MISP User Training - General usage of MISP

MISP - Threat Sharing

Team CIRCL

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

NATO MUG
20191114
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)
MISP - Event (Correlations on similar attributes)
MISP - Event (Proposals)
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
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
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