MISP User Training - General usage of MISP

MISP - Threat Sharing

Team CIRCL

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

ESDC 20200303
- **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
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)
MISP - Event (Correlations on similar attributes)
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
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
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
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>
Download an event
Quick glance at the APIs
Download search results
Cached exports
MISP - Shorthand admin (if no admin training)

- Settings
- Troubleshooting
- Workers
- Logs