

# MISP USER TRAINING - GENERAL USAGE OF MISP

## MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: [@MISPPROJECT](https://twitter.com/MISPPROJECT)

CIRCL - UNI.LU



**MISP**  
Threat Sharing

## ■ Credentials

- ▶ MISP admin: admin@admin.test/admin
- ▶ SSH: misp/Password1234

## ■ Available at the following location (VirtualBox and VMWare):

- ▶ <https://www.circl.lu/misp-images/latest/>

## ■ It is a bit broken.

- ▶ `sudo -s`
- ▶ `cd /var/www/MISP/`
- ▶ `sudo pear install`  
`INSTALL/dependencies/Console_CommandLine/package.xml`
- ▶ `sudo pear install`  
`INSTALL/dependencies/Crypt_GPG/package.xml`
- ▶ `cd /usr/local/src/misp-modules`
- ▶ `pip3 install -r REQUIREMENTS`
- ▶ `pip3 install .`
- ▶ `reboot`

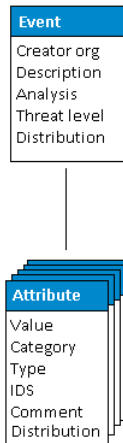
## Plan for this part of the training

- Data model
- Viewing data
- Creating data
- Co-operation
- Distribution
- Exports

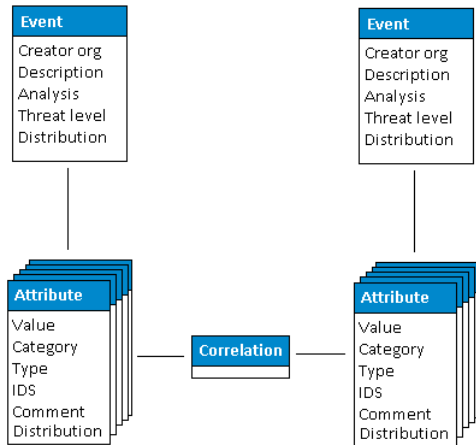
# MISP - EVENT (MISP's BASIC BUILDING BLOCK)

Event
Creator org
Description
Analysis
Threat level
Distribution

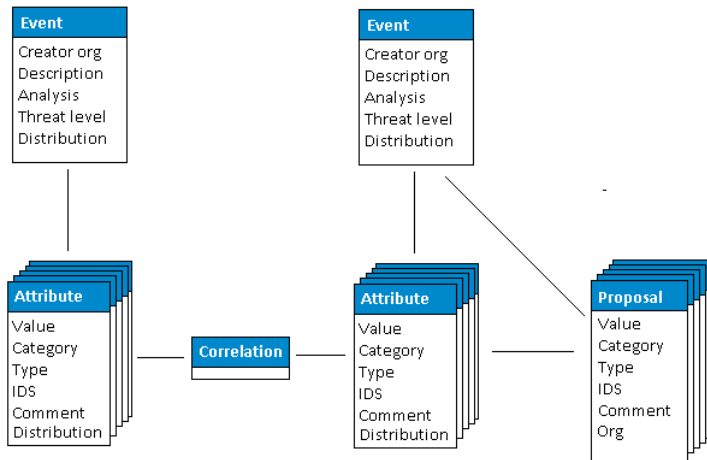
# MISP - EVENT (ATTRIBUTES, GIVING MEANING TO EVENTS)



# MISP - EVENT (CORRELATIONS ON SIMILAR ATTRIBUTES)

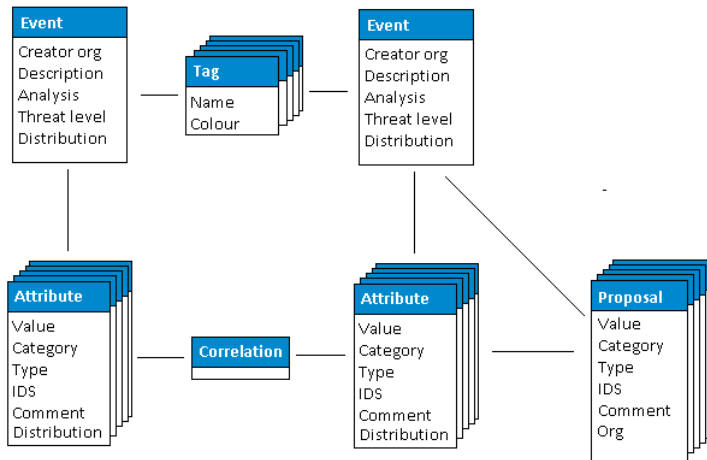


# MISP - EVENT (PROPOSALS)

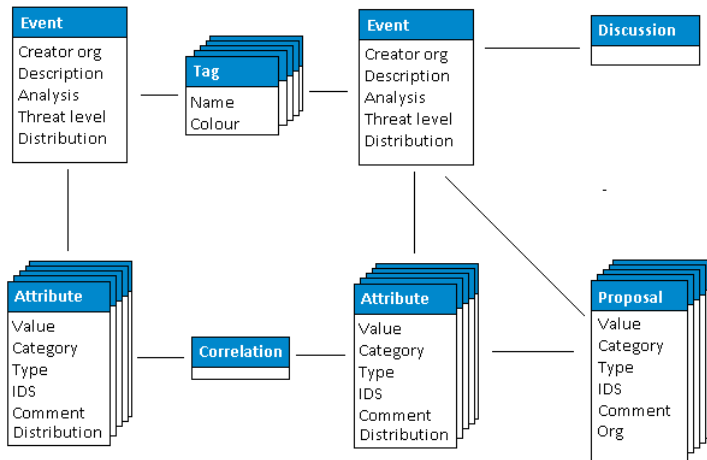




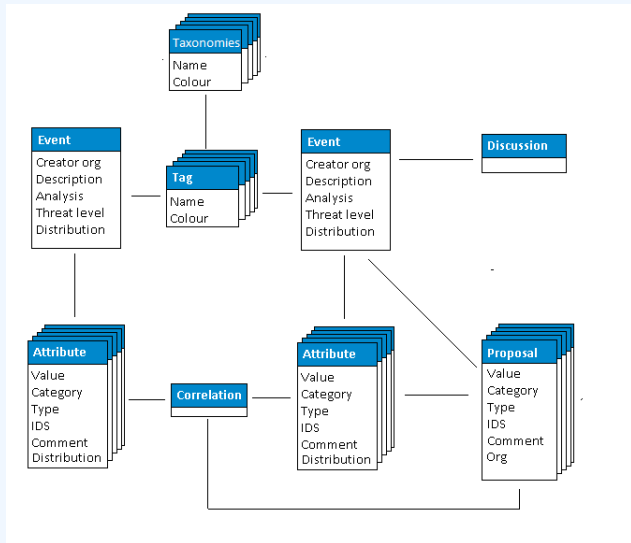
# MISP - EVENT (TAGS)



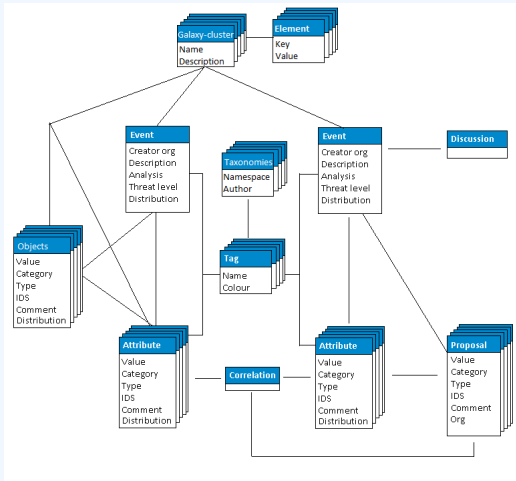
# MISP - EVENT (DISCUSSIONS)



# MISP - EVENT (TAXONOMIES AND PROPOSAL CORRELATIONS)



# MISP - EVENT (THE STATE OF THE ART MISP DATAMODEL)



## ■ Event Index

- ▶ Event context
- ▶ Tags
- ▶ Distribution
- ▶ Correlations

## ■ Filters

## ■ Event View

- ▶ Event context
- ▶ Attributes
  - Category/type, IDS, Correlations
- ▶ Objects
- ▶ Galaxies
- ▶ Proposals
- ▶ Discussions

## ■ Tools to find what you are looking for

## ■ Correlation graphs

# MISP - CREATING AND POPULATING EVENTS IN VARIOUS WAYS (DEMO)

- The main tools to populate an event
  - ▶ Adding attributes / batch add
  - ▶ Adding objects and how the object templates work
  - ▶ Freetext import
  - ▶ Import
  - ▶ Templates
  - ▶ Adding attachments / screenshots
  - ▶ API

- What happens automatically when adding data?
  - ▶ Automatic correlation
  - ▶ Input modification via validation and filters (regex)
  - ▶ Tagging / Galaxy Clusters
- Various ways to publish data
  - ▶ Publish with/without e-mail
  - ▶ Publishing via the API
  - ▶ Delegation



- Correlation graphs
- Downloading the data in various formats
- API (explained later)
- Collaborating with users (proposals, discussions, emails)

# MISP - SYNC EXPLAINED (IF NO ADMIN TRAINING)

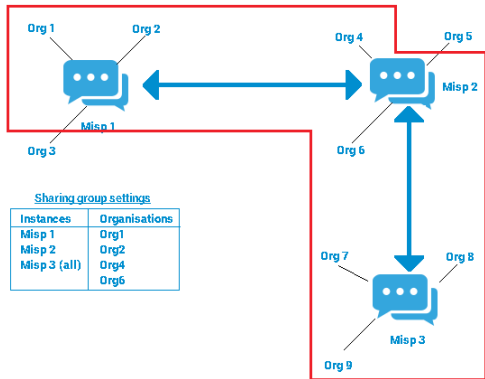
- Sync connections
- Pull/push model
- Previewing instances
- Filtering the sync
- Connection test tool
- Cherry pick mode

# MISP - FEEDS EXPLAINED (IF NO ADMIN TRAINING)

- Feed types (MISP, Freetext, CSV)
- Adding/editing feeds
- Previewing feeds
- Local vs Network feeds

- Your Organisation Only
- This Community Only
- Connected Communities
- All Communities
- Sharing Group

# MISP - DISTRIBUTION AND TOPOLOGY



- Download an event
- Quick glance at the APIs
- Download search results
- ReST API and query builder

# MISP - SHORTHAND ADMIN (IF NO ADMIN TRAINING)

- Settings
- Troubleshooting
- Workers
- Logs