MISP User Training - General usage of MISP

MISP - Malware Information Sharing Platform & Threat Sharing

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy
Andras Iklody
Raphaël Vinot

TLP:WHITE

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

MISP Training @ Luxembourg
20180116

MISP - VM

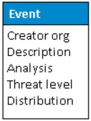
- Credentials
  - MISP admin: admin@admin.test/admin
  - SSH: misp/Password1234
- Available at the following location (VirtualBox and VMWare):
  - `https://www.circl.lu/misp-images/latest/`

MISP - General Usage

Plan for this part of the training

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

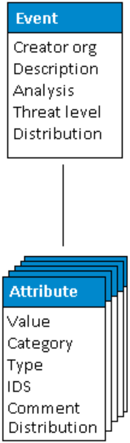
MISP - Event (MISP's basic building block)



Event

Creator org
Description
Analysis
Threat level
Distribution

MISP - Event (Attributes, giving meaning to events)



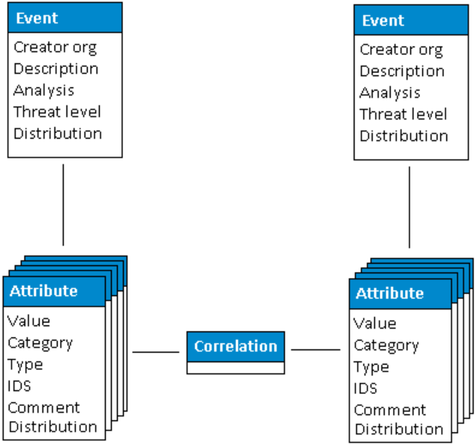
Event

Creator org
Description
Analysis
Threat level
Distribution

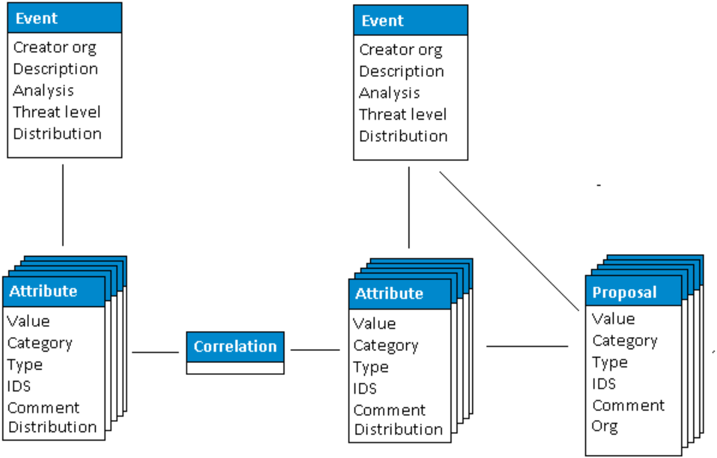
Attribute

Value
Category
Type
IDS
Comment
Distribution

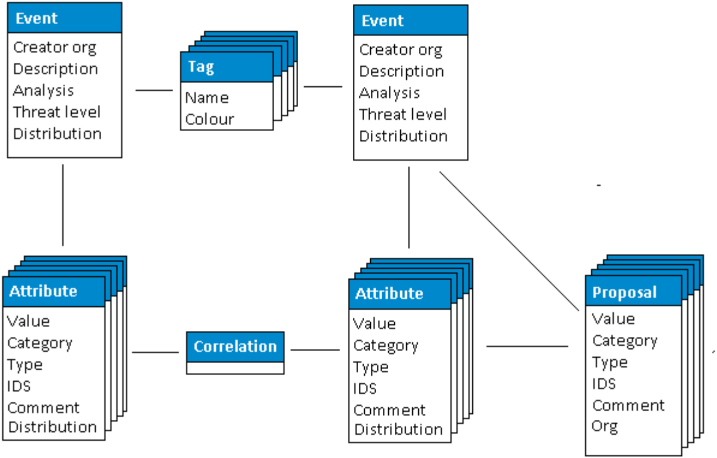
MISP - Event (Correlations on similar attributes)



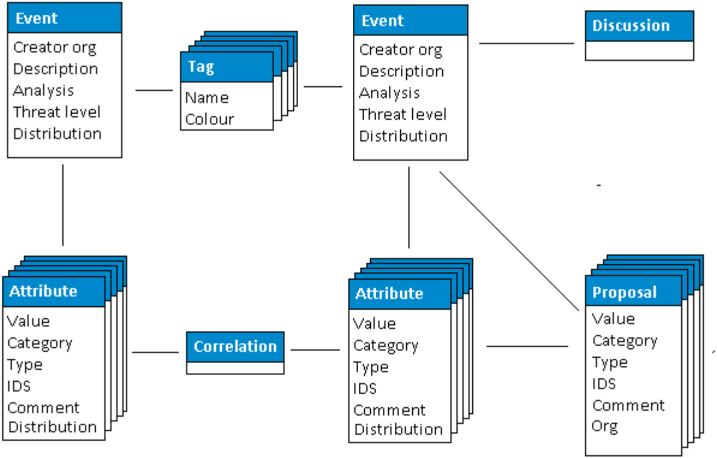
MISP - Event (Proposals)



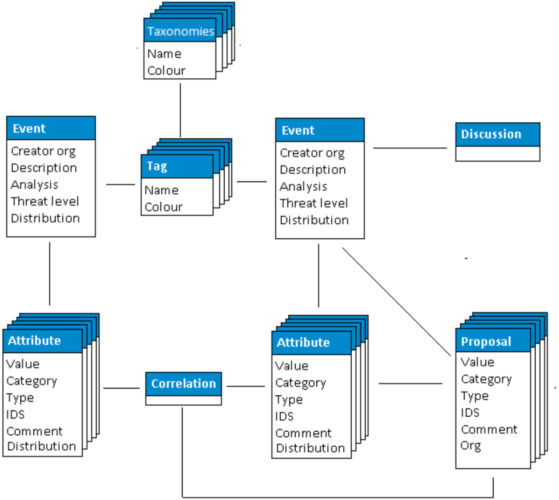
MISP - Event (Tags)



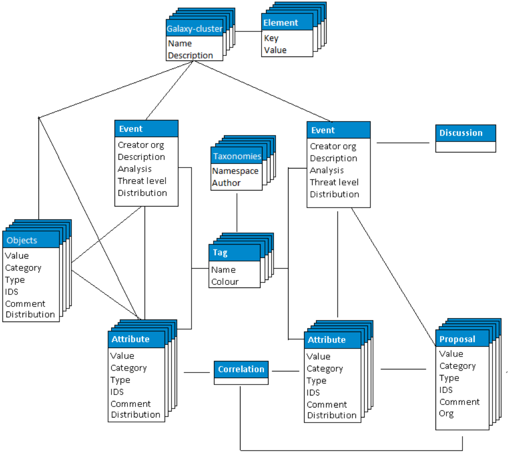
MISP - Event (Discussions)



MISP - Event (Taxonomies and proposal correlations)



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



MISP - 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 - 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 - Using the data

- Correlation graphs
- Downloading the data in various formats
- Cached exports
- 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

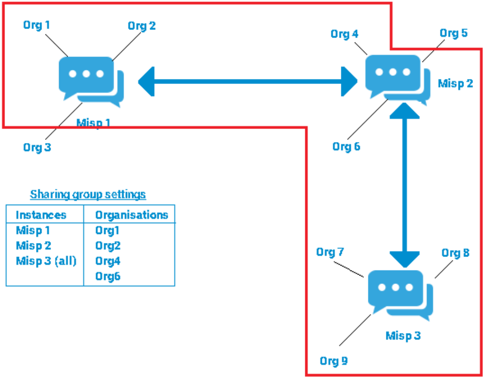
MISP - Feeds explained (if no admin training)

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

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 - Exports and API

- Download an event
- Quick glance at the APIs
- Download search results
- Cached exports

MISP - Shorthand admin (if no admin training)

- Settings
- Troubleshooting
- Workers
- Logs