MISP User Training - General usage of MISP

MISP - Threat Sharing

CIRCL / Team MISP Project

http://www.misp-project.org/
Twitter: @MISPProject

MISP Project

MISP User Training - General usage of MISP
MISP - Threat Sharing
CIRCL / Team MISP Project
http://www.misp-project.org/
Twitter: @MISPProject
MISP Project
MISP
Threat Sharing

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/

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/

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

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

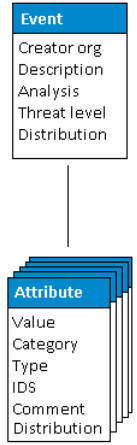
- Data model
- Viewing data
- Creating data
- Co-operation
- Distribution
- Exports

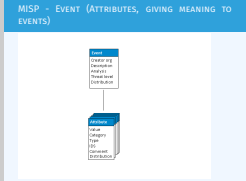
MISP - General Usage
Plan for this part of the training
Data model
Viewing data
Creating data
Co-operation
Distribution
Exports

MISP - Event (MISP's basic building block)

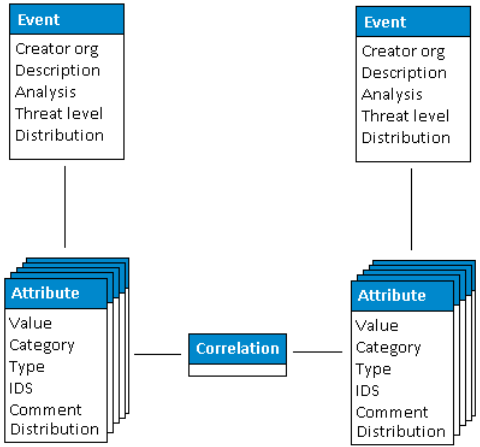
MISP - Event (MISP's basic building block)

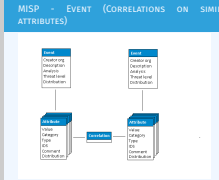
MISP - Event (Attributes, giving meaning to events)



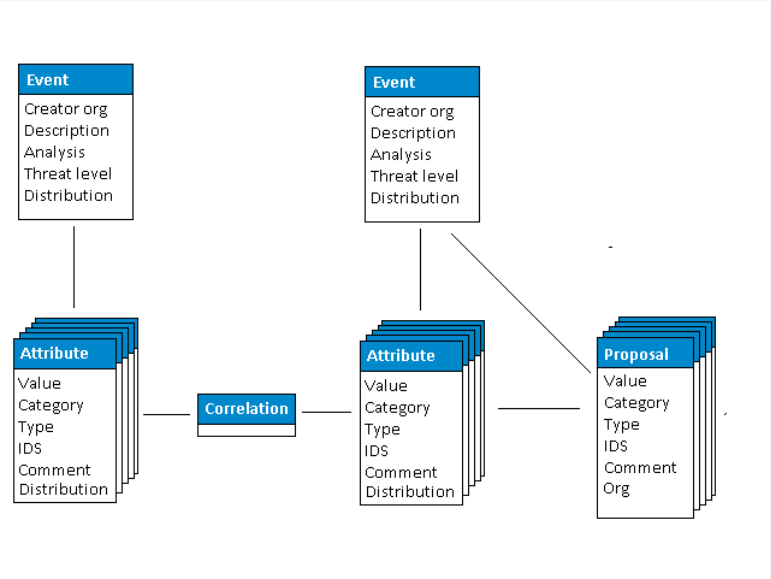


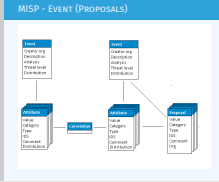
MISP - Event (Correlations on similar attributes)



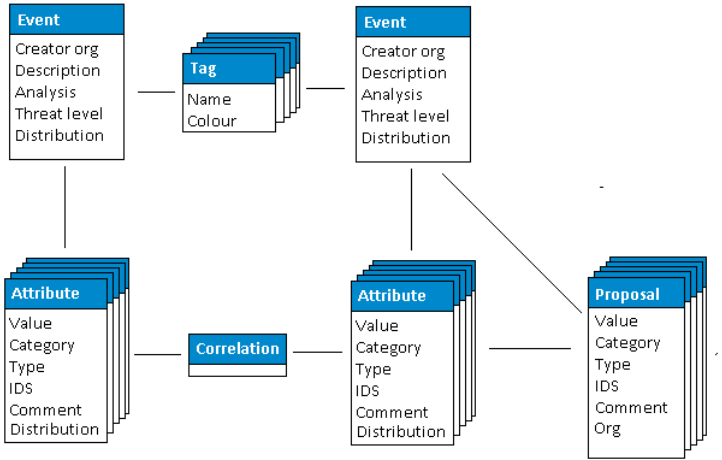


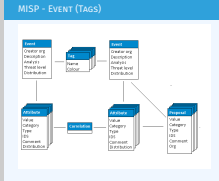
MISP - Event (Proposals)



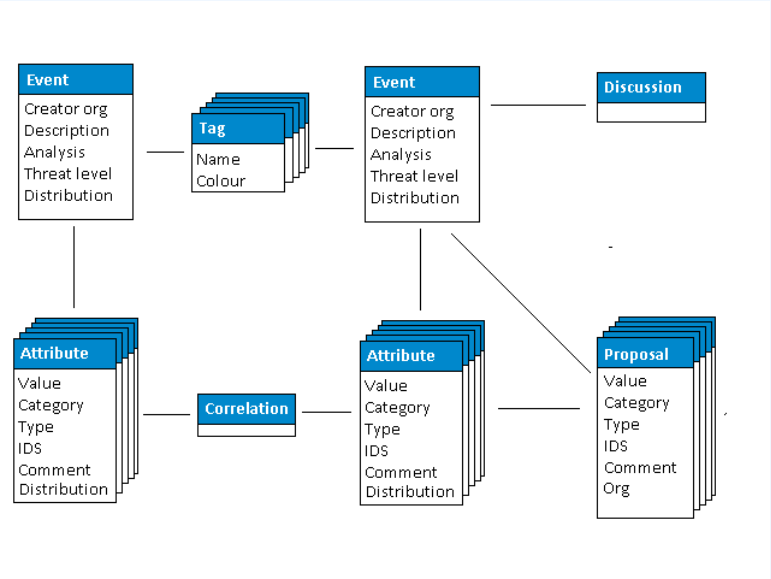


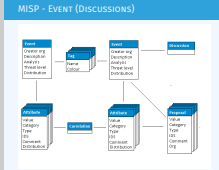
MISP - Event (Tags)



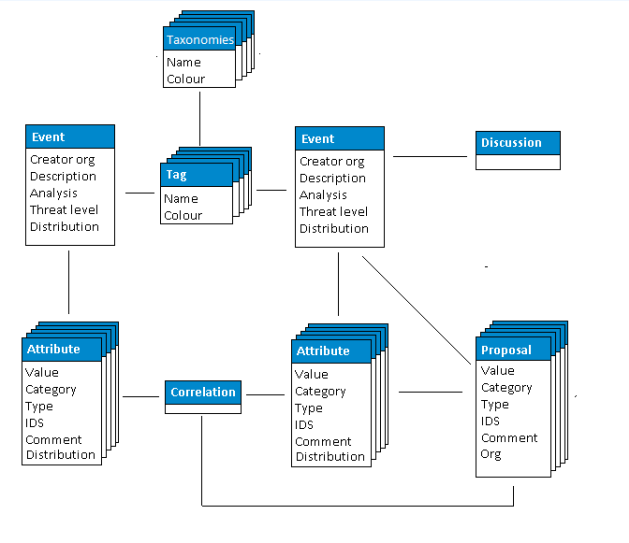


MISP - Event (Discussions)

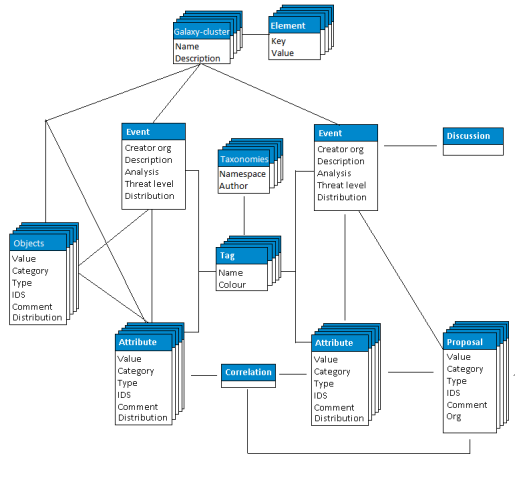




MISP - Event (Taxonomies and proposal correlations)



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



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

MISP - Viewing the Event Index

- Event Index
  - Event context
  - Tags
  - Distribution
  - Correlations
- Filters

MISP - Viewing the Event Index
Event Index
Event context
Tags
Distribution
Correlations
Filters

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 - 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

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

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

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

MISP - Using the data

- 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)

MISP - Sync explained (if no admin training)

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

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

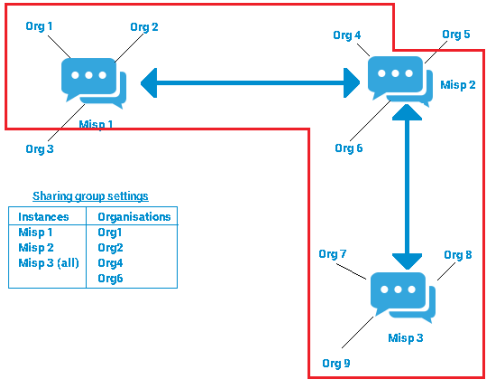
MISP - Feeds explained (if no admin training)
Feed types (MISP, Freetext, CSV)
Adding/editing feeds
Previewing feeds
Local vs Network feeds

MISP - Distributions explained

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

MISP - Distributions explained
Your Organisation Only
This Community Only
Connected Communities
All Communities
Sharing Group

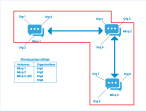
MISP - Distribution and Topology



Sharing group settings

Instances	Organisations
Misp 1	Org1
Misp 2	Org2
Misp 3 (all)	Org4
	Org6

MISP - Distribution and Topology



MISP - Exports and API

- 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

MISP - Shorthand admin (if no admin training)

- Settings
- Troubleshooting
- Workers
- Logs

MISP - Shorthand admin (if no admin training)
Settings
Troubleshooting
Workers
Logs