MISP USER TRAINING - ADMINISTRA-TION OF MISP 2.4

MISP THREAT SHARING

CIRCL / TEAM MISP PROJECT

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

NSPA



MISP User Training - Administration of MISP 2.4



- 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 Organisation administr
Sharing group creation
Implicit
Tags and Tags and Sharing
Whitelesting and Sague on these
Setting up the synchronication
Schioduled tasks
Feeds
Settings and diagnostics
Settings and diagnostics
Settings and diagnostics

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-

■ Add new user (andras.iklody@circLlu)

- Add new user (andras.iklody@circLlu)
 NIDS SID, Organisation, disable user
 Fetch the PGP key
- Re-using standard roles
 Creating a new custom ro

 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 Ar

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

 Attribute fields # Automatic tagging

2022-08

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

git submodule init && git submodule update

- 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

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,

from exports - whitelisting

- m imports blacklisting via regexp
- y on import modification via regexp aining 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 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 synchroni

Certificates
 Diboring

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

low to schedule the next execution requency, next execution that 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

MISP - SETTING UP THE SYNCHRONISATION

MISP Feeds and their generation
 PyMISP

Default free feeds
 Enabling a feed

Previewing a feed and cherry pick
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

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

- 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

-MISP - Settings and diagnostics continued

MSP - SETTINGS AND DIAGNOSTICS CONTINUED

- isic instance setup
- stomise the look and feel of your MISP
- Default behaviour (encryption, e-mailing, default distributions)
- 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

AND DIAGNOSTICS CONTINUED

■ Plugins

► Enrichment Modules

► RPZ

► ZeroMQ

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

MISP User Training - Administration of MISP 2.4

MISP - Settings and diagnostics continued

MISP - SETTINGS AND DIAGNOSTICS CO

II Diagnostics

II Updating MISP

I Writesable Directories

I Writesable Directories

I Workings

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

Workers

* Workers

* Winds do the background workers do?

* Winds do the background workers do?

* Restarting workers, adding workers, removing workers

* Worker diagnostics (speak size, jobs page)

* 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

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 fil

ump your settings to a file! ake sure to sanitise it

> us together with your issue to make our liv b (https://github.com/MISP/MISP)

Have a chat with us on gitter (https://gitter.im/MisP/N
 Ask the MISP mailing list
 If this is populate soluted, doop us a RGB appointed on

the MISP maining list is is security related, drop us a PGP en Lto: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 User Training - Administration of MISP 2.4

└─MISP - Logging

2022

Audit legs in HSP |

Audit legs in HSP |

Enable Plagging | AM legging |

Enable Plagging |

Individual HSP //ap //mp legs //arces erracting |

Audit New HSP //ap //mp legs //arces erracting |

Audit New HSP //ap //mp legs //arces electric |

Audit New HSP //ap //mp legs //arces electric |

Audit New HSP //ap //mp legs //arces electric |

Audit New HSP //ap //mp legs //ap //arces electric |

Audit New HSP //ap //mp legs //arces electric |

Audit New HSP //arces |

Audit N

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
- m git submodule init && git submodule update
- reset the permissions if it goes wrong according to t
 INSTALLEXT
 when MISP complains about missing fields, make su
- clear the caches
 in /var/www/MISP/app/tmp/cache/models remove mya
- myapp*
- 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

ipgrade scripts for minor / major versions laintenance scripts