MISP User Training - General usage of MISP

MISP - Threat Sharing

Team CIRCL

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

Cyberspace
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
Plan for this part of the training

- Data model
- Viewing data
- Creating data
- Co-operation
- Distribution
- Exports
# MISP - Event (MISP’s Basic Building Block)

<table>
<thead>
<tr>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creator org</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Analysis</td>
</tr>
<tr>
<td>Threat level</td>
</tr>
<tr>
<td>Distribution</td>
</tr>
</tbody>
</table>
MISP - Event (Attributes, giving meaning to events)
MISP - Event (Correlations on similar attributes)
MISP - Event (Proposals)
MISP - Event (Discussions)
MISP - Event (Taxonomies and Proposal Correlations)

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

Tag
- Name
- Colour

Attribute
- Value
- Category
- Type
- IDS
- Comment
- Distribution

Correlation

Proposal
- Value
- Category
- Type
- IDS
- Comment
- Org

Discussion
MISP - Event (The state of the art MISP datamodel)
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
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 - Using the data

- Correlation graphs
- Downloading the data in various formats
- Cached exports
- 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
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
Download an event
Quick glance at the APIs
Download search results
Cached exports
MISP - Shorthand Admin (If no Admin Training)

- Settings
- Troubleshooting
- Workers
- Logs