/view/{gc_id}`
- `/galaxy_clusters/add/{g_id}`
- `/roles`

Testing

- "Ensuring same response"
- Calculate Diff
 - Convert Integers into Strings
 - Ignore `None` vs. not-present
- Tests for access control:
 - create roles, organisations, sharing_groups, user, events, attributes
 - combinatorial explosion

CLI Client for initialisation

```
# create organisation, setup roles
mmisp-db setup
# create a new user in org 1
mmisp-db create-user admin@demo-01.modern-misp.dev somepassword 1 --role site_admin
```

Installation

Use `pipx install mmisp-api[granian]`

```
[Unit]
Description=Modern MISP API
After=network.target

[Service]
ExecStart=/home/mmisp/.local/pipx/venvs/mmisp-api/bin/mmisp-api
User=mmisp
Restart=on-failure
Type=simple

Environment='RUNNER=granian'
Environment='DATABASE_URL=mysql+aiomysql://demo01:*****@demo-db.modern-misp.dev:3306/demo01'
Environment='WORKER_COUNT=2'
Environment='PORT=4000'
Environment='WORKER_URL=https://worker.demo-01.modern-misp.dev'
Environment='WORKER_KEY=*****'
Environment='HASH_SECRET=*****'

[Install]
WantedBy=multi-user.target
```

Reverse proxy (e.g. caddy):

```
demo-01.modern-misp.dev {  
    try_files {path} /index.html  
    root * /var/www/misp  
    file_server  
}  
  
api.demo-01.modern-misp.dev {  
    reverse_proxy 127.0.0.1:4000  
}  
  
worker.demo-01.modern-misp.dev {  
    reverse_proxy 127.0.0.1:5000  
}
```

Use Worker to init database

- with galaxies
- with object templates
- with taxonomies

Live demo

- create event
- create attribute
- add galaxy cluster to event
- Push Job
- Freetext-Import

[skip to roadmap](#)

View Mode

Events

Filter

My Organization

My Events

ID

Description

Organizations

Tags

Clusters

Distribution

Attr.

Dates

This is a test

ghost_org

ghost_org

misp-galaxy:disarm-techniques="Action/Attitude"

Techniques

Connected communities

2

created 2025-05-13

modified 2025-05-28

published 2025-06-18

International Workers Day Attacks

ghost_org

ghost_org

All communities

1

created 2025-05-01

modified 2025-05-13

published 2025-06-18

View mode

Edit Mode

Events

+

Add Event

●

Edit mode

Filter

My Organization

My Events

0 selected

select all

Delete event

Export

ID	Description	Organizations	Tags	Clusters	Distribution	# Attr.	Dates
	This is a test	ghost_org ghost_org	misp-galaxy:disarm-techniques="Action/Attitude"	Techniques	Connected communities	# 2	created 2025-05-13 modified 2025-05-28 published 2025-06-18
	International Workers Day Attacks	ghost_org ghost_org			All communities	# 1	created 2025-05-01 modified 2025-05-13 published 2025-06-18

Add Event

Events

Cancel

Save

Edit mode

Date

06 / 17 / 2025

Distribution

Connected communities

Threat Level

undefined

Analysis

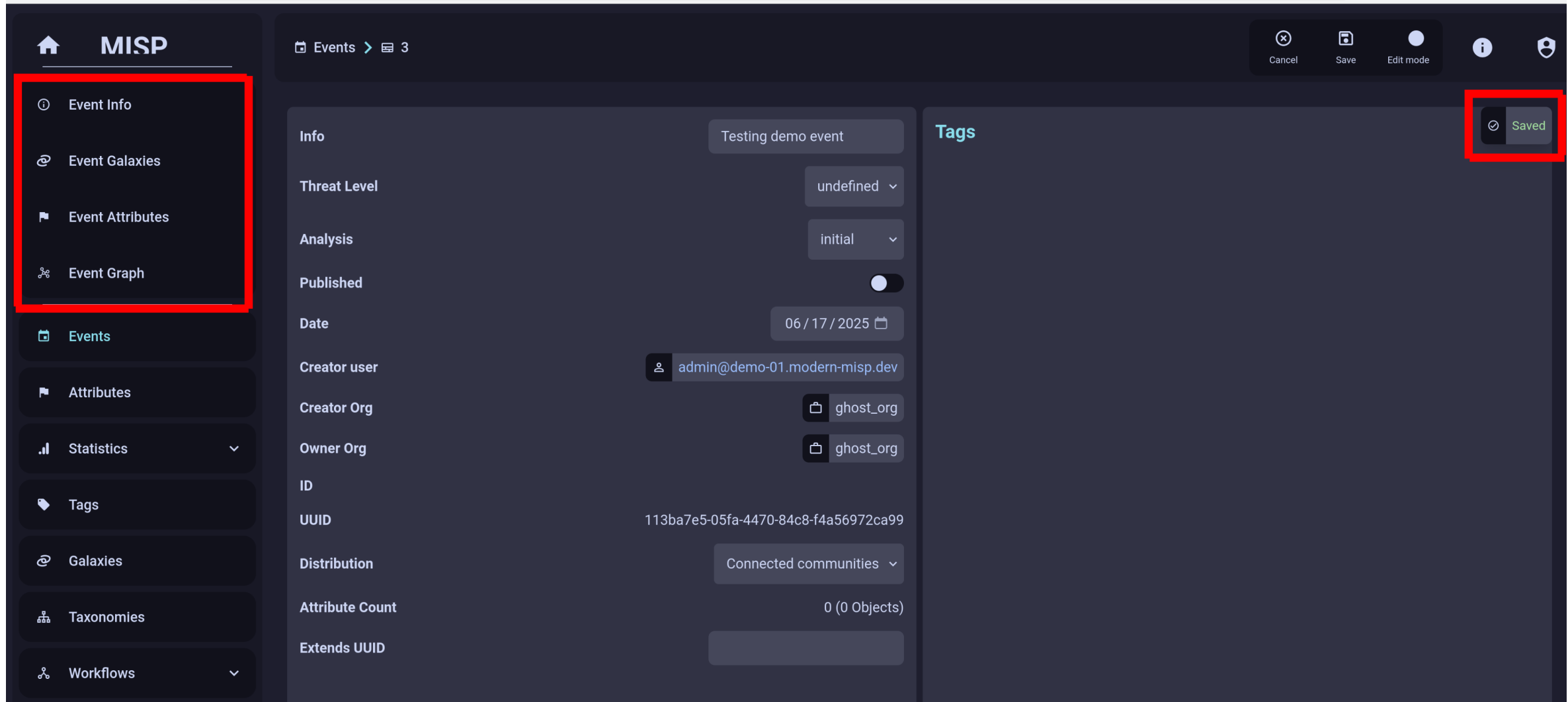
initial

Event info

Testing demo event

Extends UUID

Event Overview



MISP

Events > 3

Cancel Save Edit mode

Event Info

Event Galaxies

Event Attributes

Event Graph

Events

Attributes

Statistics

Tags

Galaxies

Taxonomies

Workflows

Info

Testing demo event

Threat Level undefined

Analysis initial

Published ☐

Date 06 / 17 / 2025

Creator user admin@demo-01.modern-misp.dev

Creator Org ghost_org

Owner Org ghost_org

ID

UUID 113ba7e5-05fa-4470-84c8-f4a56972ca99

Distribution Connected communities

Attribute Count 0 (0 Objects)

Extends UUID

Tags

Saved

Add Attribute Failure

Events > 3 > Event Attributes > New Attribute

Cancel Save Edit mode ⓘ

Value

Comment

Distribution

Category

Type

Correlate

TypeError: can't convert undefined to object

Your organization only

Payload delivery

ip-src

Add Attribute Success

Attributes > 6

Add Sighting Delete Attribute Cancel Save Edit mode

ID

Event  3

Category Payload delivery

Type ip-src

Value 127.0.0.3

Tags

 Saved

Add Galaxy Cluster to Event

Events > 3 > Event Galaxies

Cancel Save Edit mode

Add Galaxy Cluster

Local only ☐

Relationship abuses

Galaxy Actor Types

soc

social media platform adminstrator social media platform outreach social media platform owner

Galaxies

Those elements will be added:

Add Galaxy Cluster to Event 2

Add Galaxy Cluster

Local only ☐

Relationship abuses

Galaxy Actor Types

social media platform administrator

Cluster

Galaxies

Those elements will be added:

abuses social media platform administrator

Add Galaxy Cluster to Event 3

Add Galaxy Cluster

Local only ☐

Relationship abuses

Galaxy Actor Types

social media platform administrator

Cluster

Galaxies

Actor Types

social media platform administrator

Changed 1 elements.

Those elements will be added:

Add Galaxy Cluster to Event 4

Info

Testing demo event

Threat Level

undefined ▾

Analysis

initial ▾

Published

☐

Date

06 / 17 / 2025 📅

Creator user

👤 admin@demo-01.modern-misp.dev

Creator Org

🏢 ghost_org

Owner Org

🏢 ghost_org

ID

UUID

113ba7e5-05fa-4470-84c8-f4a56972ca99

Distribution

Connected communities ▾

Attribute Count

1 (0 Objects)

Extends UUID

Tags

🔖 misp-galaxy:disarm-actortypes="social media platform adminstrator" 🗑

Push Job

sync

POST

/job/pull

Create Pull Job

🔒

⌵

POST

/job/push

Create Push Job

🔒

⌵

Parameters

Cancel

Reset

No parameters

Request body

required

application/json

⌵

Edit Value

Schema

```
{  "user": {    "user_id": 0  },  "data": {    "server_id": 1,    "technique": "full"  }}
```

Push Job Result

https://demo-02.modern-misp.dev/events

Events

Filter My Organization My Events

ID	Description	Organizations	Tags	Clusters	Distribution	# Attr.	Dates
	This is a test	ghost_org			☒ This community only	# 2	created 2025-05-13 modified 2025-06-18 published 2025-06-18
	Testing demo event	ghost_org			☒ This community only	# 1	created 2025-06-17 modified 2025-06-18 published 2025-06-18

Freetext Import

📅 Events > 📋 3 > 🏷️ Event Attributes

0 selected ☐ select all  Delete Attribute

Freetext Import

Do you know about kit.edu

Freertext Import 2

Events > 3 > Event Attributes

0 selected ☒ select all

 Delete Attribute

Freertext Import

These attributes have been added:

0 selected ☒ select all

 Save

Value	Type
kit.edu	domain

KIT-CERT @ FIRSTCON25 | June 2025 TLP:CLEAR

30

Roadmap

- DB: Complete Schema → Alembic
 - Manage Migrations
- ~~Pull/Push Jobs~~
- Restsearch
 - Sightings
- Scheduler for Jobs

Demo Instance

<https://demo-01.modern-misp.dev/>

User: admin@demo-01.modern-misp.dev

PW: firstdemo2025

<https://demo-02.modern-misp.dev/>

User: admin@demo-02.modern-misp.dev

PW: firstdemo2025

api.demo-01.modern-misp.dev/docs

worker.demo-01.modern-misp.dev/docs

... valid at least for this week

github.com/Modern-Misp

modern-misp.dev

Thanks for your attention!