# MISP User Training - General US-Age of MISP

**MISP - THREAT SHARING** 

CIRCL / TEAM MISP PROJECT

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

**MISP PROJECT** 



MISP User Training - General usage of MISP

9



MISP - VM

MISP User Training - General usage of MISP

└─MISP - VM

09-16

2022-

- Credentials
   MISP admin-admin@admin.test/admin
- Mise aumic aum/gadmintest/admin
   SSH: misp/Password1234
- Available at the following location (VirtualBox and VMWar
- 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

10

2022-09

ISP - VM

- It is a bit broken.
- ► sudo -s
- cd /var/www/MISP/
   sudo pear install
- INSTALL/dependencies/Console\_CommandLine/pac
- sudo pear install INSTALL/dependencies/Crypt\_GPG/package.xml
- cd /usr/local/src/misp-modules
   plog install or REQUIREMENTS
- pip3 install .

- 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

Distribution
 Exports

# Plan for this part of the training

- Data model
- Viewing data
- Creating data
- Co-operation
- Distribution
- Exports

# MISP - Event (MISP'S BASIC BUILDING BLOCK)

#### MISP User Training - General usage of MISP

MISP - Event (MISP's basic building block)

Devel Constances Newspron Accepto Thrust Newspron Distribution

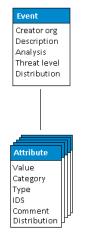
Event Creator org Description Analysis Threat level Distribution 16

# MISP - EVENT (ATTRIBUTES, GIVING MEANING TO EVENTS)

MISP User Training - General usage of MISP

MISP - Event (Attributes, giving meaning to events)



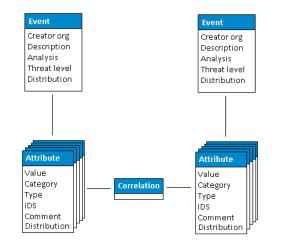


# MISP - Event (Correlations on similar attributes)

MISP User Training - General usage of MISP

└─MISP - Event (Correlations on similar attributes)





22

~

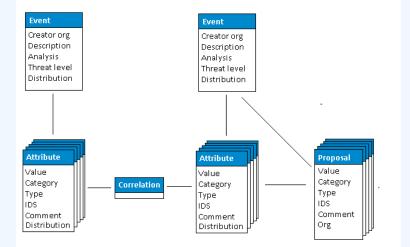
-16

# MISP - EVENT (PROPOSALS)



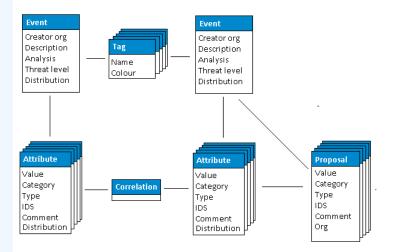
MISP - Event (Proposals)





22

# MISP - EVENT (TAGS)



MISP User Training - General usage of MISP

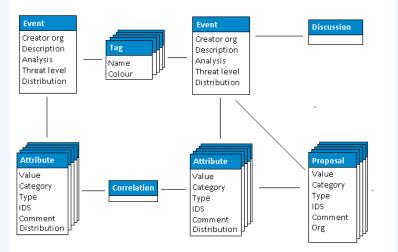
└─MISP - Event (Tags)



#### 8

10

# MISP - EVENT (DISCUSSIONS)



#### MISP User Training - General usage of MISP

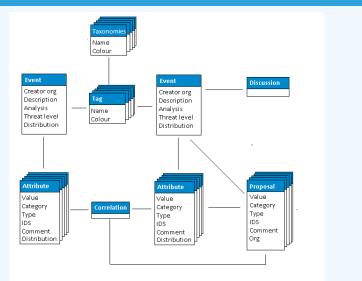
└─MISP - Event (Discussions)



9

10

# MISP - Event (Taxonomies and proposal correlations)



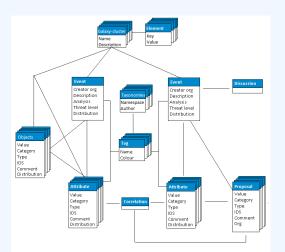
MISP User Training - General usage of MISP

└─MISP - Event (Taxonomies and proposal correlations)

MISP - EVENT (TAXONOMIES AND PROPOSAL CORRELATIONS)

09-16

# 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)

09-16

# 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

# **MISP - VIEWING AN EVENT**

#### MISP User Training - General usage of MISP

MISP - Viewing an Event

Event View
 Event costat
 Extractist
 Costat
 Costation
 Costation
 Costation
 Costation
 Poposals
 Mosasions
 Tools to find what you are looking for
 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

16

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

2022-09-16

#### 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 temps
   Freetext import
  - Import
     Tomplates
- Adding attachments / screensh

#### 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

10

2022-09

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 (reg
- Tagging / Galaxy Clusters
   Wariour wave to publish data
- Publish with/without e-mail
- Publishing via
   Delogation

- 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

## MISP - USING THE DATA

MISP User Training - General usage of MISP

MISP - Using the data

-09-16

2022-

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
Full/push model
Freviewing 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

-09-16

# MISP - FEEDS EXPLAINED (IF NO ADMIN TRAINING)

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

# ■ Feed types (MISP, Freetext, CSV)

- Adding/editing feeds
- Previewing feeds
- Local vs Network feeds

-09-16

## MISP - DISTRIBUTIONS EXPLAINED

#### MISP User Training - General usage of MISP

16

2022-09

MISP - Distributions explained

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

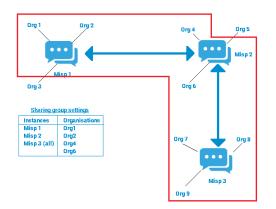
- Your Organisation Only
- This Community Only
- Connected Communities
- All Communities
- Sharing Group

# MISP - DISTRIBUTION AND TOPOLOGY

#### MISP User Training - General usage of MISP

└─MISP - Distribution and Topology





16

## **MISP - EXPORTS AND API**

#### MISP User Training - General usage of MISP

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)

Settings
 Troubleshootin
 Workers

Logs

#### Settings

Troubleshooting

Workers

Logs

16