MISP User Training - General usage of MISP

MISP - Threat Sharing

Team CIRCL

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

MISP Training @ Luxembourg December Edition 2019
20191203
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)
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 (Tags)

Event
Creator org
Description
Analysis
Threat level
Distribution

Tag
Name
Colour

Event
Creator org
Description
Analysis
Threat level
Distribution

Attribute
Value
Category
Type
IDS
Comment
Distribution

Correlation

Attribute
Value
Category
Type
IDS
Comment
Distribution

Proposal
Value
Category
Type
IDS
Comment
Org
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
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
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
MISP - DISTRIBUTION AND TOPOLOGY

![Diagram of MISP distribution and topology]

Sharing group settings

<table>
<thead>
<tr>
<th>Instances</th>
<th>Organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misp 1</td>
<td>Org1</td>
</tr>
<tr>
<td>Misp 2</td>
<td>Org2</td>
</tr>
<tr>
<td>Misp 3 (all)</td>
<td>Org3, Org4, Org6</td>
</tr>
</tbody>
</table>

Org 1 → Org 2 → Misp 1 → Org 3
Org 4 → Org 5 → Misp 2
Org 6 → Org 7 → Misp 3 → Org 8
Org 9 → Misp 3
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