MISP User Training - Administration of MISP 2.4

MISP - Malware Information Sharing Platform & Threat Sharing

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy
Andras Iklody
Raphaël Vinot
Gerard Wagener

TLP:WHITE

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

MISP Training @ Luxembourg
20180116

MISP - VM

- 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

MISP - Administration

- Plan for this part of the training
  - User and Organisaton 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

MISP - Creating Users

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

MISP - Creating Organisations

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

MISP - Sharing groups

- 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

MISP - Templates

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

MISP - Tags and Taxonomies

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

MISP - Object Templates

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

MISP - Whitelisting, Regexp entries, Warninglists

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

MISP - Setting up the synchronisation

- 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

MISP - Scheduled tasks

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

MISP - Setting up the synchronisation

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

MISP - Settings and diagnostics

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

MISP - Settings and diagnostics continued

- 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

MISP - Settings and diagnostics continued

- Plugins
  - Enrichment Modules
  - RPZ
  - ZeroMQ

MISP - Settings and diagnostics continued

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

MISP - Settings and diagnostics continued

- 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

MISP - Settings and diagnostics continued

- 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`

MISP - Logging

- 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

MISP - Updating MISP

- 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

MISP - Administrative tools

- Upgrade scripts for minor / major versions
- Maintenance scripts