MISP User Training - General us-AGE OF MISP

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

HTTP://WWW.MISP-PROJECT.ORG/ **TWITTER:** (*OMISPPROJECT*

13TH ENISA-EC3 WORKSHOP



MISP User Training - General usage of MISP



MISP - VM

2024-09-11

MISP User Training - General usage of MISP

└─MISP - VM

51---VIN

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/

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/

MISP - VM

MISP User Training - General usage of MISP

└─MISP - VM

2024-09

It is a bit broken.
 sudo -s
 cd /var/www/MISP/
 sudo paar install

- sudo pear install
- INSTALL/dependencies/Console_CommandLine/pa sudo pear install
- INSTALL/dependencies/Crypt_GPG/package.xml

 Cd_fusr/local/src/misp-modules
- cd /usr/tocal/src/misp-modules
 pip3 install -r REQUIREMENTS
- pip3 install
 reboot

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

MISP - GENERAL USAGE

MISP User Training - General usage of MISP

└─MISP - General Usage

Plan for this part of the training Data model Viewing data Creating data Co-operation Distribution Exports

Plan for this part of the training

Data model

Viewing data

Creating data

Co-operation

Distribution

Exports

7

MISP - EVENT (MISP'S BASIC BUILDING BLOCK)

MISP User Training - General usage of MISP

7

2024-09

MISP - Event (MISP's basic building block)

been Stankering Harright Historykt Distriction

Event Creator org Description Analysis Threat level Distribution

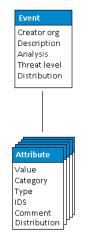
MISP - EVENT (ATTRIBUTES, GIVING MEANING TO EVENTS)

MISP User Training - General usage of MISP

└─MISP - Event (Attributes, giving meaning to events)



Event Creator any Creator any Horizan Darkout Darkout Creator Type Type Darkout Composition



22

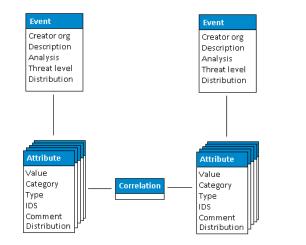
7

MISP - Event (Correlations on similar attributes)

MISP User Training - General usage of MISP

└─MISP - Event (Correlations on similar attributes)

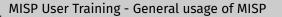




.

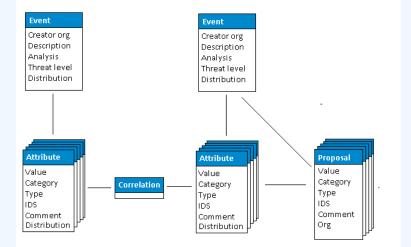
7

MISP - EVENT (PROPOSALS)



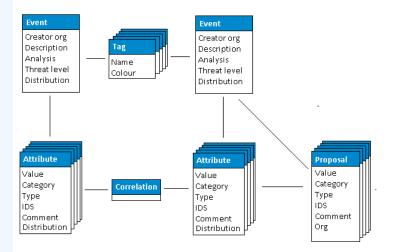
MISP - Event (Proposals)





22

MISP - EVENT (TAGS)



MISP User Training - General usage of MISP

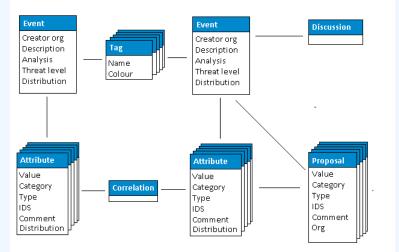
└─MISP - Event (Tags)



8

7

MISP - EVENT (DISCUSSIONS)

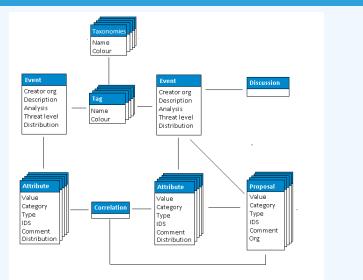


MISP User Training - General usage of MISP

└─MISP - Event (Discussions)



MISP - Event (Taxonomies and proposal correlations)



MISP User Training - General usage of MISP

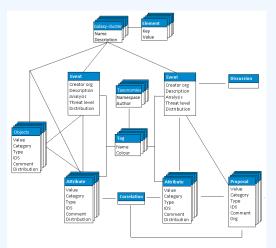
MISP - Event (Taxonomies and proposal correlations)

MISP - EVENT (TAXONOMIES AND PROPOSAL CORRELATIONS)



7

MISP - Event (The state of the art MISP datamodel)



MISP User Training - General usage of MISP

MISP - Event (The state of the art MISP datamodel)

MISP - EVENT (THE STATE OF THE ART MISP DATAMODEL)



MISP - VIEWING THE EVENT INDEX

MISP User Training - General usage of MISP

└─MISP - Viewing the Event Index

Event Index
 Event context
 Tags
 Distribution
 Correlations
 Filters

Event Index

- Event context
- Tags
- Distribution
- Correlations

Filters

12

7

MISP - VIEWING AN EVENT

MISP User Training - General usage of MISP

MISP - Viewing an Event

Event View Event conset Attributes Category/type, tDS, Correlations Object Gataxies Froposals Piclosasions Tools to find what you are looking for E Correlation graphs

Event View

- Event context
- Attributes
 - Category/type, IDS, Correlations
- Objects
- Galaxies
- Proposals
- **Discussions**
- Tools to find what you are looking for
- Correlation graphs

3

MISP - CREATING AND POPULATING EVENTS IN VARIOUS WAYS (DEMO)

2024-09-11

MISP User Training - General usage of MISP

MISP - Creating and populating events in various ways (demo)

MISP - CREATING AND POPULATING EVENTS IN VARIOUS WAYS (DEMO)

The main tools to populate an event

- Adding attributes / batch add
- Adding objects and now the object tempta
 Freetext import
 - Import
 Tomolator
- Adding attachments / screenshi

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

MISP - VARIOUS FEATURES WHILE ADDING DATA

MISP User Training - General usage of MISP

–MISP - Various features while adding data

MISP - VARIOUS FEATURES WHILE ADDING DATA

- What happens automatically when adding data?
- Automatic correlation
- Input modification via validation and filters
 Targing / Galaxy Clusters
- Various ways to publish data
- Publish with/without e-mail
- Publishing via
 Delegation

- 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

2024-09

MISP - USING THE DATA

2024-09-1

MISP User Training - General usage of MISP

MISP - Using the data

Correlation graphs
 Oownloading the data in various formats
 API (explained later)
 Collaborating with users (proposals, discussions, emails)

Correlation graphs

- Downloading the data in various formats
- API (explained later)
- Collaborating with users (proposals, discussions, emails)

MISP - Sync explained (if no admin training)

MISP User Training - General usage of MISP

MISP - Sync explained (if no admin training)

Sync connections
 Pull/push model
 Previewing instances
 Filtering the sync
 Connection test tool
 Cherry pick mode

Sync connections
 Pull/push model
 Previewing instances

Filtering the sync

Connection test tool

Cherry pick mode

MISP - FEEDS EXPLAINED (IF NO ADMIN TRAINING)

2024-09-1

MISP User Training - General usage of MISP

MISP - Feeds explained (if no admin training)

- Feed types (MISP, Freetext, CSV)
- Adding/editing feeds
- Previewing feeds
- Local vs Network feeds

MISP - DISTRIBUTIONS EXPLAINED

MISP User Training - General usage of MISP

MISP - Distributions explained

2024-09

Your Organisation Only
 This Community Only
 Connected Communities
 All Communities
 Sharing Group

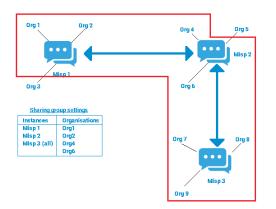
- Your Organisation Only
- This Community Only
- Connected Communities
- All Communities
- Sharing Group

MISP - DISTRIBUTION AND TOPOLOGY

MISP User Training - General usage of MISP

└─MISP - Distribution and Topology





MISP - EXPORTS AND API

$_{\rm \Xi}$ MISP User Training - General usage of MISP $_{\rm \Xi}$

MISP - Exports and API

Download an event
 Quick glance at the APIs
 Download search results
 ReST API and guery builder

- Download an event
- Quick glance at the APIs
- Download search results
- ReST API and query builder

MISP - Shorthand admin (if no admin training)

MISP User Training - General usage of MISP

└─MISP - Shorthand admin (if no admin training)

Troubleshooting

Workers

Logs

7

2024-09

Settings
 Troubleshootin
 Workers

Logs