

How to install MISP on Ubuntu

If you are looking to install MISP for work or on your home lab, then this quick guide might be of use for you.

MISP has done a good job in creating install scripts that do most if not all the work for you.

You can easily run the following to do about 99% of the configuration for you.

```
wget -O /tmp/INSTALL.sh  
https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh ; bash  
/tmp/INSTALL.sh
```

```
wget -O /tmp/INSTALL.sh  
https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh ; bash  
/tmp/INSTALL.sh -c
```

Once the deployment finishes, you should be able to navigate to the IP or hostname of the machine you deployed MISP on. Example, <https://hostname> or https://IP_address.

At the login screen you should use the following default credentials, this will then prompt you to change the default admin password.

```
Username: admin@admin.test  
Password: admin
```

Congratulations! At this point you should have the base installation of MISP and will be ready to go!

Initial Install, please configure



Welcome to MISP on ubuntu, change this message in
MISP Settings

Login

Email

Password

[No account yet? Register now!](#)

Login

On doit modifier le mot de passe de admin (le mot de passe doit être complexe et assez long).

[Home](#) [Event Actions](#) [Dashboard](#) [Galaxies](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Administration](#) [Logs](#) [API](#)

[Edit My Profile](#)
[Change Password](#)
[My Profile](#)
[My Settings](#)
[Set Setting](#)
[Dashboard](#)
[List Organisations](#)
[Role Permissions](#)
[List Sharing Groups](#)
[Add Sharing Group](#)

[User Guide](#)
[Terms & Conditions](#)
[Statistics](#)

Change Password

Password ⓘ

Confirm Password

Confirm with your current password

Submit

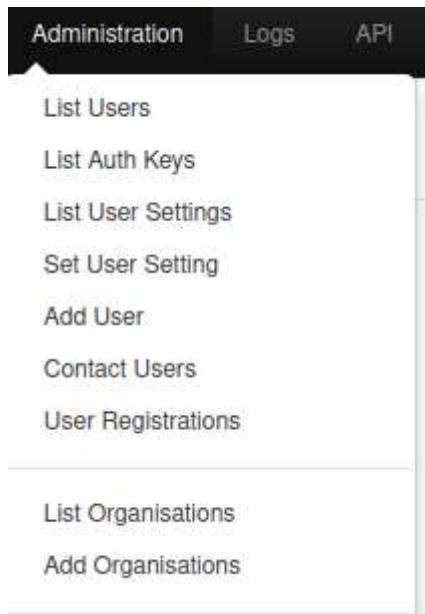
L'installation de MISP est finie.

Configuration de MISP

Création d'une nouvelle organisation

Nous allons ajouter une nouvelle organisation en relation avec notre entreprise.

Pour cela, on clique sur Administration -> Add Organisations



On renseigne les informations.

Add Organisation

Mandatory Fields

☒ Local organisation

ⓘ If the organisation should have access to this instance, make sure that the Local organisation setting is checked. If you would only like to add a known external organisation for inclusion in sharing groups, uncheck the Local organisation setting.

Organisation Identifier

CtechMat

UUID

f14b44e1-be08-42bd-9ea2-8d5481110af8

Generate UUID

Optional Fields

A brief description of the organisation

Organisation de CtechMat

Bind user accounts to domains (line separated)

ctechmat.fr

Logo (48×48 PNG or SVG)

Parcourir... Aucun fichier sélectionné.

Nationality

France

Sector

Home

Type of organisation

Organisation personnelle

Contact details

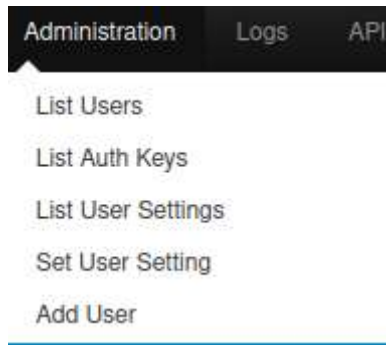
admin@ctechmat.fr

Submit

Création d'un administrateur pour la nouvelle organisation

On va maintenant ajouter un utilisateur administrateur de notre nouvelle organisation.

On clique sur Administration -> Add User



On renseigne les informations.

Admin Add User

Email

☒ Set password

Password ⓘ

Confirm Password

Organisation

Role

NIDS SID



Sync user for

PGP key

Paste the user's PGP key here or try to retrieve it from the CIRCL key server by clicking on "Fetch PGP key" below.

Fetch PGP key

- ☒ Receive email alerts when events are published
- ☒ Receive email alerts from "Contact reporter" requests
- ☐ Immediately disable this user account
- ☒ Send credentials automatically

Create user

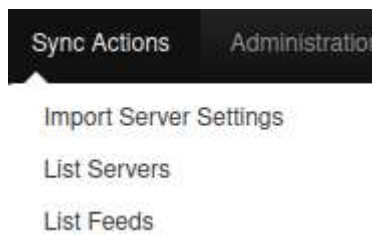
On clique sur Create user

Activation des feeds est importation des IOCs

Maintenant nous allons ajouter des feeds c'est à dire des IOCs partagés par d'autres organisations.

On se connecte avec l'utilisateur admin de notre nouvelle organisation.

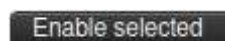
On clique sur Sync Actions -> List Feeds



On sélectionne les feeds qu'on souhaite activer. A vous de voir ce que vous souhaitez cocher (en fonction de votre type d'organisation ou de vos besoins).

A table with columns for selection, name, type, source, URL, status, and actions. It lists several feeds like 'CVE sources', 'Security Scanner', 'Phishbox', 'Threatbox', 'StressOverflow', and 'URLbase'. Each row has checkboxes for 'Feed not enabled', 'Feed not enabled', and 'Feed not enabled', along with a 'Feed not enabled' button and a 'Not enabled' status indicator.

On clique sur Enable selected



Maintenant on peut cliquer sur Fetch and store all feed data.



En cliquant sur Home, vous devriez voir arriver les Events. L'arrivée des informations peut mettre un certain temps.

A table with columns for selection, name, type, source, tags, date, info, and actions. It lists several events like 'OSINT Exposure on Cybermatics cyber attacks against small and medium targets going on for a year by Moscow', 'OSINT Exposure on Additional intelligence relating to Turkey (APT38) phishing campaign by FWC', and 'OSINT Exposure: Tracking from high-level command groups by Synapse'. Each row has checkboxes for 'Published', 'Created on', 'Created on', and 'Created on', along with a 'Published' button and a 'Not published' status indicator.

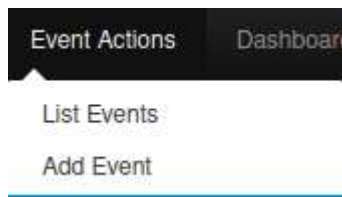
Pour voir le contenu d'un event, il faut cliquer sur l'œil en bout de ligne.

Ajout d'event "à la main"

On va maintenant voir comment ajouter un Event et comment ajouter des attributs "à la main". Par attribut, on veut dire un IOC tel que une url, un hash de fichier, un nom de domaine etc...

Ces Events et attributs sont souvent ajoutés par rapport à vos trouvailles lors de votre veille techno ou lors de vos investigations sur votre infrastructure.

On clique sur Event Actions -> Add Event



On renseigne les informations.

Add Event







Date	Distribution ⓘ
<input type="text" value="2021-10-11"/>	<input type="text" value="Your organisation only"/>
Threat Level ⓘ	Analysis ⓘ
<input type="text" value="Medium"/>	<input type="text" value="Initial"/>
Event Info	
<input type="text" value="Test - Ajout premier event"/>	
Extends Event	
<input type="text" value="Event UUID or ID. Leave blank if not applicable."/>	
<input type="button" value="Submit"/>	








- Date : date de création de l'événement
- Distribution : avec qui on souhaite partager les informations
- Threat Level : la criticité que l'on souhaite attribuer à cet événement
- Analysis : progression de la création
- Event Info : Le titre de l'événement

On clique sur Submit.

Nous arrivons sur notre Event.

Test - Ajout premier event

Event ID	1554
UUID	0d03a427-5a81-4635-a5ec-8b748d9d322b  
Creator org	CachMat
Owner org	CachMat
Creator user	admin@cachmat.fr
Tags	 
Date	2021-10-11
Threat Level	— Medium
Analysis	Initial
Distribution	Your organisation only 
Info	Test - Ajout premier event
Published	No
#Attributes	0 (0 Objects)
First recorded change	
Last change	2021-10-11 21:12:39
Modification map	
Sightings	0 (0) - restricted to own organisation only 

 [Phish](#)  [Galaxy](#)  [Event graph](#)  [Event timeline](#)  [Correlation graph](#)  [ATT&CK matrix](#)  [Event reports](#)  [Attributes](#)  [Discussion](#)

 1554: Test - Ajout p...

On va maintenant ajouter un attribut de type domaine. Pour cela, on clique sur Add Attribute sur la partie droite.

View Event

View Correlation Graph

View Event History

—

Edit Event

Delete Event

Add Attribute

Nous renseignons les informations.

Add Attribute

Category ⓘ

Network activity ▼

Type ⓘ

domain ▼

Distribution ⓘ

Inherit event ▼

Value

testdomaine.fr

Contextual Comment

domaine de test

☐ For Intrusion Detection System

☐ Batch Import

☐ Disable Correlation

First seen date 📅

2021-10-11

Last seen date 📅

2021-10-11

First seen time ⌚

HH:MM:SS.ssssss+TT:TT

Last seen time ⌚

HH:MM:SS.ssssss+TT:TT

⌚ Expected format: HH:MM:SS.ssssss+TT:TT

Submit

- Category : la catégorie de l'information
- Type : le type de l'information
- Distribution : avec qui on souhaite partager les informations
- Value : la valeur de l'attribut ou de l'IOC
- Contextual Comment : un commentaire en rapport avec l'attribut

On clique sur Submit.

Notre premier attribut vient d'être ajouté.



Conclusion

Nous venons de voir comment installer et configurer MISP. Dans un prochain article, nous verrons comment utiliser les information de MISP lors de l'ingestion des logs par Graylog.

Bonne installations à tous.