

MISP User Training - Administration of MISP 2.4

MISP Threat Sharing

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

MISP Training @ SUNET
20190206



- VM can be downloaded at <https://www.circl.lu/misp-training/>
- Credentials
 - ▶ MISP admin: admin@admin.test/admin
 - ▶ SSH: misp/Password1234
- 2 network interfaces
 - ▶ NAT
 - ▶ Host only adapter
- Start the enrichment system by typing:
 - ▶ `cd /home/misp/misp-modules/bin`
 - ▶ `python3 misp-modules.py`

- Plan for this part of the training
 - ▶ User and Organisation administration
 - ▶ Sharing group creation
 - ▶ Templates
 - ▶ Tags and Taxonomy
 - ▶ Whitelisting and Regexp entries
 - ▶ Setting up the synchronisation
 - ▶ Scheduled tasks
 - ▶ Feeds
 - ▶ Settings and diagnostics
 - ▶ Logging
 - ▶ Troubleshooting and updating

- Add new user (andras.iklady@circl.lu)
- NIDS SID, Organisation, disable user
- Fetch the PGP key
- Roles
 - ▶ Re-using standard roles
 - ▶ Creating a new custom role
- Send out credentials

- Adding a new organisation
- UUID
- Local vs External organisation
- Making an organisation self sustaining with Org Admins
- Creating a sync user

- The concept of a sharing group
- Creating a sharing group
- Adding extending rights to an organisation
- Include all organisations of an instance
- Not specifying an instance
- Making a sharing group active
- Reviewing the sharing group

- Why templating?
- Create a basic template
- Text fields
- Attribute fields
- Attachment fields
- Automatic tagging

- `git submodule init` && `git submodule update`
- Loading taxonomies
- Enabling taxonomies and associated tags
- Tag management
- Exportable tags

- git submodule init && git submodule update
- Enabling objects (and what about versioning)

- Block from exports - whitelisting
- Block from imports - blacklisting via regexp
- Modify on import - modification via regexp
- Maintaining the warninglists

- Requirements - versions
- Pull/Push
- One way vs Two way synchronisation
- Exchanging sync users
- Certificates
- Filtering
- Connection test tool
- Previewing an instance
- Cherry picking and keeping the list updated

- How to schedule the next execution
- Frequency, next execution
- What happens if a job fails?

- MISP Feeds and their generation
- PyMISP
- Default free feeds
- Enabling a feed
- Previewing a feed and cherry picking
- Feed filters
- Auto tagging

■ Settings

- ▶ Settings interface
- ▶ The tabs explained at a glance
- ▶ Issues and their severity
- ▶ Setting guidance and how to best use it

- Basic instance setup
- Additional features released as hotfixes
- Customise the look and feel of your MISP
- Default behaviour (encryption, e-mailing, default distributions)
- Maintenance mode
- Disabling the e-mail alerts for an initial sync

- Plugins
 - ▶ Enrichment Modules
 - ▶ RPZ
 - ▶ ZeroMQ

■ Diagnostics

- ▶ Updating MISP
- ▶ Writeable Directories
- ▶ PHP settings
- ▶ Dependency diagnostics

■ Workers

- ▶ What do the background workers do?
- ▶ Queues
- ▶ Restarting workers, adding workers, removing workers
- ▶ Worker diagnostics (queue size, jobs page)
- ▶ Clearing worker queues
- ▶ Worker and background job debugging

■ Seeking help

- ▶ Dump your settings to a file!
- ▶ Make sure to sanitise it
- ▶ Send it to us together with your issue to make our lives easier
- ▶ Ask Github (<https://github.com/MISP/MISP>)
- ▶ Have a chat with us on gitter (<https://gitter.im/MISP/MISP>)
- ▶ Ask the MISP mailing list
- ▶ If this is security related, drop us a PGP encrypted email to `mailto:info@circl.lu`

- Audit logs in MISP
- Enable IP logging / API logging
- Search the logs, the fields explained
- External logs
 - ▶ `/var/www/MISP/app/tmp/logs/error.log`
 - ▶ `/var/www/MISP/app/tmp/logs/resque-worker-error.log`
 - ▶ `/var/www/MISP/app/tmp/logs/resque-scheduler-error.log`
 - ▶ `/var/www/MISP/app/tmp/logs/resque-[date].log`
 - ▶ `/var/www/MISP/app/tmp/logs/error.log`
 - ▶ apache access logs

- `git pull`
- `git submodule init` && `git submodule update`
- reset the permissions if it goes wrong according to the `INSTALL.txt`
- when MISP complains about missing fields, make sure to clear the caches
 - ▶ in `/var/www/MISP/app/tmp/cache/models` remove `myapp*`
 - ▶ in `/var/www/MISP/app/tmp/cache/persistent` remove `myapp*`
- No additional action required on hotfix level
- Read the migration guide for major and minor version changes

- Upgrade scripts for minor / major versions
- Maintenance scripts