# MISP USER TRAINING - ADMINISTRA-TION OF MISP 2.4

MISP THREAT SHARING

CIRCL / TEAM MISP PROJECT

HTTP://WWW.MISP-PROJECT.ORG/ TWITTER: @MISPPROJECT

MISP PROJECT



MISP User Training - Administration of MISP 2.4



# 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 User Training - Administration of MISP 2.4

-MISP - VM

2022-

W VM can be downloaded at https://www.circl.lu/misp-training

# Credentials

# 2 network interfaces

# Start the enrichment system by typing

# 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 User Training - Administration of MISP 2.4

└─MISP - Administration

2022-

# Plan for this part of the training

\* User and Organization administrat

\* Sharing group creation

\* Templature

\* Templature

\* Templature

\* Setting and Regeap entries

\* Setting up the synchronization

\* Scheduled tasks

\* Settings and diagnostics

\* Logging

\* Logging

# 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 User Training - Administration of MISP 2.4

☐MISP - Creating Users

2022-09

Add new user (andras iklody@circllu)
INIDS 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 User Training - Administration of MISP 2.4

☐ MISP - Creating Organisations

MISP - CREATING ORGANISATIONS

UUID

Making an organisation self sustaining with Org Adi

# 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 User Training - Administration of MISP 2.4

-MISP - Sharing groups

2022-

· The concept of a sharing group

- Creating a sharing group
- Include all organisations of an instance
- · Making a sharing group active
- m Reviewing the sharing group

# MISP - TEMPLATES

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

MISP User Training - Administration of MISP 2.4

-MISP - Templates

Why templating?
Create a basic template

Text fields

Attribute fields
 Attachment fields
 Automatic tagging

2022-09

# MISP - TAGS AND TAXONOMIES

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

MISP User Training - Administration of MISP 2.4

-MISP - Tags and Taxonomies

2022-

MISP - TAGS AND TAXONOMIES

- # git submodule init && git submodule update
- nabling taxonomies and associated tags
- Tag management
  Exportable tags

# MISP - OBJECT TEMPLATES

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

MISP User Training - Administration of MISP 2.4

–MISP - Object Templates

2022-09

m git submodule init && git submodule update m 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 User Training - Administration of MISP 2.4

MISP - Whitelisting, Regexp entries, Warninglists

· WHITELISTING, REGEXP ENTRIES, LISTS

- from exports whitelisting from imports - blacklisting via regexp
- on import modification via regexp

# 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 User Training - Administration of MISP 2.4

2022-

–MISP - Setting up the synchronisation

MISP - SETTING UP THE SYNCHRONISATION

Requirements - versions

I/Push

e way vs Two way synchronisatio

Exchanging sync users Certificates

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 User Training - Administration of MISP 2.4

└─MISP - Scheduled tasks

■ 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 User Training - Administration of MISP 2.4

2022-

-MISP - Setting up the synchronisation

SP - SETTING UP THE SYNCHRONISATION

MISP Feeds and their generation

- reeds and their generation SP
- Default free feeds
   Enabling a feed
- Enabling a feed
   Previewing a feed and cherry pickir
   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 User Training - Administration of MISP 2.4

└─MISP - Settings and diagnostics



- 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 User Training - Administration of MISP 2.4

2022 09 13

–MISP - Settings and diagnostics continued

instance setup

- litional features released as hotfixes
- Default behaviour (encryption, e-mailing, default
- stributions) sintenance mode
- m Disabling the e-mail alerts for an initial sync

- Plugins
  - ► Enrichment Modules
  - ► RPZ
  - ZeroMQ

MISP User Training - Administration of MISP 2.4

MISP - Settings and diagnostics continued

II Plugins

Enrichment Modules

INSE

2 architect

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

MISP User Training - Administration of MISP 2.4

2022-09-13

MISP - Settings and diagnostics continued

MISP – SETTINGS AND DIAGNOSTICS CO

# Diagnostics

• Updating MISP

• Updating MISP

• PPP 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

MISP User Training - Administration of MISP 2.4

-MISP - Settings and diagnostics continued

Wisp - Settings and Disconstitis ContinueD

White the background workers do?

Whate the background workers do.

Whate the background workers do.

Whate the background policy do.

Whate the background policy 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

MISP User Training - Administration of MISP 2.4

-MISP - Settings and diagnostics continued

IISP - SETTINGS AND DIAGNOSTICS CONTINUED

■ Seeking help

• Dump your settings to a fi

p your settings to a file! I sure to sanitise it

> o us together with your issue to make our live ub (https://github.com/MISP/MISP)

Ask the MISP mailing list
 If this is constituted door us a BGB control of the MISP mailing list.

# 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 User Training - Administration of MISP 2.4

└─MISP - Logging

2022

Audit logs in MSP
 It Inable IP logging
 It Inable IP logging
 It Share I logging
 It Start to log. The fields explained
 It External logs.
 It for logging in the logging in the

## 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 User Training - Administration of MISP 2.4

-MISP - Updating MISP

- m git pull
- # git submodule init && git submodule update m reset the permissions if it goes wrong according to the
- when MISP complains about missing fields, make sur
- No additional action required on hotfix level

# MISP - ADMINISTRATIVE TOOLS

- Upgrade scripts for minor / major versions
- Maintenance scripts

MISP User Training - Administration of MISP 2.4

■ Upgrade scripts for minor / major versions
■ Maintenance scripts

└─MISP - Administrative tools