

# 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

MISP PROJECT



2024-04-15

MISP User Training - General usage of MISp

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

MISP PROJECT



## ■ 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/>

### └─ MISP - VM

- 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

## └─ MISP - VM

- 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 - General Usage

Plan for this part of the training

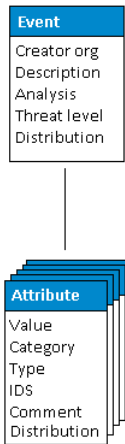
- Data model
- Viewing data
- Creating data
- Co-operation
- Distribution
- Exports

Event
Creator org
Description
Analysis
Threat level
Distribution

└─ MISP - Event (MISP's basic building block)



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



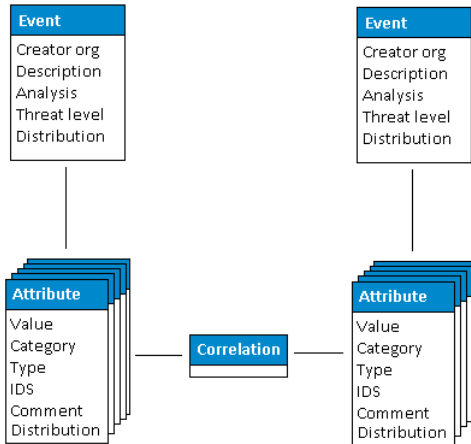
2024-04-15

## MISP User Training - General usage of MISP

↳ MISP - Event (Attributes, giving meaning to events)



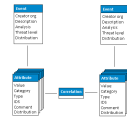
# MISP - EVENT (CORRELATIONS ON SIMILAR ATTRIBUTES)



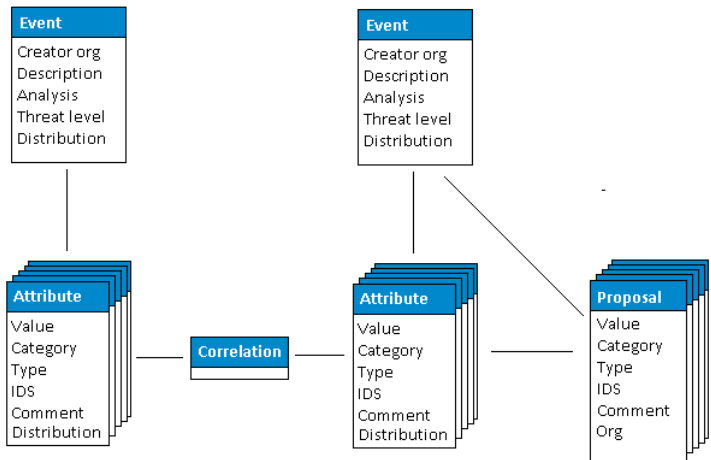
2024-04-15

## MISP User Training - General usage of MISP

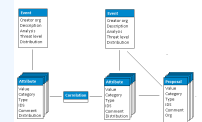
↳ MISP - Event (Correlations on similar attributes)



# MISP - EVENT (PROPOSALS)

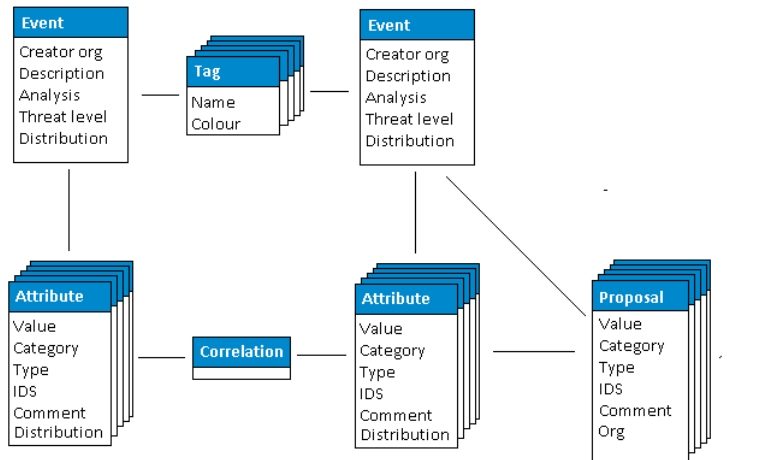


### MISP - Event (Proposals)





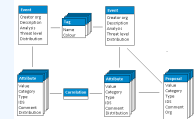
# MISP - EVENT (TAGS)



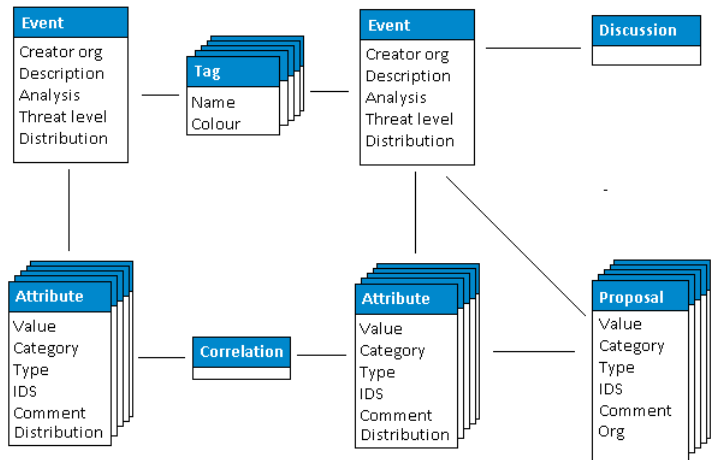
2024-04-15

## MISP User Training - General usage of MISP

### MISP - Event (Tags)



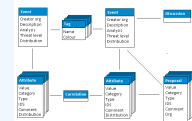
# MISP - EVENT (DISCUSSIONS)



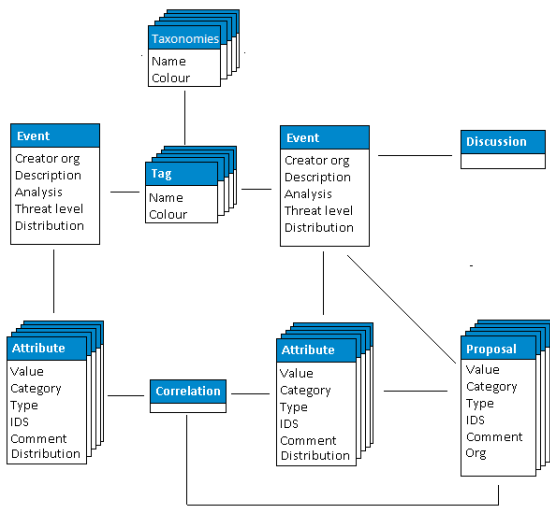
2024-04-15

## MISP User Training - General usage of MISP

### MISP - Event (Discussions)



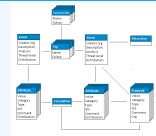
# MISP - EVENT (TAXONOMIES AND PROPOSAL CORRELATIONS)



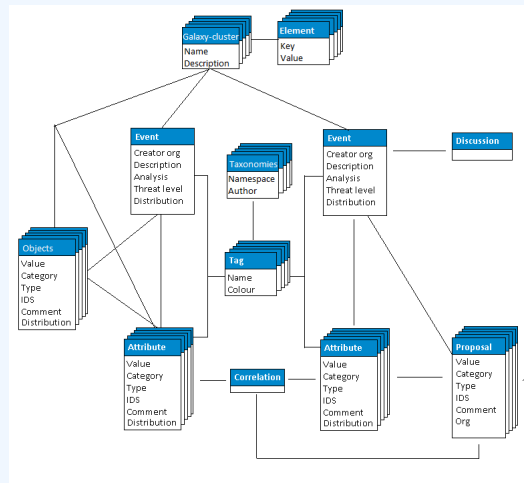
2024-04-15

## MISP User Training - General usage of MISP

↳ MISP - Event (Taxonomies and proposal correlations)



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



## MISP User Training - General usage of MISP

↳ MISP - Event (The state of the art MISP datamodel)



2024-04-15

## ■ Event Index

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

## ■ Filters

### └─ MISP - Viewing the Event Index

- 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 - Viewing an Event

- 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

2024-04-15

## MISP User Training - General usage of MISP

### └─ 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

### └─ MISP - Various features while adding data

- 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 - Using the data

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

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

2024-04-15

└─ MISP - Sync explained (if no admin training)

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

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

### └─ MISP - Feeds explained (if no admin training)

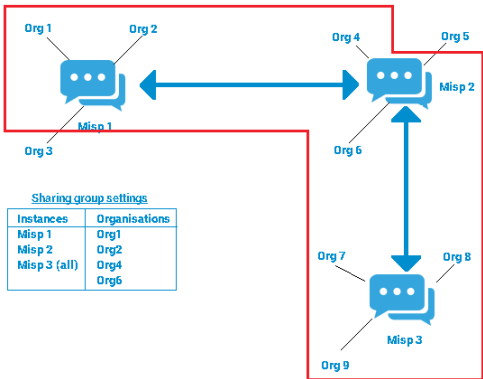
- Feed types (MISP, Freetext, CSV)
- Adding/editing feeds
- Previewing feeds
- Local vs Network feeds

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

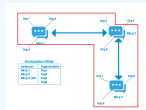
2024-04-15

### └─ MISP - Distributions explained

- 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 - Exports and API

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

- Settings
- Troubleshooting
- Workers
- Logs

2024-04-15

## MISP User Training - General usage of MISP

└─ MISP - Shorthand admin (if no admin training)

- Settings
- Troubleshooting
- Workers
- Logs