

MISP User Training - General usage of MISP 2.4

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
20170207

MISP - VM

- Credentials
 - MISP admin: admin@misp.training/Password1234
 - MISP user: user@misp.training/Password1234
 - SSH: misp/Password1234
 - Mysql: root/Password1234 - misp/Password1234
- 2 network interfaces
 - NAT
 - Host only adapter

MISP - General Usage

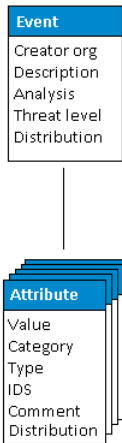
Plan for this part of the training

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

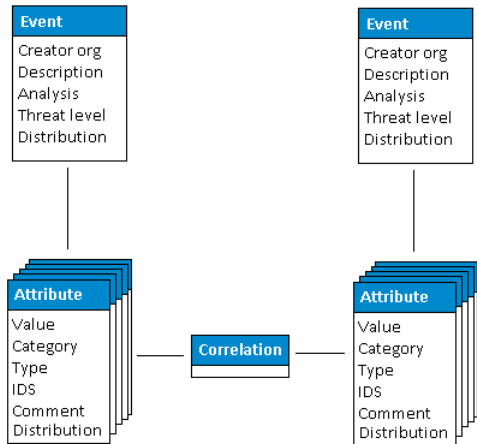
MISP - Event (MISP's basic building block)

| Event |
|--------------|
| Creator org |
| Description |
| Analysis |
| Threat level |
| Distribution |

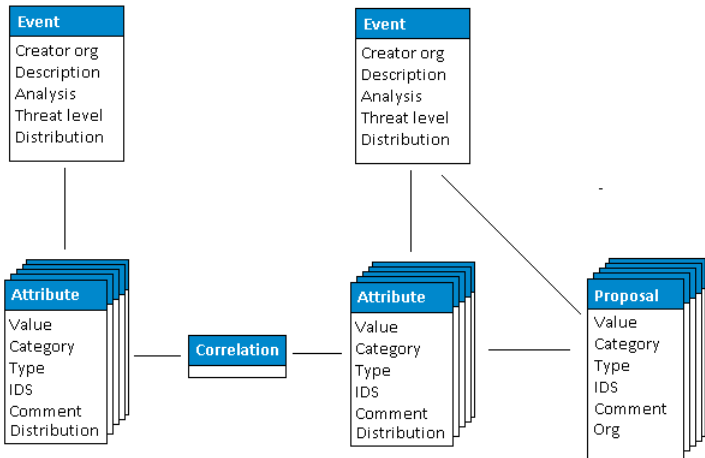
MISP - Event (Attributes, giving meaning to events)



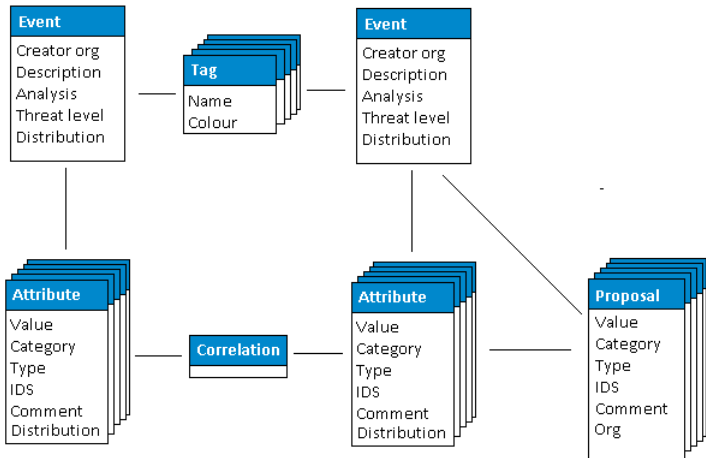
MISP - Event (Correlations on similar attributes)



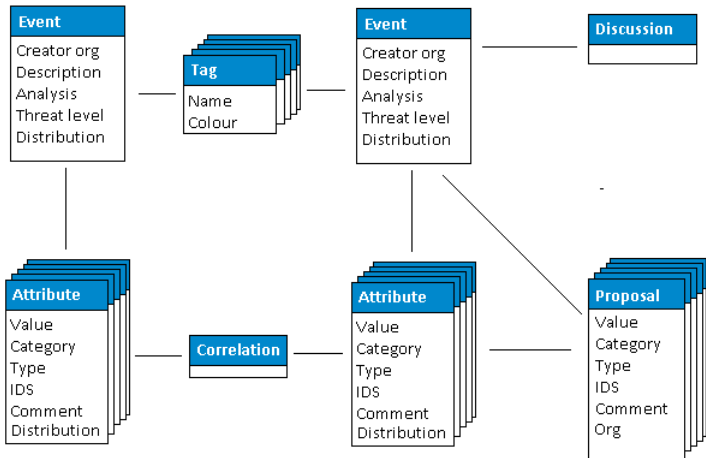
MISP - Event (Proposals)



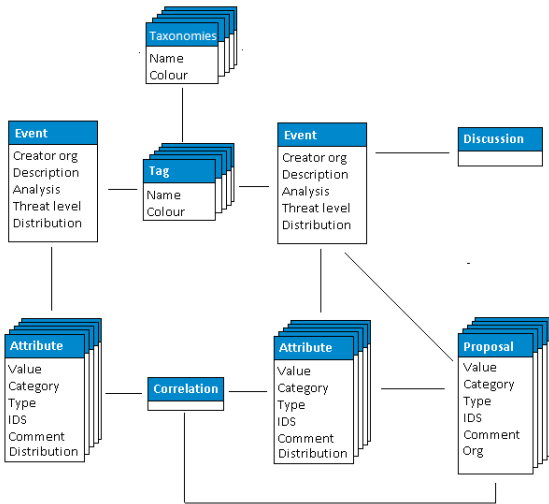
MISP - Event (Tags)



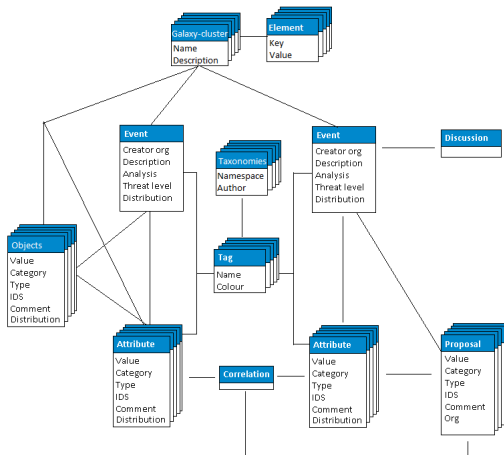
MISP - Event (Discussions)



MISP - Event (Taxonomies and proposal correlations)



MISP - Event (The Future of MISP's 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
 - 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
 - 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

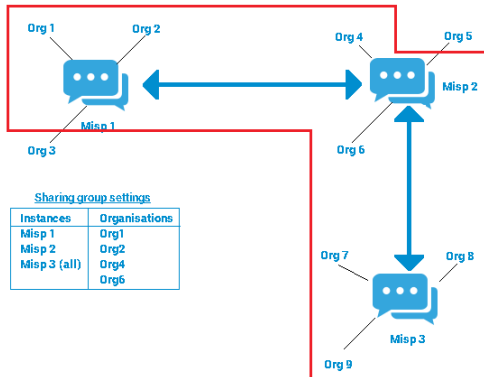
MISP - Feeds explained (if no admin training)

- 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



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