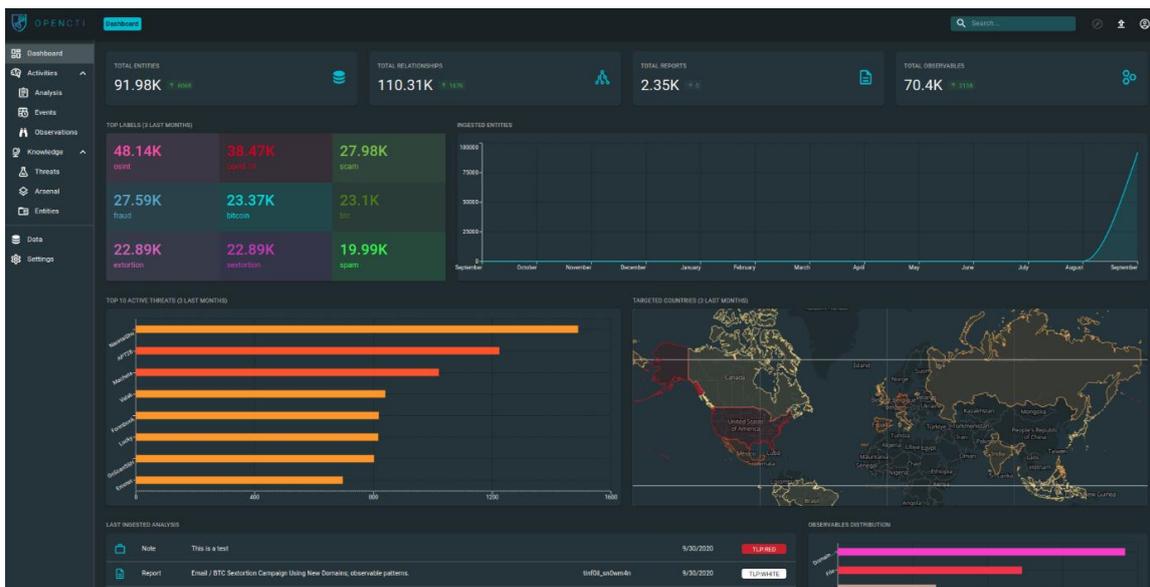
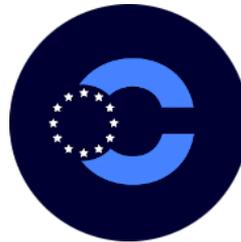


Dates des modifications :	Intervenants :	Modifications apportées :
-	Matthieu BILLAUX (@_euzebius)	Nummmber One Mentor !
Samedi 19 Février 2022	Julien RICHARD (@richardjulien)	Co-fondateur de OpenCTI et Relecture (v0.0.6)
Mercredi 16 Février 2022	Philippe SEGRET (Pich)	Finalisation du document (v0.0.5)
Lundi 14 Février 2022 Samedi 15 Janvier 2022	Mudsor MASOOD (@_mudpak)	Ajout de la partie OpenCTI (v0.0.4)
Mercredi 5 Janvier 2022	(@_mudpak)	Ajout de la partie docker (v0.0.3)
Mardi 23 Novembre 2021	Hamza KONDAH (@kondah_ha)	Aide Technique et Webinaire (v0.0.2)
Dimanche 31 Octobre 2021	(@_mudpak)	Création du document (v0.0.1)



# OPENCTI



## Table des matières

0.	Avant-propos.....	5
1.	Prérequis .....	6
2.	OpenCTI – Présentation de la plateforme.....	7
2.1	Fondateurs.....	7
2.2	Site Officiel .....	8
2.2.1	Télécharger.....	8
2.2.2	Démonstration.....	9
2.2.3	Feuille de route / Roadmap.....	10
2.2.4	Ecosystème.....	10
2.2.5	Documentation.....	11
2.2.6	GitHub.....	12
2.2.7	Blog.....	13
2.2.8	Contact .....	13
2.2.9	Swag .....	14
3.	Ubuntu Server .....	15
3.1	Installation.....	15
3.1.1	Willkommen ! Bienvenue ! Welcome !.....	15
3.1.2	Mise à jour de l'installateur.....	15
3.1.3	Configuration clavier .....	16
3.1.4	Connexions réseau .....	17
3.1.5	Configurer le proxy.....	18
3.1.6	Configuration du serveur miroir.....	18
3.1.7	Configuration guidée du stockage.....	19
3.1.8	Configuration du stockage.....	20
3.1.9	Confirmer l'action.....	20
3.1.10	Configuration du profil .....	21
3.1.11	SSH Setup.....	22
3.1.12	Featured Server Snaps.....	23
3.1.13	Installation du système .....	24
3.1.14	Installation terminée !.....	25
3.1.15	Première connexion .....	25
3.1.16	Configuration IP.....	26
3.2	Connexion SSH.....	27
3.3	Mise à jour de la liste des paquets.....	28

3.4	Installation des nouveaux paquets.....	29
4.	Docker .....	31
4.1	Passage en mode « root » .....	31
4.2	Récupération du script .....	31
4.3	Exécution du script .....	32
4.4	Installation.....	32
4.5	Ajout au groupe « docker ».....	34
4.6	Vérification des changements.....	34
5.	Docker-Compose – Part 1.....	35
5.1	Installation de docker-compose .....	35
5.2	Vérification de la version.....	36
6.	OpenCTI – Installation .....	37
6.1	Via l’image virtuelle .....	37
6.2	Via Terraform .....	37
6.3	Manuelle.....	38
6.4	Via Docker.....	39
6.4.1	Création du répertoire.....	39
6.4.2	Récupération du répertoire.....	40
6.4.3	Contenu du répertoire.....	40
6.4.4	.env .....	41
6.4.5	ElasticSearch.....	43
6.4.6	docker-compose.yml .....	43
7.	Sources de données gratuites .....	51
7.1	AlienVault OTX.....	52
7.1.1	SIGN UP.....	52
7.1.2	Welcome to AlientVault OTX.....	53
7.1.3	LOG IN.....	54
7.1.4	Ajout du connecteur.....	56
7.2	CVE.....	57
8.	Sources de données payantes.....	58
9.	Docker Compose – Part 2 .....	59
10.	OpenCTI – Découverte de l’interface web .....	61
10.1	Connexion à l’interface web.....	61
10.2	Tableau de bord.....	62
10.2.1	Recherche.....	62

10.2.2	Recherche avancée.....	62
10.2.3	Tableaux de bords personnalisés .....	64
10.2.4	Investigations .....	65
10.2.5	Importation de données.....	65
10.2.6	Profil .....	66
10.2.7	Se déconnecter.....	68
10.3	Activités .....	69
10.3.1	Analyses.....	69
10.3.2	Evènements.....	88
10.3.3	Observations.....	90
10.4	Connaissances .....	97
10.4.1	Menaces .....	97
10.4.2	Arsenal.....	101
10.4.3	Entités.....	107
10.5	Données.....	115
10.6	Paramètres .....	121
10.6.1	Paramètres .....	121
10.6.2	Accès.....	124
10.6.3	Workflows .....	130
10.6.4	Politique de rétention .....	131
10.6.5	Moteur de règles .....	131
10.6.6	Labels & attributs .....	132
11.	Erreurs courantes .....	135
11.1	Docker .....	135
11.2	Docker-Compose .....	135
11.3	OpenCTI.....	135
12.	Conclusion .....	136
13.	Sources .....	136

## 0. Avant-propos

Ce document a pour but de guider l'utilisateur dans la présentation, mise en place et personnalisation de la plateforme OpenCTI.

Nous allons voir en détails comment alimenter la plateforme en données CTI via les différents connecteurs.

Le monde de la CTI étant une de mes passions, j'ai eu l'occasion de tester différentes plateformes, mais je dois admettre que depuis que j'ai découvert OpenCTI je suis totalement conquis !

C'est pourquoi je ne vais pas non seulement parler de la solution mais également de tout l'environnement qui la concerne (fondateurs, site web, communauté ...).

Bien que ce document soit assez complet, il est important de noter qu'il n'a pas vocation à remplacer la documentation officielle de l'outil, qui est tenue à jour très régulièrement !

Tout au long du document je vais évoquer l'utilisation de connecteurs externes pour enrichir la plateforme, mais il faut garder en tête que c'est votre plateforme, et que les informations qui l'enrichissent peuvent très bien provenir de vos services ainsi il vous est tout à fait possible d'ajouter des éléments propres à votre contexte pour venir enrichir la plateforme en plus des données récoltées par les sources externes (prestataires, communautés CTI ...).

## 1. Prérequis

Il faut

- Avoir accès à internet
  - Pour télécharger, installer les mises à jour, les paquets nécessaires pour la solution
- Avoir une machine avec les droits root ou suffisants pour installer des programmes
  - Dans la suite un serveur Ubuntu 20.04 LTS est utilisé
- Se conformer à la configuration requise pour la solution OpenCTI
  - Les prérequis sont détaillés par la suite
- Avoir une adresse email valide pour créer les comptes sur les plateformes
  - Vous devez avoir accès à cette messagerie pour confirmer votre compte
  - Ici il est question de validation de votre compte sur les plateformes où vous allez vous inscrire pour récupérer la clé API pour alimenter OpenCTI en données et non de la création du compte sur votre instance locale
- Avoir suffisamment d'espace disque pour les données qui seront stockées à travers le temps

Remarques :

- La mise en place de certains prérequis est détaillée par la suite pour avoir un résultat le plus proche à celui du document.
- Le but est d'obtenir une CTI fonctionnelle, de nombreuses « mauvaises pratiques » sont appliquées lors de la mise en place et elles sont précisées.
- Les « bonnes pratiques » sont indiquées pour ne pas faire les mêmes erreurs.

## 2. OpenCTI – Présentation de la plateforme

OpenCTI permet la gestion et partage de connaissances et est Open-Source.

Pour avoir une présentation plus complète je vous invite à consulter les ressources suivantes :

- <https://www.opencti.io/fr/>
- <https://www.ssi.gouv.fr/actualite/opencti-la-solution-libre-pour-traiter-et-partager-la-connaissance-de-la-cybermenace/>
- <https://github.com/OpenCTI-Platform/opencti>

### 2.1 Fondateurs

OpenCTI a été fondé par les entités suivantes

- ANSSI – Agence Nationale de la Sécurité des Système d’Information
- CERT-EU – Computer Emergency Response Team

Et principalement par les personnes suivantes qui sont co-fondateurs de l’initiative Luatix.

- Samuel HASSINE
- Julien RICHARD

OpenCTI est membre de l’initiative Luatix, à cet instant voici les produits créés par cette initiative :

- <https://www.luatix.org/fr/>



**OPENEX**  
Planification d'exercices de crise



**OPENCTI**  
Analyse de la cybermenace



**OPENCRISIS**  
Gestion de crise



**HACK ME IF U CAN**  
Maîtrise des risques

## 2.2 Site Officiel

Nous allons voir le site de OpenCTI rapidement, les ressources présentes dessus vont nous être utiles par la suite.

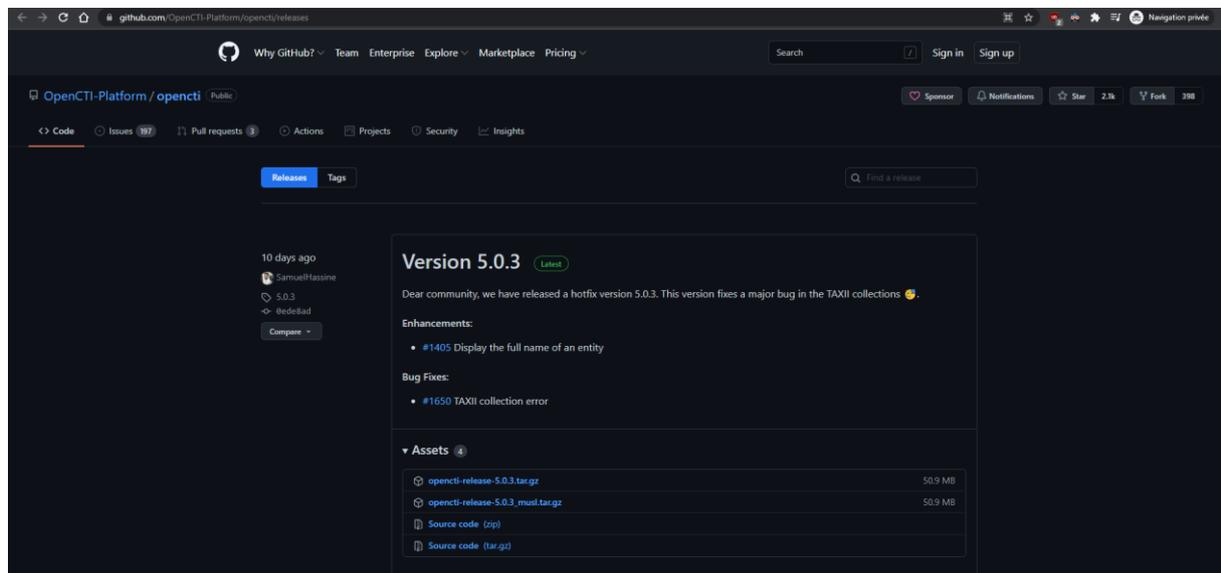
Le site officiel se trouve à l'adresse suivante :

- <https://www.opencti.io/fr/>



### 2.2.1 Télécharger

En cliquant sur « TELECHARGER » vous êtes redirigés vers la page GitHub :



### 2.2.2 Démonstration

En cliquant sur « DEMONSTRATION » vous pouvez visualiser une démonstration live de la solution avant sa mise en place.



Pour visualiser la démo vous pouvez utiliser un compte existant

- Google
- GitHub
- Facebook

Ou créer un compte via une adresse email :



### 2.2.3 Feuille de route / Roadmap

Cette page permet de consulter les évolutions à venir sur la plateforme :

**STABILISATION ET DOCUMENTATION**  
T3 2019 : ACCUEIL LES NOUVEAUX UTILISATEURS

La première priorité des version mineures qui ont suivi la publication du code source a été de stabiliser les fonctionnalités basiques. L'objectif actuel est de permettre aux nouveaux utilisateurs de s'approprier le schéma de connaissance et l'implémentation du modèle hypergraphe grâce à une documentation complète et une instance de démonstration peuplée par des données. Il s'agit aussi d'expliquer la vision à long terme de la plateforme.

**GESTION DES CONNAISSANCES**  
T3 2019 : ORGANISATION DES CONNAISSANCES DE LA CYBERMENACE

La première version d'OpenCTI a été créée pour permettre aux organisations de capitaliser et de visualiser simplement leur connaissance de la cybermenace. Des premières fonctionnalités basiques ont été implémentées pour modéliser cette connaissance (schéma hypergraphe) en se basant sur les rapports entrés dans la plateforme. Différentes visualisations ont été développées pour permettre de parcourir et de pivoter autour de cette connaissance ont été développées.

### 2.2.4 Ecosystème

Cette page recense les informations sur l'API, les connecteurs, les méthodes d'enrichissement de la plateforme, les modules d'importations et les modules tiers.

OpenCTI Ecosystem

OpenCTI is an open and modular platform, so the community provides a lot of documentation, video, components or connectors that work with the platform.

We maintain a list of these elements here as soon as we know they exist.

API clients  
Connectors  
About OpenCTI

#### API clients

Clients list

Language	Last version	Documentation
Python client	5.0.3	Read The Doc
Go client	-	-

COUNT 2

#### Connectors

Data import

- AlienVault  
OpenCTI Community  
5.0.X  
Data import External service
- AM!TT  
CoqSec Collaborative  
5.0.X  
Data import External service
- CrowdStrike  
OpenCTI Community  
5.0.X  
Data import External service
- Cryptolaemus  
Luustik  
5.0.X  
Data import External service

## 2.2.5 Documentation

Cette page recense la documentation et informations nécessaires sur la plateforme :

OpenCTI Public Knowledge Base

Comment

Search

...

Try Notion



# OpenCTI Public Knowledge Base

Welcome to the OpenCTI documentation. Here you will be able to find all documents, meeting notes and presentations about the platform. This base is maintained by the [Luatix](#) non-profit organization and other OpenCTI [contributors](#).

💡 You need some help? You have questions about the platform? [Join us on Slack!](#)

We are doing our best to keep this documentation up to date with the current OpenCTI version. If you find something which is not sufficiently explained or out of date, please create a comment or hit us on the slack channel.

## Documentation

Please find below the documentation about how to deploy and maintain the platform, how to use it and how to contribute.

### Deployment & setup

- 🌐 [Overview](#)
- 📦 [Installation and upgrade](#)
- 🔧 [Configuration](#)
- 🔗 [Connectors](#)
- 🔥 [Troubleshooting](#)

### Usage

- 📖 [Introduction](#)
- 🔗 [Data model](#)
- 🕒 [Browse the knowledge](#)
- 📄 [Update the knowledge](#)
- 📁 [Import & Export](#)

### Development

- 🌟 [GraphQL API](#)
- 📺 [Events streaming](#)
- 🏠 [Environment setup](#)
- 🔗 [Connector Development](#)
- 🔧 [Frontend](#)

## Tutorials

📖 All tutorials are published directly on the [Medium blog](#), this section provides a comprehensive list of the most important ones.

🔧 [Tutorial 1](#)

🔧 [Tutorial 2](#)

🔧 [Tutorial 3](#)

## Community & product

🔥 No one is working full time developing OpenCTI yet. You want to help us? Please consult the [👉 We need help](#) dedicated section.

👉 [We need help](#)

📊 [Performances tests & metrics](#)

🌐 [OpenCTI Ecosystem](#)

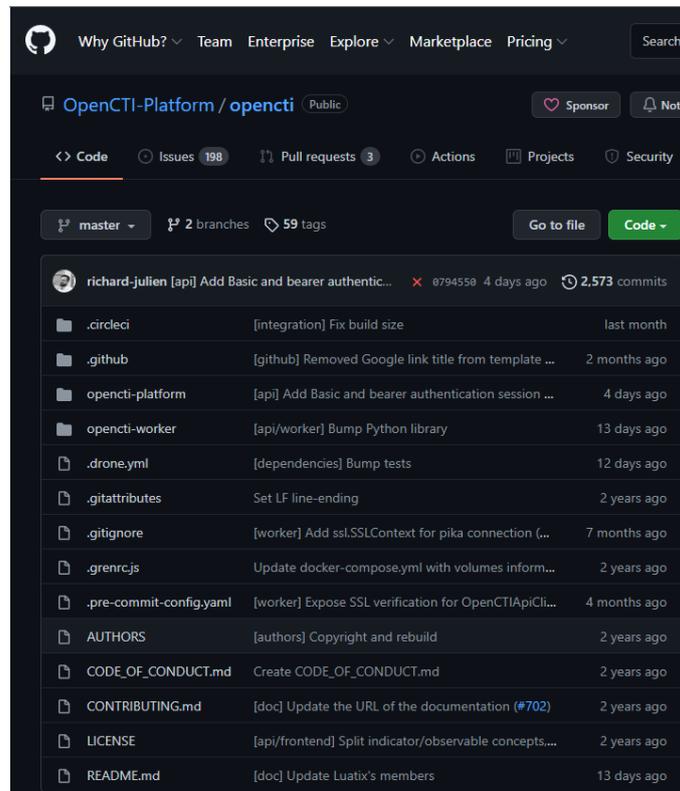
📅 [Events & conferences](#)

📚 [Trainings](#)

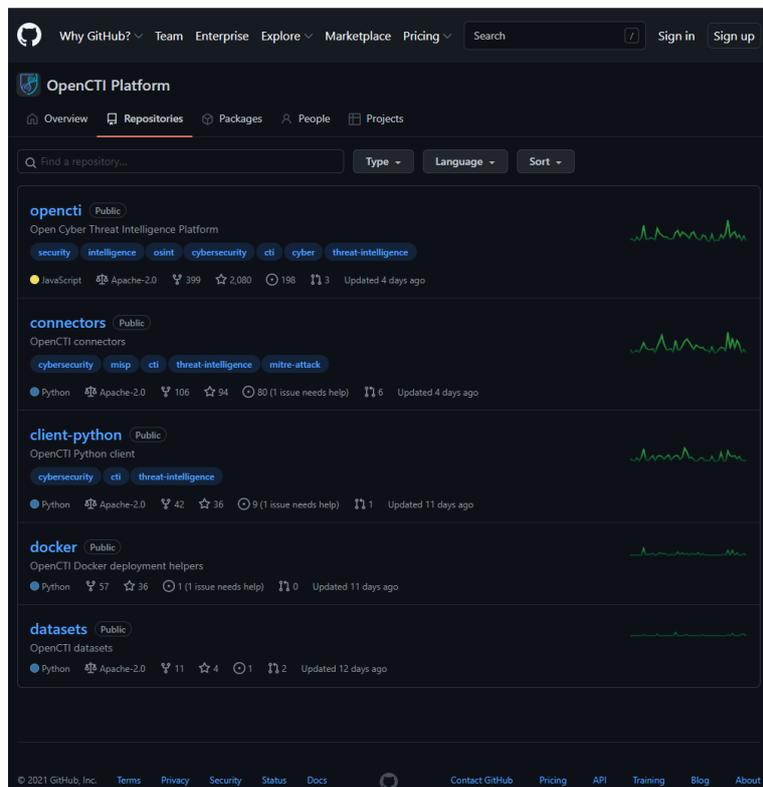
🗺️ [Strategic roadmap](#)

## 2.2.6 GitHub

La page GitHub du projet est la suivante :

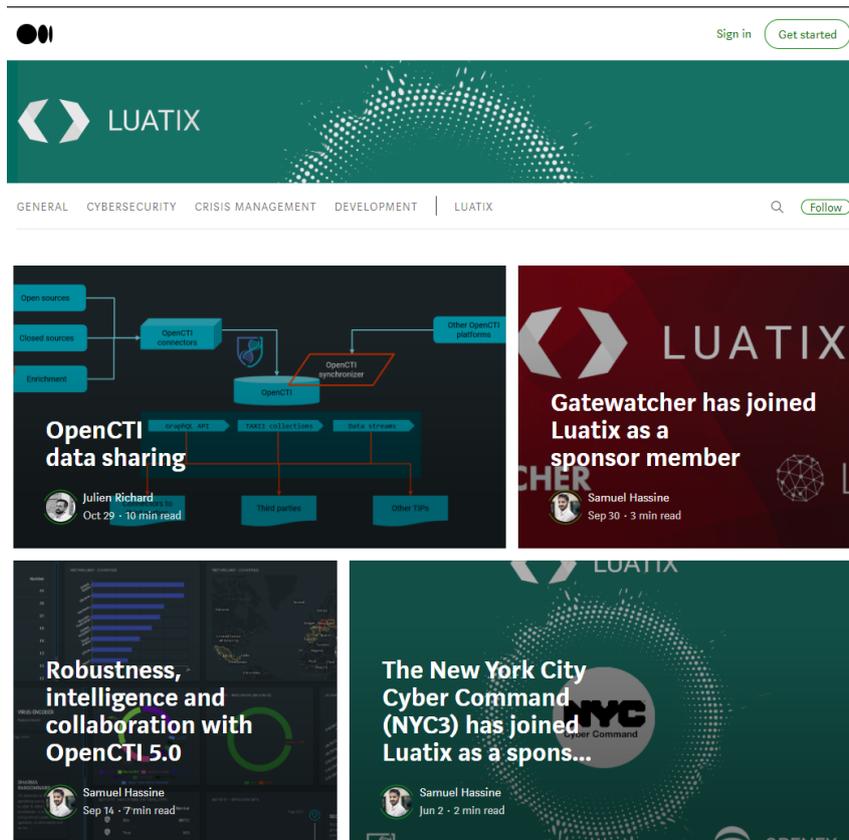


D'autres répertoires du même projet nous seront utiles par la suite :



## 2.2.7 Blog

Des articles intéressants sont disponibles sur le blog :



## 2.2.8 Contact

Si vous souhaitez contacter les membres du site vous pouvez soit les contacter via Slack ou soit remplir le formulaire :

The screenshot shows the LUATIX contact page. The header includes the LUATIX logo and navigation links for BLOG, SLACK, A PROPOS, and CONTACT. The page is divided into two main sections:

- Information**: A text block stating: "Vous avez des questions concernant Luatix ou ses produits ? Vous avez besoin de support ou de services ? N'hésitez pas à rentrer en contact avec nous."
- CONTACT**: A form with the following fields:
  - Prénom \*
  - Nom \*
  - Email \*
  - Site internet
  - Message

Below the form, there are two buttons: "Rejoindre notre espace Slack" (with a Slack icon) and "Ecrire un email" (with an email icon). A red "CONTACTEZ-NOUS" button is located at the bottom right of the form area.

### 2.2.9 Swag

Si vous souhaitez acheter des goodies OpenCTI, vous pouvez les commander à cet endroit :

The screenshot shows the OpenCTI Swag Store interface. At the top, there are navigation links for 'Men', 'Women', and 'Accessories & Hats', along with a user profile icon and a shopping cart icon with a red notification bubble. Below the navigation is a dark header with the OpenCTI logo and the text 'OPENCTI'. The main content area is titled 'OpenCTI Swag Store' with the tagline 'No harmed animals, no profit margin'. The store displays a grid of nine merchandise items, each with a product image, a caption, and a price:

Item	Price
Painting - Keep calm	31.52€
Hoodie - Women - Embroidery	31.5€
Polo - Men - Embroidery - Ce...	36.4€
Bag - Ethical	20.7€
Sport bag - Center	31€
Polo - Women - Embroidery	29€
Beanie - Grey	10€
Beanie - Blue	10.5€
Mug - Center	11.22€

## 3. Ubuntu Server

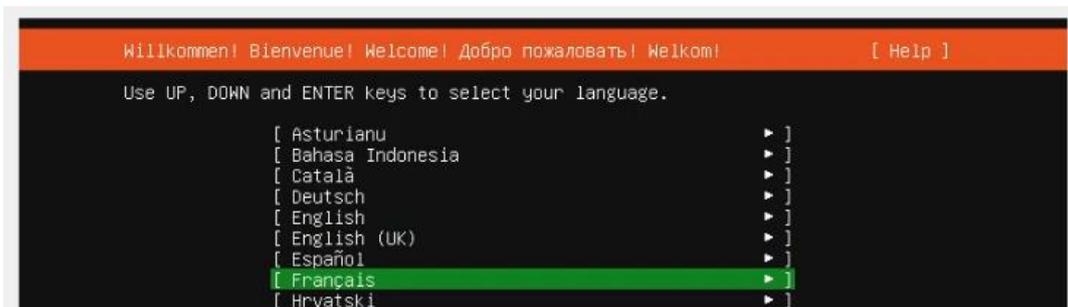
### 3.1 Installation

Nous allons détailler le processus d'installation du système d'exploitation.

#### 3.1.1 Willkommen ! Bienvenue ! Welcome !

Sélectionner la langue d'installation désirée et appuyer sur la touche « Entrée », dans le cas présent nous avons choisi la langue Française :

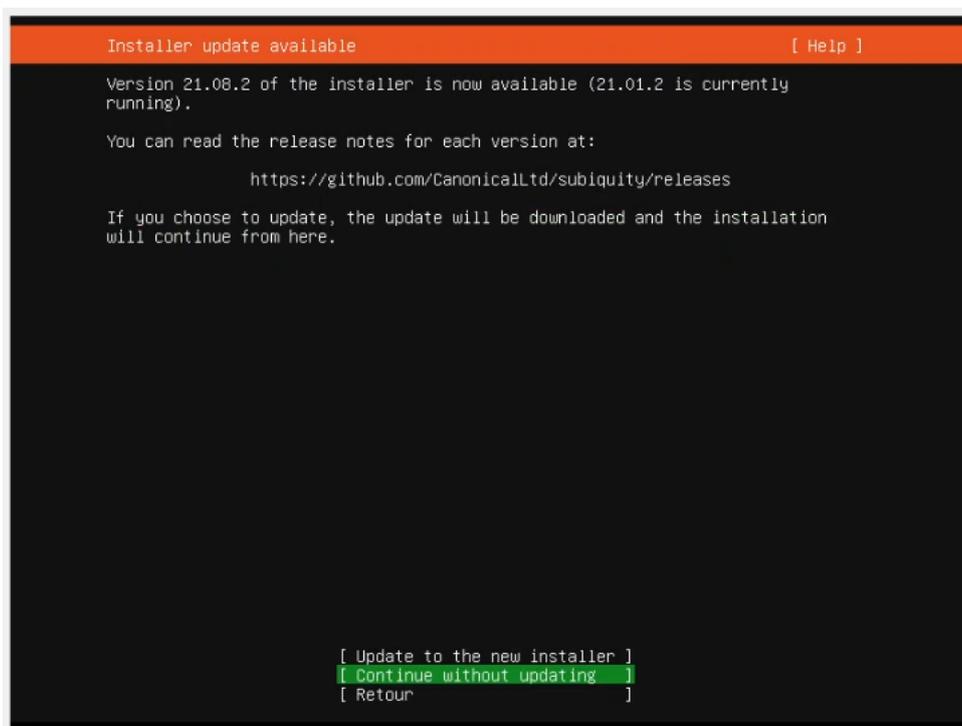
- Français



#### 3.1.2 Mise à jour de l'installateur

Selon la version de votre ISO il se peut que l'installateur ne soit pas le plus récent, il vous est possible de choisir un plus récent ou l'ignorer, dans notre cas nous allons ignorer, sélectionner :

- Continue without updating



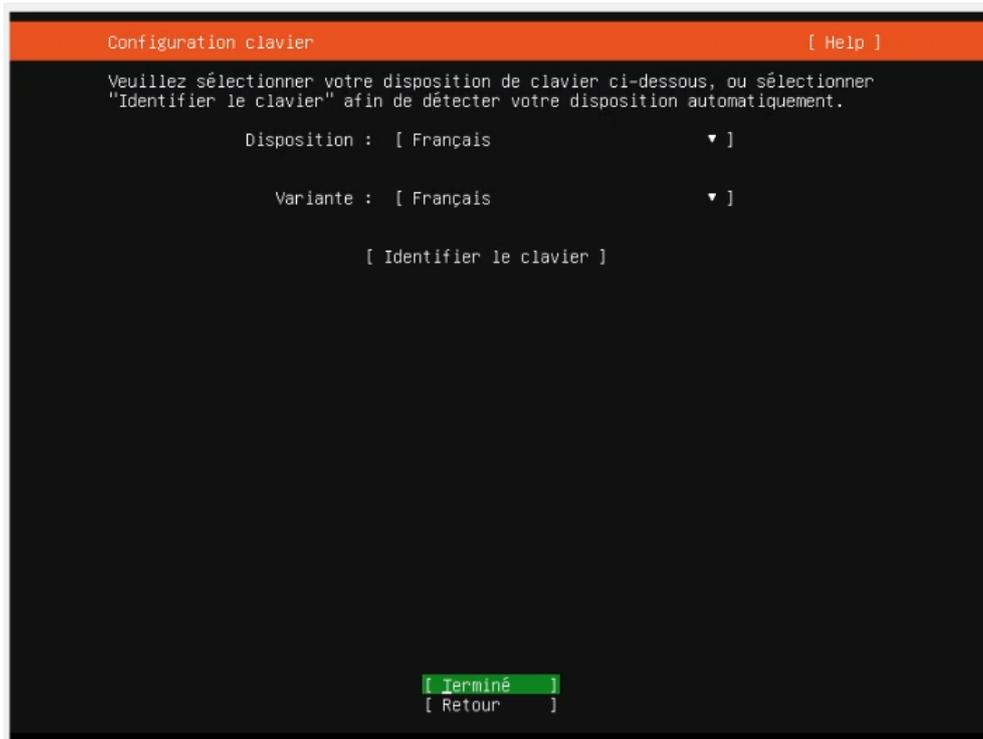
### 3.1.3 Configuration clavier

Normalement selon la langue choisie votre clavier devrait être sélectionné, sinon vous pouvez choisir le clavier souhaité en sélectionnant et parcourant les paramètres :

- Dispositif
- Variante

Lorsque vous avez terminé sélectionner :

- Terminé

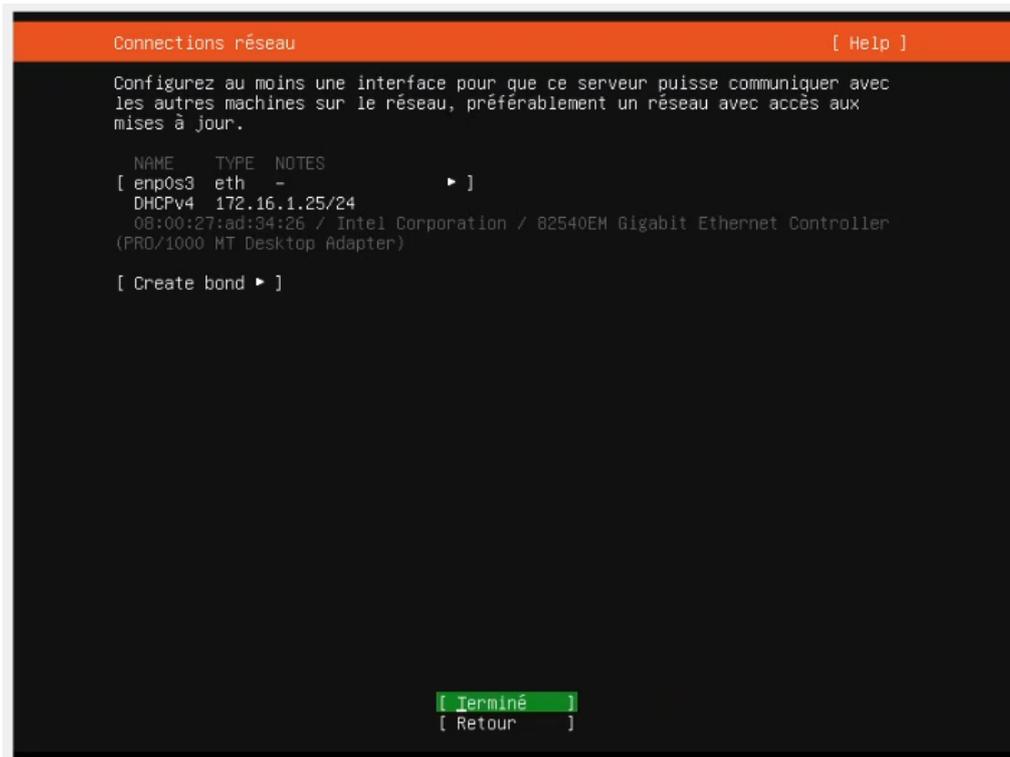


### 3.1.4 Connexions réseau

Par défaut la carte réseau est détectée et une configuration réseau est distribuée par votre serveur DHCP, si vous souhaitez avoir une configuration statique c'est à ce niveau-là que vous pouvez modifier ce paramètre.

Lorsque la configuration vous convient, sélectionner :

- Terminé



```
Connexions réseau [ Help ]

Configurez au moins une interface pour que ce serveur puisse communiquer avec
les autres machines sur le réseau, préférablement un réseau avec accès aux
mises à jour.

NAME    TYPE  NOTES
[ enp0s3 eth -          ► ]
DHCIPv4 172.16.1.25/24
08:00:27:ad:34:26 / Intel Corporation / 82540EM Gigabit Ethernet Controller
(PRO/1000 MT Desktop Adapter)

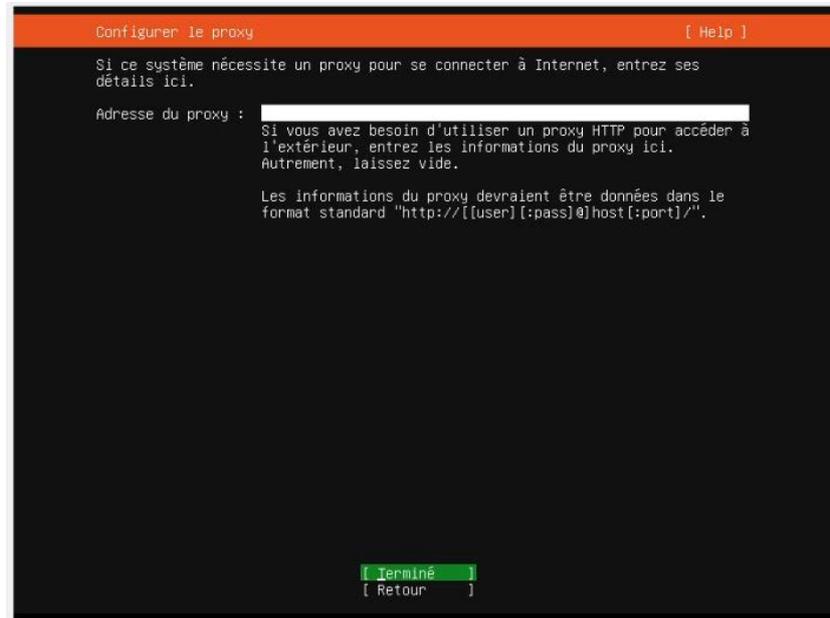
[ Create bond ► ]

[ Terminé ]
[ Retour   ]
```

### 3.1.5 Configurer le proxy

Si vous utilisez un proxy pour vous connecter à internet vous pouvez le spécifier à cet endroit et sélectionner :

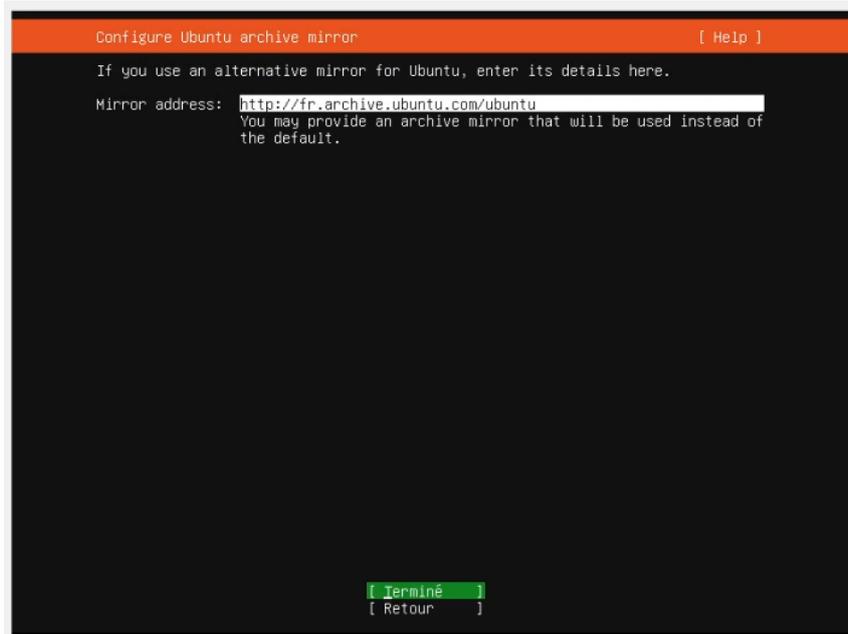
- Terminé



### 3.1.6 Configuration du serveur miroir

Pour ce qui va être des mises à jours et installation des paquets si vous souhaitez les récupérer depuis des serveurs spécifiques vous pouvez indiquer à cette étape le serveur de récupération ou laisser le paramètre par défaut et sélectionner :

- Terminé



### 3.1.7 Configuration guidée du stockage

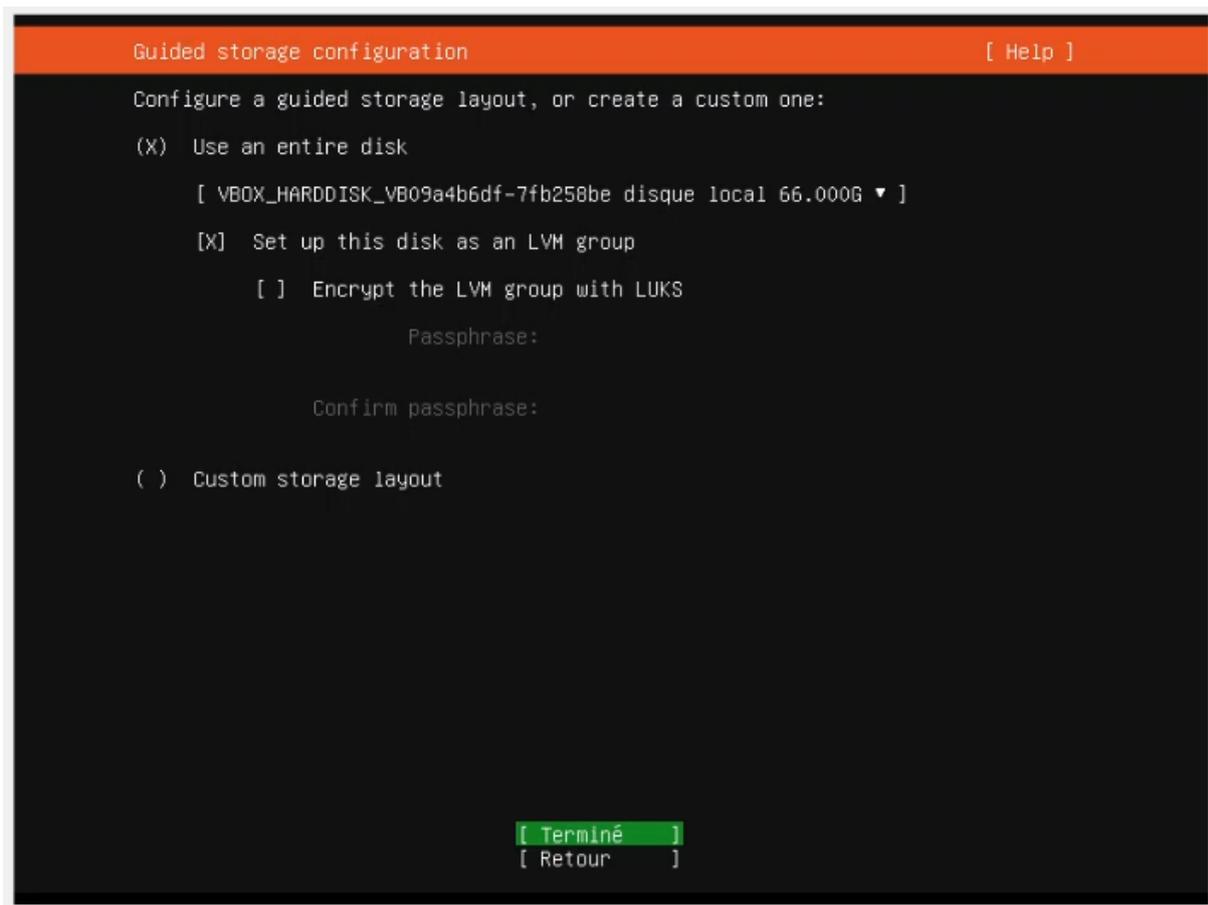
Vous pouvez configurer le partitionnement selon vos préférences, dans notre cas pour des besoins de démonstrations nous n'avons pas chiffrer le disque mais puisque les données contenues peuvent être de nature confidentielle je vous recommande de le chiffrer.

Vous pouvez également partitionner plus finement le disque pour par exemple séparer les partitions qui contiennent des données utilisateurs et d'autres qui contiennent que les données des différents services.

Quel que soit votre choix il faut veiller à ce qu'il y ait suffisamment d'espace disque pour stocker les données.

Dans notre cas nous allons utiliser l'option par défaut et sélectionner :

- Terminé



### 3.1.8 Configuration du stockage

Le système se charge de créer les différentes partitions pour confirmer sélectionner :

- Terminé

```
Storage configuration [ Help ]

SOMMAIRE DU SYSTÈME DE FICHIERS

  POINT DE MONTAGE  TAILLE  TYPE  TYPE DE PÉRIPHÉRIQUE
[ /                32.498G new ext4 new LVM logical volume ▶ ]
[ /boot           1.000G new ext4 new partition of disque local ▶ ]

DISQUES DISPONIBLES

  PÉRIPHÉRIQUE  TYPE  TAILLE
[ ubuntu-vg (new)  LVM volume group  64.996G ▶ ]
  espace libre  32.498G

[ Create software RAID (md) ▶ ]
[ Create volume group (LVM) ▶ ]

USED DEVICES

  PÉRIPHÉRIQUE  TYPE  TAILLE
[ ubuntu-vg (new)  LVM volume group  64.996G ▶ ]
  ubuntu-lv      new, to be formatted as ext4, mounted at /  32.498G ▶ ]

[ VBOX_HARDDISK_VB09a4b6df-7fb258be  disque local  66.000G ▶ ]
  partition 1  new, bios_grub  1.000M ▶ ]
  partition 2  new, to be formatted as ext4, mounted at /boot  1.000G ▶ ]
  partition 3  new, PV of LVM volume group ubuntu-vg  64.997G ▶ ]

[ Terminé ]
[ Rétablir ]
[ Retour ]
```

### 3.1.9 Confirmer l'action

Puisque le partitionnement va formater le disque, pour des raisons de sécurité une confirmation nous ait demandée, sélectionner :

- Continuer

```
Confirming l'action

Selecting Continue below will begin the installation process and
result in the loss of data on the disks selected to be formatted.

You will not be able to return to this or a previous screen once the
installation has started.

Are you sure you want to continue?

[ Non ]
[ Continuer ]
```

### 3.1.10 Configuration du profil

Vous êtes invités à créer un compte utilisateur, il faut spécifier les champs suivants

- Votre nom :
  - Le nom complet de l'utilisateur
- Le nom de cette machine :
  - Par le nom qui sera affiché sur le poste et par lequel il sera identifié sur le réseau
- Choisir un nom d'utilisateur :
  - Un nom ou un pseudonyme que l'utilisateur va utiliser pour se connecter sur le poste
- Choisir un mot de passe :
  - Un mot de passe d'au moins 16 caractères composé de chiffres, lettres et symboles
  - Il est recommandé d'utiliser un mot de passe complexe, et non comme c'est le cas ci-dessous où il n'est composé que de 4 caractères
- Confirmer votre mot de passe :
  - Saisir à nouveau le mot de passe pour s'assurer que vous ne vous êtes pas trompé

Lorsque les champs sont renseignés, sélectionner :

- Terminé

The screenshot shows a terminal window titled "Configuration du profil" with a "[ Help ]" link in the top right corner. The terminal text reads: "Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo." Below this, there are five input fields with labels and their respective values: "Votre nom : mudpak", "Le nom de cette machine: opencti" (with a sub-label "Le nom qu'il utilise pour communiquer avec d'autres ordinateurs."), "Choisir un nom d'utilisateur : mudpak", "Choisir un mot de passe : \*\*\*\*", and "Confirmer votre mot de passe: \*\*\*\*". At the bottom center, there is a green button labeled "[ Terminé ]".

### 3.1.11 SSH Setup

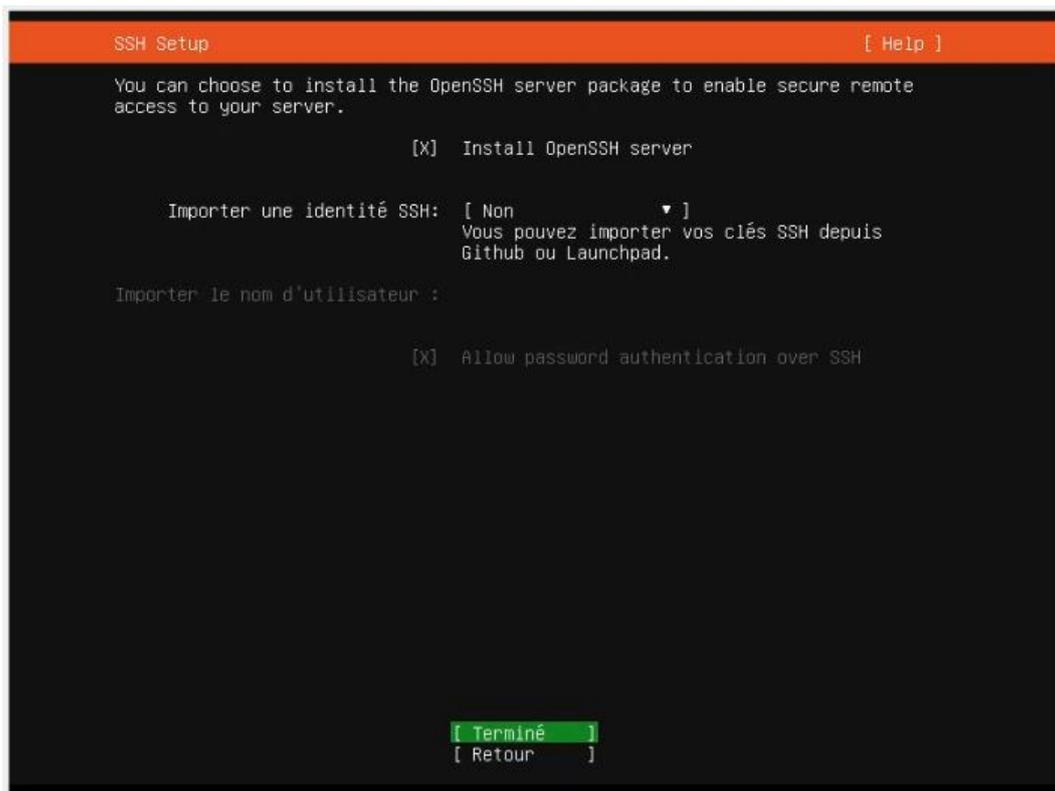
Pour des raisons de simplicité et d'administration je vous recommande fortement l'installation du serveur SSH qui vous permettra par la suite d'administrer le serveur à distance.

Sélectionner :

- Install OpenSSH server

Sélectionner :

- Terminé



### 3.1.12 Featured Server Snaps

Vous pouvez installer d'autres packages si vous le souhaitez, pour l'instant je vous recommande de ne rien sélectionner d'autres et sélectionner :

- Terminé

```
Featured Server Snaps [ Help ]

These are popular snaps in server environments. Select or deselect with SPACE,
press ENTER to see more details of the package, publisher and versions
available.

[ ] microk8s           Kubernetes for workstations and appliances ▶
[ ] nextcloud         Nextcloud Server - A safe home for all your data ▶
[ ] wekan             The open-source kanban ▶
[ ] kata-containers  Build lightweight VMs that seamlessly plug into the c ▶
[ ] docker            Docker container runtime ▶
[ ] canonical-livepatch Canonical Livepatch Client ▶
[ ] rocketchat-server Rocket.Chat server ▶
[ ] mosquito         Eclipse Mosquitto MQTT broker ▶
[ ] etcd             Resilient key-value store by CoreOS ▶
[ ] powershell      PowerShell for every system! ▶
[ ] stress-ng        tool to load and stress a computer ▶
[ ] sabnzbd          SABnzbd ▶
[ ] wormhole         get things from one computer to another, safely ▶
[ ] aws-cli          Universal Command Line Interface for Amazon Web Servi ▶
[ ] google-cloud-sdk Google Cloud SDK ▶
[ ] sicli            Python based SoftLayer API Tool. ▶
[ ] doctl            The official DigitalOcean command line interface ▶
[ ] conjure-up       Package runtime for conjure-up spells ▶
[ ] postgresql10    PostgreSQL is a powerful, open source object-relatio ▶
[ ] heroku           CLI client for Heroku ▶
[ ] keepalived       High availability VRRP/BFD and load-balancing for Lin ▶
[ ] prometheus       The Prometheus monitoring system and time series data ▶
[ ] juju             Juju - a model-driven operator lifecycle manager for ▶

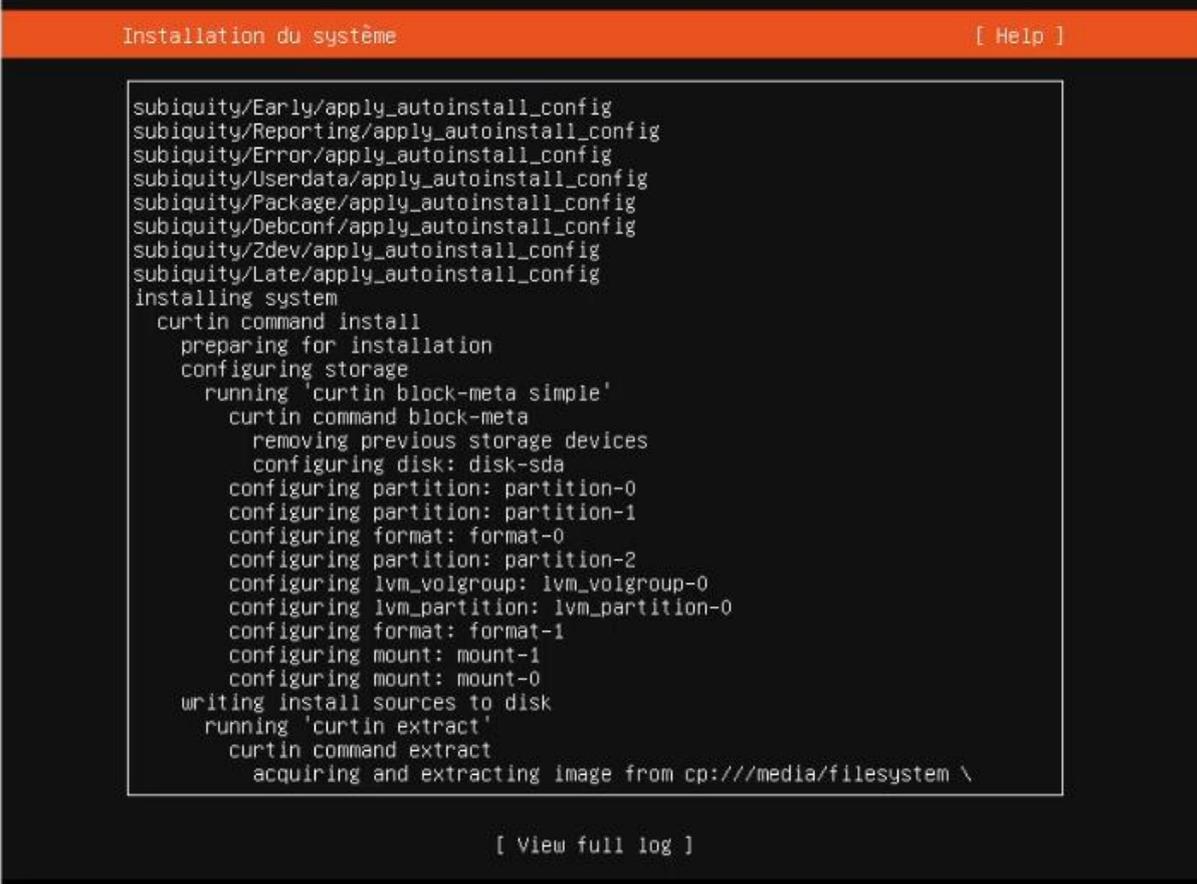
[ Terminé ]
[ Retour ]
```

### 3.1.13 Installation du système

L'installation du système d'exploitation commence, elle va prendre un certain temps.

Vous pouvez suivre l'installation en détails en sélectionnant :

- [View full log](#)



```
Installation du système [ Help ]
subiquity/Early/apply_autoinstall_config
subiquity/Reporting/apply_autoinstall_config
subiquity/Error/apply_autoinstall_config
subiquity/Userdata/apply_autoinstall_config
subiquity/Package/apply_autoinstall_config
subiquity/Debconf/apply_autoinstall_config
subiquity/Zdev/apply_autoinstall_config
subiquity/Late/apply_autoinstall_config
installing system
  curtin command install
  preparing for installation
  configuring storage
    running 'curtin block-meta simple'
    curtin command block-meta
      removing previous storage devices
      configuring disk: disk-sda
      configuring partition: partition-0
      configuring partition: partition-1
      configuring format: format-0
      configuring partition: partition-2
      configuring lvm_volgroup: lvm_volgroup-0
      configuring lvm_partition: lvm_partition-0
      configuring format: format-1
      configuring mount: mount-1
      configuring mount: mount-0
  writing install sources to disk
    running 'curtin extract'
    curtin command extract
      acquiring and extracting image from cp:///media/filesystem \

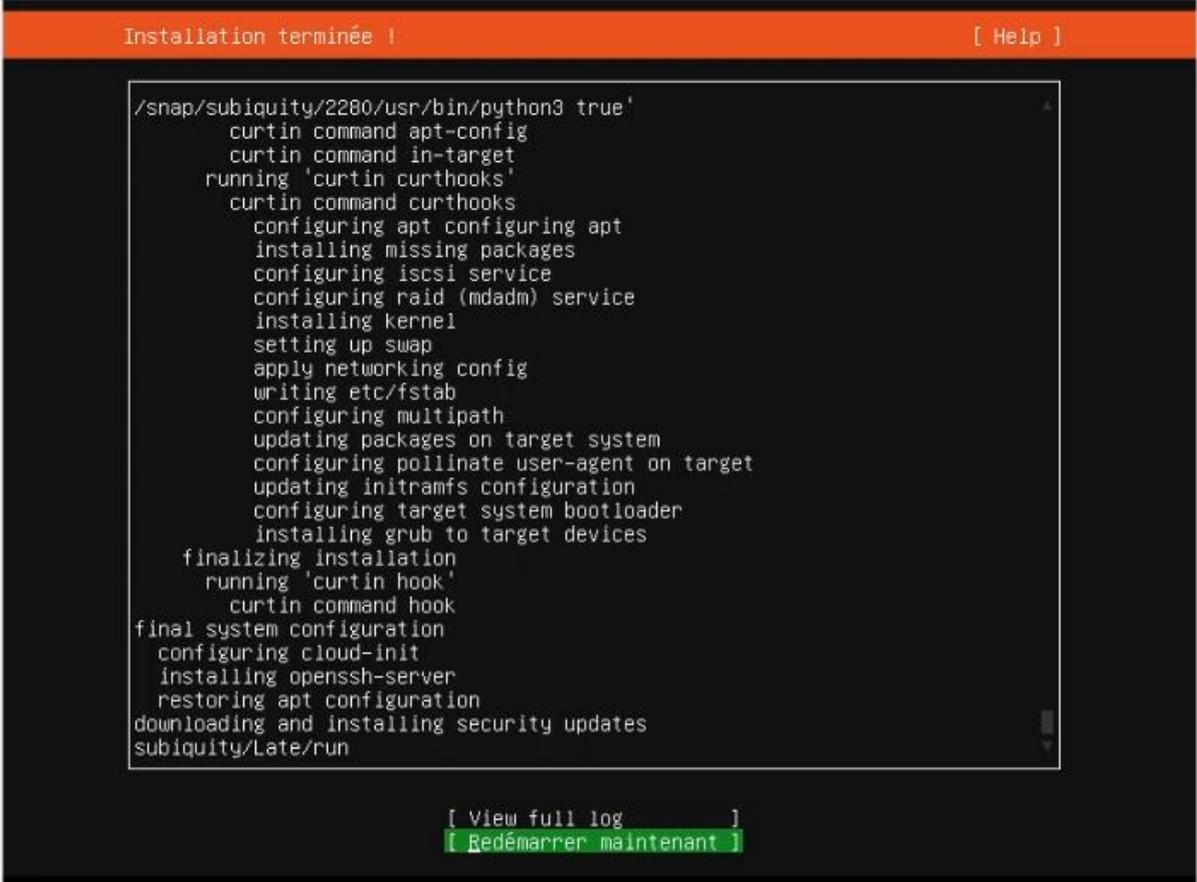
[ View full log ]
```

### 3.1.14 Installation terminée !

Lorsque l'installation est terminée vous en êtes informé, il faut redémarrer le système pour cela sélectionner :

- Redémarrer maintenant

Remarque : Il vous sera demandé de retirer le média d'installation pour que le redémarrage puisse s'effectuer.



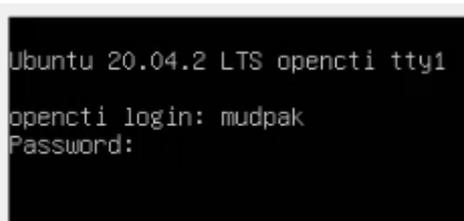
```
Installation terminée ! [ Help ]

/snap/subiquity/2280/usr/bin/python3 true'
curtin command apt-config
curtin command in-target
running 'curtin curthooks'
curtin command curthooks
configuring apt configuring apt
installing missing packages
configuring iscsi service
configuring raid (mdadm) service
installing kernel
setting up swap
apply networking config
writing etc/fstab
configuring multipath
updating packages on target system
configuring pollinate user-agent on target
updating initramfs configuration
configuring target system bootloader
installing grub to target devices
finalizing installation
running 'curtin hook'
curtin command hook
final system configuration
configuring cloud-init
installing openssh-server
restoring apt configuration
downloading and installing security updates
subiquity/Late/run

[ View full log ]
[ Redémarrer maintenant ]
```

### 3.1.15 Première connexion

Lorsque le redémarrage est terminé, vous pouvez vous connecter sur le poste avec le compte précédemment crée :



```
Ubuntu 20.04.2 LTS opencti tty1
opencti login: mudpak
Password:
```

### 3.1.16 Configuration IP

Puisque nous avons choisi l'installation du serveur SSH pour administrer la machine à distance, il nous faut son adresse IP, pour l'obtenir saisir la commande :

- ip a

Détails de la commande :

- ip : programme auquel on fait appel
- a : paramètre qui permet d'obtenir l'adresse IP de la machine

Dans le cas présent notre machine à l'adresse IP « 172.16.1.25 », ainsi pour la suite je peux me connecter en utilisant mon compte et administrer la machine.

```
mudpak@opencti:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:34:26 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.25/24 brd 172.16.1.255 scope global dynamic enp0s3
        valid_lft 7138sec preferred_lft 7138sec
    inet6 fe80::a00:27ff:fead:3426/64 scope link
        valid_lft forever preferred_lft forever
```

### 3.2 Connexion SSH

Pour les opérations d'administration du serveur le protocole SSH (Secure SHell) sera utilisé, nous allons utiliser la commande suivante pour nous connecter :

- `ssh mudpak@172.16.1.25`

Détails de la commande :

- `ssh` : programme auquel on fais appel, ici on parle de `ssh-client`
- `mudpak` : le compte utilisateur qui sera utilisé pour se connecter
- `@172.16.1.25` : ajout du paramètre pour définir l'adresse IP de l'hôte distant sur lequel nous souhaitons nous connecter

```
PS C:\Users\mudpak> ssh mudpak@172.16.1.25
```

Puisque c'est la première fois que nous nous connectons au poste distant, pour des raisons de sécurité nous devons confirmer que c'est un l'hôte souhaité en vérifiant son identité (= que l'empreinte numérique est bien celle de la machine).

Saisir

- « Yes »

Et appuyer sur la touche

- « Entrée »

```
The authenticity of host '172.16.1.25 (172.16.1.25)' can't be established.  
ECDSA key fingerprint is SHA256:mr2[REDACTED]N2g.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '172.16.1.25' (ECDSA) to the list of known hosts.
```

Vous êtes invité à saisir le mot de passe du compte utilisateur, saisir le mot de passe et appuyer sur la touche

- « Entrée »

Remarque : si vous ne voyez pas le mot de passe que vous avez saisi c'est tout à fait normal, il s'agit d'une mesure de sécurité sous Linux.

```
mudpak@172.16.1.25's password:
```

Lorsque l'authentification s'effectue avec succès vous devez obtenir un résultat similaire à ci-dessous :

```
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-89-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information disabled due to load higher than 1.0

96 updates can be installed immediately.
1 of these updates is a security update.
To see these additional updates run: apt list --upgradable

Last login: Mon Nov  1 15:07:17 2021
```

Le système nous informe que 96 mises à jour peuvent être installées dont 1 concernant la sécurité de celui-ci.

```
96 updates can be installed immediately.
1 of these updates is a security update.
To see these additional updates run: apt list --upgradable
```

### 3.3 Mise à jour de la liste des paquets

Maintenant que le système d'exploitation est installé et que nous sommes connectés à la machine, il faut en premier lieu procéder à la mise à jour.

Saisir la commande suivante :

- `sudo apt update -y`

Détails de la commande :

- `sudo` : pour exécuter avec les privilèges élevés
- `apt` : programme à utiliser
- `update` : paramètre spécifié, dans le cas présent on demande la mise à jour des paquets
- `-y` : accepter la mise à jour des paquets sans demander la confirmation
  - Cela peut aussi être une mauvaise pratique si vous voulez absolument savoir quels paquets seront installés, supprimés donc à utiliser avec précaution

```
mudpak@CTI:~$ sudo apt update -y
```

Selon la vitesse de votre connexion internet ce processus peut prendre un certain temps.

Dans le cas présent il n'a pas duré longtemps et nous sommes invités à utiliser la commande

- `apt list --upgradable`

Pour afficher la liste des paquets qui peuvent être mis à jour.

```
[sudo] password for mudpak:
Hit:1 http://fr.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://fr.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://fr.archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Get:4 http://fr.archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Fetched 328 kB in 1s (301 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
79 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

### 3.4 Installation des nouveaux paquets

Pour mettre à jour les paquets saisir la commande suivante :

- `sudo apt upgrade -y`

```
mudpak@CTI:~$ sudo apt upgrade -y
```

La liste des paquets qui sera mise à jour et en quelle version s'affiche et la mise à jour commence sans nous demander la confirmation puisque nous avons spécifié le paramètre « -y » :

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  distro-info libatasmart4 libblockdev-cryptoz libblockdev-fs2 libblockdev-loop2 libblockdev-part-err2 libblockdev-part2 libblockdev-swap2 libblockdev-utils2 libblockdev2 libjcat1 libnspr4 libnss3
  libparted-fs-resize0 libudisks2-0 libvolume-key1 udisks2
The following packages will be upgraded:
  alsa-ucm-conf apt apt-utils base-files cloud-init dirnmg friendly-recovery fwupd fwupd-signed gnupg gnupg-l10n gnupg-utils gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf gpgme gpgv initscripts-tools
  initscripts-tools-bin initscripts-tools-core landscape-common libapt-pkg6.0 libasound2 libasound2-data libdrm-common libdrm2 libfwupd2 libfwupdplugin1 libgl1.0-0 libgl1.0-bin libgl1.0-data libldap-2.4-2
  libldap-common libnetplan libnss-systemd libpam-modules libpam-modules-bin libpam-runtime libpam-systemd libpam0g libpc3 libpcreps libseccomp2 libsystemd0 libudev1 libxmlb linux-base login
  motd-news-config netplan.io networkd-dispatcher open-iscsi open-vm-tools passwd pciutils pollinate procs python-apt-common python3-apt python3-distupgrade python3-software-properties python3-twisted
  python3-twisted-bin python3-update-manager snapd software-properties-common sosreport systemd-sysv systemd-timesyncd tmux ubuntu-advantage-tools ubuntu-keyring ubuntu-release-upgrader-core udev
  update-manager-core update-notifier-common
79 upgraded, 17 newly installed, 0 to remove and 0 not upgraded.
Need to get 54,7 MB of archives.
After this operation, 19,0 MB of additional disk space will be used.
```

Selon votre connexion internet et le nombre de paquets à mettre à jour ce processus peut prendre un certain temps :

```
Get:1 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 motd-news-config all 11ubuntu5.4 [4544 B]
Get:2 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 base-files amd64 11ubuntu5.4 [60.6 kB]
Get:3 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 login amd64 1:4.8.1-1ubuntu5.20.04.1 [220 kB]
Get:4 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 libnss-systemd amd64 245.4-4ubuntu3.13 [95.8 kB]
Get:5 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 udev amd64 245.4-4ubuntu3.13 [1365 kB]
Get:6 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 libudev1 amd64 245.4-4ubuntu3.13 [77.6 kB]
Get:7 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 systemd-sysv amd64 245.4-4ubuntu3.13 [10.3 kB]
Get:8 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 systemd-timesyncd amd64 245.4-4ubuntu3.13 [28.1 kB]
Get:9 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 libpam0g amd64 1.3.1-5ubuntu4.3 [55.4 kB]
Get:10 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 libpam-modules-bin amd64 1.3.1-5ubuntu4.3 [41.2 kB]
Get:11 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 libpam-modules amd64 1.3.1-5ubuntu4.3 [260 kB]
Get:12 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 libpam-runtime all 1.3.1-5ubuntu4.3 [37.3 kB]
Get:13 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 libpam-systemd amd64 245.4-4ubuntu3.13 [186 kB]
Get:14 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 libseccomp2 amd64 2.5.1-1ubuntu1~20.04.1 [42.9 kB]
Get:15 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 systemd amd64 245.4-4ubuntu3.13 [3809 kB]
Get:16 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 libsystemd0 amd64 245.4-4ubuntu3.13 [270 kB]
Get:17 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 libapt-pkg6.0 amd64 2.0.6 [835 kB]
Get:18 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 apt amd64 2.0.6 [1296 kB]
Get:19 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 apt-utils amd64 2.0.6 [216 kB]
Get:20 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 gpg-wks-client amd64 2.2.19-3ubuntu2.1 [97.6 kB]
Get:21 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 dirnmg amd64 2.2.19-3ubuntu2.1 [329 kB]
Get:22 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 gnupg-utils amd64 2.2.19-3ubuntu2.1 [480 kB]
Get:23 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 gpg-wks-server amd64 2.2.19-3ubuntu2.1 [90.3 kB]
Get:24 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 gpg-agent amd64 2.2.19-3ubuntu2.1 [232 kB]
```

Ci-dessous nous pouvons voir un exemple de ce qui est fait lors de cette phase tel que :

- Installation de la nouvelle version des paquets
- Mise à jour des fichiers de configuration
- ...

```
update-initramfs: deferring update (trigger activated)
Setting up gpg-wks-client (2.2.19-3ubuntu2.1) ...
Setting up software-properties-common (0.98.9.5) ...
Setting up libvolume-key1 (0.3.12-3.1) ...
Setting up libblockdev-crypto2:amd64 (2.23-2ubuntu3) ...
Setting up systemd (245.4-4ubuntu3.13) ...
Installing new version of config file /etc/dhcp/dhclient-enter-hooks.d/resolved ...
Setting up python3-distupgrade (1:20.04.36) ...
Setting up netplan.io (0.103-0ubuntu5~20.04.2) ...
Setting up systemd-timesyncd (245.4-4ubuntu3.13) ...
Setting up ubuntu-release-upgrader-core (1:20.04.36) ...
Setting up python3-update-manager (1:20.04.10.9) ...
Setting up snapd (2.51.1+20.04ubuntu2) ...
Installing new version of config file /etc/apparmor.d/usr.lib.snapd.snap-confine.real ...
Installing new version of config file /etc/profile.d/apps-bin-path.sh ...
snapd.failure.service is a disabled or a static unit, not starting it.
snapd.snap-repair.service is a disabled or a static unit, not starting it.
Setting up systemd-sysv (245.4-4ubuntu3.13) ...
Setting up cloud-init (21.3-1-g6803368d-0ubuntu1~20.04.4) ...
Installing new version of config file /etc/cloud/cloud.cfg ...
Installing new version of config file /etc/cloud/templates/chef_client.rb.tpl ...
Installing new version of config file /etc/cloud/templates/resolv.conf.tpl ...
```

Les changements de versions de certains paquets requièrent un redémarrage du système, pour faire cela saisir la commande suivante :

- `sudo reboot`

```
mudpak@CTI:~$ sudo reboot
```

## 4. Docker

Maintenant que notre système est à jour nous allons pouvoir commencer l'installation de docker.

### 4.1 Passage en mode « root »

L'installation de docker doit s'effectuer en mode « root », saisir la commande suivante :

- `sudo -i`

Détails de la commande :

- `sudo` : pour passer en mode « SUPER user » ou « SU » et « DO » (=passe en mode super user)
- `-i` : paramètre qui demande le chargement de l'environnement root

Remarque : vous ne pourrez exécuter cette commande que si vous êtes membre du groupe « sudo ».

```
mudpak@CTI:~$ sudo -i
```

Nous devons saisir le mot de passe du compte utilisateur :

```
[sudo] password for mudpak:
```

### 4.2 Récupération du script

Pour installer docker, il existe différentes méthodes.

Dans le cas présent nous allons utiliser le script présent sur leur site, l'avantage est qu'avec cette méthode la version la plus récente et la plus adaptée à notre architecture sera fait automatiquement !

Saisir la commande suivante :

- `curl -fsSL https://get.docker.com -o get-docker.sh`

Détails de la commande :

- `curl` : utilitaire utilisé pour récupérer le script
- `-fsSL` : paramètres à appliquer
  - `f` : pour « -- form »
  - `s` : pour « -- silent »
  - `S` : pour « -- show-error »
  - `L` : pour « -- location »
- `https://get.docker.com` : adresse où se trouve le script à récupérer
- `-o` : paramètre pour spécifier un nom de sortie du fichier
- `get-docker.sh` : nom du fichier récupéré

```
root@CTI:~# curl -fsSL https://get.docker.com -o get-docker.sh
```

Pour vérifier que nous avons bien récupéré le script, saisir la commande suivante :

- `ls -al | grep "get-docker.sh"`

Détails de la commande :

- `ls -al` : pour afficher les fichiers et dossiers même cachés
- `|` : pour envoyer le résultat de la commande précédente vers la commande suivante
- `grep` : effectuer un tri sur un critère défini
- `"get-docker.sh"` : le critère défini

Nous pouvons voir ci-dessous que le script à bien été récupéré le 1<sup>er</sup> Novembre :

```
root@CTI:~# ls -al | grep "get-docker.sh"
-rw-r--r--  1 root root 18617 Nov  1 15:18 get-docker.sh
```

### 4.3 Exécution du script

Pour exécuter le script d'installation, saisir la commande suivante :

- `sh get-docker.sh`

Détails de la commande :

- `sh` : commande équivalente à « `./nom-du-script.sh` »
- `get-docker.sh` : script à exécuter

```
root@CTI:~# sh get-docker.sh
```

### 4.4 Installation

L'installation commence et elle peut prendre un certain temps :

```
# Executing docker install script, commit: 93d2499759296ac1f9c510605fef85052a2c32be
+ sh -c apt-get update -qq >/dev/null
+ sh -c DEBIAN_FRONTEND=noninteractive apt-get install -y -qq apt-transport-https ca-certificates curl >/dev/null
+ sh -c curl -fsSL "https://download.docker.com/linux/ubuntu/gpg" | gpg --dearmor --yes -o /usr/share/keyrings/docker-archive-keyring.gpg
+ sh -c echo "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu focal stable" > /etc/apt/sources.list.d/docker.list
+ sh -c apt-get update -qq >/dev/null
+ sh -c DEBIAN_FRONTEND=noninteractive apt-get install -y -qq --no-install-recommends docker-ce-cli docker-scanner-plugin docker-ce >/dev/null
+ version_gte 20.10
+ [ -z ]
+ return 0
+ sh -c DEBIAN_FRONTEND=noninteractive apt-get install -y -qq docker-ce-rootless-extras >/dev/null
+ sh -c docker version
```

Lorsque l'installation est terminée, voici un exemple de résultat qui s'affiche avec les informations suivantes :

- Client : Docker Engine – Community
- Server : Docker Engine – Community

En effet le script installe à la fois « docker server » et « docker client » en plus de cela c'est la version « Community » qui est installée car autrement il faut disposer de licences d'entreprise pour avoir d'autres fonctionnalités.

Pour nos besoins de démonstrations la version Community sera largement suffisante.

```
Client: Docker Engine - Community
Version: 20.10.10
API version: 1.41
Go version: go1.16.9
Git commit: b485636
Built: Mon Oct 25 07:42:59 2021
OS/Arch: linux/amd64
Context: default
Experimental: true

Server: Docker Engine - Community
Engine:
Version: 20.10.10
API version: 1.41 (minimum version 1.12)
Go version: go1.16.9
Git commit: e2f740d
Built: Mon Oct 25 07:41:08 2021
OS/Arch: linux/amd64
Experimental: false
containerd:
Version: 1.4.11
GitCommit: 5b46e404f6b9f661a205e28d59c982d3634148f8
runc:
Version: 1.0.2
GitCommit: v1.0.2-0-g52b36a2
docker-init:
Version: 0.19.0
GitCommit: de40ad0
```

Il est important de noter que l'installation de docker s'est effectuée via des droits « root » et pour des raisons de sécurité il est désormais possible d'exécuter docker en mode « rootless » :

```
=====
To run Docker as a non-privileged user, consider setting up the
Docker daemon in rootless mode for your user:

    dockerd-rootless-setuptool.sh install

Visit https://docs.docker.com/go/rootless/ to learn about rootless mode.

To run the Docker daemon as a fully privileged service, but granting non-root
users access, refer to https://docs.docker.com/go/daemon-access/

WARNING: Access to the remote API on a privileged Docker daemon is equivalent
to root access on the host. Refer to the 'Docker daemon attack surface'
documentation for details: https://docs.docker.com/go/attack-surface/
=====
```

#### 4.5 Ajout au groupe « docker »

Il est recommandé d'utiliser la méthode ci-dessus, mais pour des raisons de simplicité je préfère utiliser une méthode alternative.

Dans le cas présent je vais ajouter mon compte utilisateur « mudpak » au groupe « docker » afin que je puisse utiliser docker via mon « simple compte utilisateur ».

Saisir la commande suivante :

- `sudo usermod -aG docker mudpak`

Détails de la commande :

- `sudo usermod -aG docker mudpak`

```
mudpak@CTI:~$ sudo usermod -aG docker mudpak
```

#### 4.6 Vérification des changements

Nous pouvons exécuter la commande ci-dessous avec le compte « normal » pour être certain que les droits ont bien été attribués :

- `docker --version`

Détails de la commande :

- `docker` : programme à utiliser
- `--version` : paramètre pour afficher la version de docker

```
mudpak@CTI:~$ docker --version  
Docker version 20.10.10, build b485636
```

## 5. Docker-Compose – Part 1

Docker est installé, maintenant nous allons procéder à l'installation de docker-compose afin qu'il soit possible de faire de l'orchestration des containers de manière plus aisée.

### 5.1 Installation de docker-compose

Saisir la commande suivante pour commencer l'installation de docker-compose :

- `sudo apt-get install docker-compose`

```
pich@OpenCTI:~$ sudo apt-get install docker-compose
```

La liste des paquets qui seront installés est affichée et une confirmation est demandée avant de procéder à leur installation.

Saisir « Y » pour confirmer et appuyer sur la touche « Entrée » :

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  pigz python3-cached-property python3-docker python3-dockerpty python3-doccopt python3-texttable python3-websocket
Recommended packages:
  docker.io
The following NEW packages will be installed:
  docker-compose pigz python3-cached-property python3-docker python3-dockerpty python3-doccopt python3-texttable python3-websocket
0 upgraded, 8 newly installed, 0 to remove and 146 not upgraded.
Need to get 319 kB of archives.
After this operation, 1,875 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Le téléchargement et installation des paquets peut prendre un certain temps :

```
Get:1 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 pigz amd64 2.4-1 [57.4 kB]
Get:2 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 python3-cached-property all 1.5.1-4 [10.9 kB]
Get:3 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 python3-websocket all 0.53.0-2ubuntu1 [32.3 kB]
Get:4 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 python3-docker all 4.1.0-1 [83.8 kB]
Get:5 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 python3-dockerpty all 0.4.1-2 [11.1 kB]
Get:6 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 python3-doccopt all 0.6.2-2.2ubuntu1 [19.7 kB]
Get:7 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 python3-texttable all 1.6.2-2 [11.0 kB]
Get:8 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 docker-compose all 1.25.0-1 [92.7 kB]
Fetched 319 kB in 1s (360 kB/s)
Selecting previously unselected package pigz.
(Reading database ... 107608 files and directories currently installed.)
Preparing to unpack .../0-pigz_2.4-1_amd64.deb ...
Unpacking pigz (2.4-1) ...
Selecting previously unselected package python3-cached-property.
Preparing to unpack .../1-python3-cached-property_1.5.1-4_all.deb ...
Unpacking python3-cached-property (1.5.1-4) ...
Selecting previously unselected package python3-websocket.
Preparing to unpack .../2-python3-websocket_0.53.0-2ubuntu1_all.deb ...
Unpacking python3-websocket (0.53.0-2ubuntu1) ...
Selecting previously unselected package python3-docker.
Preparing to unpack .../3-python3-docker_4.1.0-1_all.deb ...
Unpacking python3-docker (4.1.0-1) ...
Selecting previously unselected package python3-dockerpty.
Preparing to unpack .../4-python3-dockerpty_0.4.1-2_all.deb ...
Unpacking python3-dockerpty (0.4.1-2) ...
Selecting previously unselected package python3-doccopt.
```

## 5.2 Vérification de la version

Lorsque l'installation est terminée, nous pouvons le vérifier par exemple en affichant la version installée en saisissant la commande suivante :

- `docker-compose --version`

```
pich@OpenCTI:~$ docker-compose --version
docker-compose version 1.25.0, build unknown
```

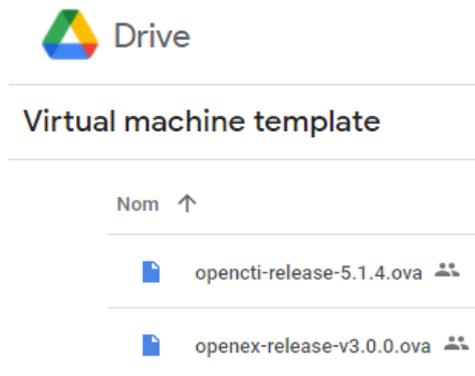
## 6. OpenCTI – Installation

Maintenant que le système est installé et mis à jour, docker et docker-compose sont installés nous avons différentes options pour la suite des opérations.

### 6.1 Via l'image virtuelle

OpenCTI fournit une image virtuelle toute prête à l'usage, il suffit de la télécharger depuis l'adresse suivante et l'utiliser avec VirtualBox :

- [https://drive.google.com/drive/folders/1bvB6RmdQNHMW\\_3h-88KbAit9GRZIL5Bj](https://drive.google.com/drive/folders/1bvB6RmdQNHMW_3h-88KbAit9GRZIL5Bj)



Remarque : il faudra penser à configurer certains éléments, mais c'est la solution la plus rapide pour avoir une plateforme OpenCTI fonctionnelle.

### 6.2 Via Terraform

Vous pouvez installer la solution via Terraform, pour cela je vous invite à vous référer à la documentation à la page suivante :

- <https://github.com/newcontext-oss/opencti-terraform>

## 6.3 Manuelle

Si vous souhaitez installer tous les composants de la plateforme manuellement et tout configurer il est tout à fait possible !

OpenCTI Public Knowle... / Installation and upgrade / Manual deployment



# Manual deployment

## Prerequisites

### Dependencies

Component	Version	Link
NodeJS	≥ 16	<a href="https://nodejs.org/en/download">https://nodejs.org/en/download</a>
Python	≥ 3.9	<a href="https://www.python.org/downloads">https://www.python.org/downloads</a>
ElasticSearch or OpenSearch	≥ 7.17 (ElasticSearch) or ≥ 7.10 (OpenSearch)	<a href="https://www.elastic.co/downloads/elasticsearch">https://www.elastic.co/downloads/elasticsearch</a>
MinIO	≥ RELEASE.2021-03-*	<a href="https://min.io/download">https://min.io/download</a>
Redis	≥ 6.2.* && < 7.0	<a href="https://redis.io/download">https://redis.io/download</a>
RabbitMQ	≥ 3.8 && < 3.9	<a href="https://www.rabbitmq.com/download.html">https://www.rabbitmq.com/download.html</a>
RabbitMQ Management plugin	≥ 3.8 && < 3.9	<a href="https://www.rabbitmq.com/management.html">https://www.rabbitmq.com/management.html</a>

Pour faire cela je vous invite à consulter la documentation officielle :

- <https://www.notion.so/Manual-deployment-b911beba44234f179841582ab3894bb1#45c57896db064780b5f893a10340a0f0>

## 6.4 Via Docker

Et enfin la méthode que nous allons utiliser pour l'installation de la plateforme se fera via Docker.

### 6.4.1 Création du répertoire

Il est recommandé de créer un répertoire dédié à OpenCTI, en effet dans les prochaines étapes nous allons le peupler avec des fichiers et dossiers ainsi il sera plus simple de s'y retrouver.

Saisir la commande suivante pour créer un dossier :

- `mkdir opencti`

Détails de la commande :

- `mkdir` : commande pour créer un répertoire
  - `mk` : pour MaKe
  - `dir` : pour DIRectory
- `opencti` : le nom du répertoire qui sera créé

```
pich@OpenCTI:~$ mkdir opencti
```

Pour nous déplacer dans le répertoire créé à l'étape précédente, nous allons utiliser la commande suivante :

- `cd opencti`

Détails de la commande :

- `cd` : pour changer de répertoire (=Change Directory)
- `opencti` : le répertoire dans lequel nous souhaitons nous déplacer

```
pich@OpenCTI:~$ cd opencti/
```

#### 6.4.2 Récupération du répertoire

Nous allons récupérer un répertoire depuis le GitHub officiel de la solution via la commande suivante :

- `git clone https://github.com/OpenCTI-Platform/docker.git`

Détails de la commande :

- `git` : programme à utiliser
- `clone` : paramètre pour créer une copie locale du répertoire cible
- `https://github.com/OpenCTI-Platform/docker.git` : adresse du répertoire cible

```
pich@OpenCTI:~/opencti$ git clone https://github.com/OpenCTI-Platform/docker.git
```

Ce qui aura pour conséquence la copie du répertoire distant dans un répertoire local nommé « docker » :

```
Cloning into 'docker'...
remote: Enumerating objects: 374, done.
remote: Counting objects: 100% (213/213), done.
remote: Compressing objects: 100% (95/95), done.
remote: Total 374 (delta 138), reused 188 (delta 115), pack-reused 161
Receiving objects: 100% (374/374), 60.58 KiB | 4.33 MiB/s, done.
Resolving deltas: 100% (233/233), done.
```

Puisque les documents copiés se trouvent dans un répertoire nommé « docker », il ne faut pas oublier de se déplacer dans le répertoire pour la suite des opérations :

```
pich@OpenCTI:~/opencti$ cd docker/
```

#### 6.4.3 Contenu du répertoire

Avant d'aller plus loin nous allons prendre le temps de regarder les éléments présents dans le répertoire et voir les fichiers qui seront essentiels pour la suite des évènements.

Saisir la commande suivante pour afficher tous les éléments présents dans le dossier :

- `ls -al`

```
pich@OpenCTI:~/opencti/docker$ ls -al
```

Nous pouvons voir qu'il y a au total 52 éléments dans le dossier et sous-dossiers mais les éléments qui nous intéressent sont présents ici :

```
pich@OpenCTI:~/opencti/docker$ ls -al
total 52
drwxrwxr-x 4 pich pich 4096 Jan 15 22:51 .
drwxrwxr-x 3 pich pich 4096 Jan 15 22:51 ..
-rw-rw-r-- 1 pich pich 1591 Jan 15 22:51 docker-compose-dev.yml
-rw-rw-r-- 1 pich pich 6231 Jan 15 22:51 docker-compose.yml
-rw-rw-r-- 1 pich pich  471 Jan 15 22:51 .env.sample
drwxrwxr-x 8 pich pich 4096 Jan 15 22:51 .git
drwxrwxr-x 2 pich pich 4096 Jan 15 22:51 .github
-rw-rw-r-- 1 pich pich  11 Jan 15 22:51 .gitignore
-rw-rw-r-- 1 pich pich 1478 Jan 15 22:51 init.py
-rw-rw-r-- 1 pich pich 6601 Jan 15 22:51 README.md
-rw-rw-r-- 1 pich pich  36 Jan 15 22:51 requirements.txt
```

Voici les deux fichiers essentiels pour la suite :

- « .env.sample » :
  - Nous allons copier ce fichier pour créer un fichier qui corresponde à notre configuration souhaitée.
  - Ce fichier contiendra les éléments sensibles tels que les informations de connexion à la plateforme, les clés API des connecteurs
- « docker-compose.yml » :
  - Ce fichier contient déjà des éléments mais nous allons pouvoir par exemple ajouter des éléments tels que des connecteurs pour alimenter la plateforme.

Remarque : pour des raisons de sécurité il est fortement déconseillé de mettre des éléments sensibles dans le fichier « docker-compose.yml » et à la place utiliser des variables dont la valeur sera stockée dans le fichier « .env ».

#### 6.4.4 .env

Nous allons copier le fichier « .env.sample » pour le personnaliser avec notre configuration souhaitée, pour cela saisir la commande suivante :

- `cp .env.sample .env`

Détails de la commande :

- `cp` : commander pour copier un élément (=CoPy)
- `.env.sample` : le nom du fichier à copier
- `.env` : le nom du fichier de destination

Remarque : la présence du symbole point « . » devant un fichier sous Linux signifie que ce fichier est par défaut caché.

```
pich@OpenCTI:~/opencti/docker$ cp .env.sample .env
```

Nous pouvons désormais utiliser un éditeur de texte pour modifier le fichier et insérer le contenu qu'on souhaite, saisir la commande suivante :

- nano .env

Détails de la commande :

- nano : éditeur de texte à utiliser
- .env : fichier à modifier

```
pich@OpenCTI:~/opencti/docker$ nano .env
```

Voici les champs qui doivent au minimum être complétés pour passer à l'étape suivante :

```
OPENCTI_ADMIN_EMAIL=admin@opencti.io # Valid email address
OPENCTI_ADMIN_PASSWORD=ChangeMe # String
OPENCTI_ADMIN_TOKEN=ChangeMe # Valid UUIDv4
MINIO_ROOT_USER=ChangeMeAccess # String
MINIO_ROOT_PASSWORD=ChangeMeKey # String
RABBITMQ_DEFAULT_USER=guest # String
RABBITMQ_DEFAULT_PASS=guest # String
CONNECTOR_HISTORY_ID=ChangeMe # Valid UUIDv4
CONNECTOR_EXPORT_FILE_STIX_ID=ChangeMe # Valid UUIDv4
CONNECTOR_EXPORT_FILE_CSV_ID=ChangeMe # Valid UUIDv4
CONNECTOR_IMPORT_FILE_STIX_ID=ChangeMe # Valid UUIDv4
CONNECTOR_IMPORT_FILE_PDF_OBSERVABLES_ID=ChangeMe # Valid UUIDv4
```

Important :

- Dans les bonnes pratiques OpenCTI, il est recommandé que chaque connecteur ait un identifiant UUID v4.
- Il ne faut en aucun cas qu'un connecteur ait l'ID du compte administrateur ou tout autre compte qu'un compte de type « connecteur », en effet en cas de compromission cela pourrait causer des dégâts plus élevés.

Si vous souhaitez obtenir des UUID v4 conformes je vous invite à en générer sur le site suivant par exemple :

<https://www.uuidgenerator.net/version4>

Saisir la commande suivante pour activer le service docker au démarrage, ainsi à chaque redémarrage du poste docker sera automatiquement démarré :

- `sudo systemctl start docker.service`

Détails de la commande :

- `sudo` : pour exécuter avec des privilèges élevés
- `systemctl` : gestionnaire de systemd et des services
- `start` : pour démarrer un service
- `docker.service` : le service à démarrer

```
pich@OpenCTI:~$ sudo systemctl start docker.service
```

#### 6.4.5 ElasticSearch

Il faut insérer un paramètre à la fin de fichier « `/etc/sysctl.conf` », pour faire cela saisir la commande suivante :

- `sudo nano /etc/sysctl.conf`

```
pich@OpenCTI:~$ sudo nano /etc/sysctl.conf
```

A la fin du fichier ajouter le paramètre suivant :

- `vm.max_map_count=262144`

#### 6.4.6 docker-compose.yml

Ce fichier étant relativement long, nous allons le découper en plusieurs parties pour voir les éléments présents avant de déployer la stack.

Pour afficher le contenu du fichier saisir la commande suivante :

- `cat docker-compose.yml`

```
pich@OpenCTI:~/opencti/docker$ cat docker-compose.yml
```

Important : selon la version et la date de consultation du contenu de ce fichier, les éléments peuvent changer, ici je montre le fichier de configuration pour montrer un exemple de contenu attendu.

#### 6.4.6.1 Redis

```
redis:
  image: redis:6.2.6
  restart: always
  volumes:
    - redisdata:/data
```

#### 6.4.6.2 ElasticSearch

```
elasticsearch:
  image: docker.elastic.co/elasticsearch/elasticsearch:7.16.2
  volumes:
    - esdata:/usr/share/elasticsearch/data
  environment:
    - discovery.type=single-node
    - xpack.ml.enabled=false
  restart: always
  ulimits:
    memlock:
      soft: -1
      hard: -1
    nofile:
      soft: 65536
      hard: 65536
```

#### 6.4.6.3 Minio

```
minio:
  image: minio/minio:RELEASE.2021-11-09T03-21-45Z
  volumes:
    - s3data:/data
  ports:
    - "9000:9000"
  environment:
    MINIO_ROOT_USER: ${MINIO_ROOT_USER}
    MINIO_ROOT_PASSWORD: ${MINIO_ROOT_PASSWORD}
  command: server /data
  healthcheck:
    test: ["CMD", "curl", "-f", "http://localhost:9000/minio/health/live"]
    interval: 30s
    timeout: 20s
    retries: 3
  restart: always
```

#### 6.4.6.4 RabbitMQ

```
rabbitmq:
  image: rabbitmq:3.9-management
  environment:
    - RABBITMQ_DEFAULT_USER=${RABBITMQ_DEFAULT_USER}
    - RABBITMQ_DEFAULT_PASS=${RABBITMQ_DEFAULT_PASS}
  volumes:
    - amqpdata:/var/lib/rabbitmq
  restart: always
```

#### 6.4.6.5 OpenCTI

Voici sans doute le container le plus important, puisque le but après tout c'est d'avoir du OpenCTI fonctionnel !

Nous pouvons noter dès à présent le port par défaut pour accéder à l'interface web de la plateforme depuis le port « 8080 ».

```
opentcti:
  image: opentcti/platform:5.1.3
  environment:
    - NODE_OPTIONS=--max-old-space-size=8096
    - APP_PORT=8080
    - APP_ADMIN_EMAIL=${OPENTCTI_ADMIN_EMAIL}
    - APP_ADMIN_PASSWORD=${OPENTCTI_ADMIN_PASSWORD}
    - APP_ADMIN_TOKEN=${OPENTCTI_ADMIN_TOKEN}
    - APP_APP_LOGS_LOGS_LEVEL=error
    - REDIS_HOSTNAME=redis
    - REDIS_PORT=6379
    - ELASTICSEARCH_URL=http://elasticsearch:9200
    - MINIO_ENDPOINT=minio
    - MINIO_PORT=9000
    - MINIO_USE_SSL=false
    - MINIO_ACCESS_KEY=${MINIO_ROOT_USER}
    - MINIO_SECRET_KEY=${MINIO_ROOT_PASSWORD}
    - RABBITMQ_HOSTNAME=rabbitmq
    - RABBITMQ_PORT=5672
    - RABBITMQ_PORT_MANAGEMENT=15672
    - RABBITMQ_MANAGEMENT_SSL=false
    - RABBITMQ_USERNAME=${RABBITMQ_DEFAULT_USER}
    - RABBITMQ_PASSWORD=${RABBITMQ_DEFAULT_PASS}
    - SMTP_HOSTNAME=${SMTP_HOSTNAME}
    - SMTP_PORT=25
    - PROVIDERS_LOCAL_STRATEGY=LocalStrategy
  ports:
    - "8080:8080"
  depends_on:
    - redis
    - elasticsearch
    - minio
    - rabbitmq
  restart: always
```

#### 6.4.6.6 Worker

Par défaut « 3 » workers sont créés, vous pouvez ajuster ce paramètre :

```
worker:
  image: opencti/worker:5.1.3
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - WORKER_LOG_LEVEL=info
  depends_on:
    - opencti
  deploy:
    mode: replicated
    replicas: 3
    restart: always
```

#### 6.4.6.7 Connector-History

Ce connecteur va permettre d'ajouter l'historique des éléments par exemple date de création, modification, auteur ...

```
connector-history:
  image: opencti/connector-history:5.1.3
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${CONNECTOR_HISTORY_ID} # Valid UUIDv4
    - CONNECTOR_TYPE=STREAM
    - CONNECTOR_NAME=History
    - CONNECTOR_SCOPE=history
    - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=info
  restart: always
  depends_on:
    - opencti
```

#### 6.4.6.8 Connector Export File STIX

Ce connecteur va permettre d'exporter les éléments au format STIX

```
connector-export-file-stix:
  image: opencti/connector-export-file-stix:5.1.3
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${CONNECTOR_EXPORT_FILE_STIX_ID} # Valid UUIDv4
    - CONNECTOR_TYPE=INTERNAL_EXPORT_FILE
    - CONNECTOR_NAME=ExportFileStix2
    - CONNECTOR_SCOPE=application/json
    - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=info
  restart: always
  depends_on:
    - opencti
```

#### 6.4.6.9 Connector Export File CSV

Ce connecteur va permettre d'exporter les éléments au format CSV

```
connector-export-file-csv:
  image: opencti/connector-export-file-csv:5.1.3
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${CONNECTOR_EXPORT_FILE_CSV_ID} # Valid UUIDv4
    - CONNECTOR_TYPE=INTERNAL_EXPORT_FILE
    - CONNECTOR_NAME=ExportFileCsv
    - CONNECTOR_SCOPE=text/csv
    - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=info
  restart: always
  depends_on:
    - opencti
```

#### 6.4.6.10 Connector Export File TXT

Ce connecteur va permettre d'exporter les éléments au format TXT

```
connector-export-file-txt:
  image: opencti/connector-export-file-txt:5.1.3
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${CONNECTOR_EXPORT_FILE_TXT_ID} # Valid UUIDv4
    - CONNECTOR_TYPE=INTERNAL_EXPORT_FILE
    - CONNECTOR_NAME=ExportFileTxt
    - CONNECTOR_SCOPE=text/plain
    - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=info
  restart: always
  depends_on:
    - opencti
```

#### 6.4.6.11 Connector Import File STIX

Ce connecteur va permettre d'importer des éléments depuis un format STIX

```
connector-import-file-stix:
  image: opencti/connector-import-file-stix:5.1.3
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${CONNECTOR_IMPORT_FILE_STIX_ID} # Valid UUIDv4
    - CONNECTOR_TYPE=INTERNAL_IMPORT_FILE
    - CONNECTOR_NAME=ImportFileStix
    - CONNECTOR_VALIDATE_BEFORE_IMPORT=true # Validate any bundle before import
    - CONNECTOR_SCOPE=application/json,text/xml
    - CONNECTOR_AUTO=true # Enable/disable auto-import of file
    - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=info
  restart: always
  depends_on:
    - opencti
```

#### 6.4.6.12 Connector Import Document

```
connector-import-document:
  image: opencti/connector-import-document:5.1.3
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${CONNECTOR_IMPORT_DOCUMENT_ID} # Valid UUIDv4
    - CONNECTOR_TYPE=INTERNAL_IMPORT_FILE
    - CONNECTOR_NAME=ImportDocument
    - CONNECTOR_VALIDATE_BEFORE_IMPORT=true # Validate any bundle before import
    - CONNECTOR_SCOPE=application/pdf,text/plain,text/html
    - CONNECTOR_AUTO=true # Enable/disable auto-import of file
    - CONNECTOR_ONLY_CONTEXTUAL=false # Only extract data related to an entity (a report, a threat actor, etc.)
    - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=info
    - IMPORT_DOCUMENT_CREATE_INDICATOR=true
  restart: always
  depends_on:
    - opencti
```

#### 6.4.6.13 Volumes

Les données sont enregistrées sur des volumes :

```
volumes:
  esdata:
  s3data:
  redisdata:
  amqpdata:
```

#### 6.4.6.14 Cas général

Tout au long du fichier de configuration nous avons pu constater deux éléments :

- Les containers sont les uns et les autres dépendants du container « OpenCTI », ce qui signifie que tant que ce container n'est pas démarré, les autres dépendant de lui pour le bon fonctionnement
  - OpenCTI va attendre ses dépendances (elastic, redis, minio, rabbit) et les connecteurs vont attendre OpenCTI
- Les containers ont le paramètre « restart : always » ainsi même en cas de redémarrage de la machine, les services redémarrent automatiquement
- La persistance des données est assurée dans des volumes.

#### 6.4.6.15 Déploiement de la stack

Nous pouvons à ce stade déployer la stack et avoir une CTI fonctionnelle, cependant il manquera un élément essentiel, les données !

En effet la plateforme sera fonctionnelle mais puisqu'aucune source de données n'aura été renseignée nous n'aurons pas d'éléments.

Cependant pour des raisons de simplicité nous allons quand même déployer la stack maintenant et la mettre à jour par la suite pour prendre en compte les changements.

Saisir la commande suivante :

- `docker-compose up -d`

Détails de la commande :

- `docker-compose` : programme à utiliser
- `up` :
- `-d` :

Remarque : il est essentiel d'être dans le répertoire qui contient le fichier « `docker-compose.yml` ».

```
mudpak@OpenCTI:~/opencti/docker$ docker-compose up -d
```

Docker applique la configuration du fichier « `docker-compose.yml` », dans le cas présent la création d'un réseau, des volumes, téléchargement des containers sont réalisées.

Cette étape peut prendre un certain temps lorsqu'elle est exécutée pour la première fois.

```
WARNING: Some services (worker) use the 'deploy' key, which will be ignored. Compose does not support 'deploy' configuration - use 'docker stack deploy' to deploy to a swarm.
Creating network "docker_default" with the default driver
Creating volume "docker_esdata" with default driver
Creating volume "docker_s3data" with default driver
Creating volume "docker_redisdata" with default driver
Creating volume "docker_amqpdata" with default driver
Pulling redis (redis:6.2.6)...
6.2.6: Pulling from library/redis
a2abf6c4d29d: Pull complete
c7a4e4382001: Pull complete
4044b9ba67c9: Pull complete
c8308a79402f: Pull complete
413c8bb60be2: Pull complete
1abfd3011519: Pull complete
Digest: sha256:db485f2e245b5b3329fdc7eff4eb00f913e09d8feb9ca720788059fdc2ed8339
Status: Downloaded newer image for redis:6.2.6
Pulling elasticsearch (docker.elastic.co/elasticsearch/elasticsearch:7.16.2)...
7.16.2: Pulling from elasticsearch/elasticsearch
da847062c6f6: Pull complete
f9947111a3a4: Pull complete
5f47506629dc: Pull complete
6728f0016c7b: Downloading [=====] 300.4MB/371.5MB
8ee4bcac6dc4: Download complete
```

Lorsque le processus est terminé, vous devez obtenir un résultat similaire à ci-dessous :

Tous les connecteurs démarrent mais cela ne veut pas dire que la plateforme est up en effet il faut attendre un certain temps (15 à 20 minutes dans mon cas) le temps que la plateforme se mette en place et devienne accessible !

Le meilleur moyen et de regarder si elle est up, c'est de regarder les logs docker pour voir les traces de start de la plateforme.

```
Creating docker_minio_1 ... done
Creating docker_rabbitmq_1 ... done
Creating docker_elasticsearch_1 ... done
Creating docker_redis_1 ... done
Creating docker_opencti_1 ... done
Creating docker_worker_1 ... done
Creating docker_connector-export-file-csv_1 ... done
Creating docker_connector-export-file-txt_1 ... done
Creating docker_connector-export-file-stix_1 ... done
Creating docker_connector-import-document_1 ... done
Creating docker_connector-import-file-stix_1 ... done
Creating docker_connector-history_1 ... done
```

Pour enrichir notre plateforme nous allons ajouter des connecteurs externes et par la suite nous partirons sur l'exploration de la plateforme.

## 7. Sources de données gratuites

Pour « enrichir » la plateforme de données, vous pouvez importer des données via différentes méthodes, dans le cas présent nous allons parler des « connecteurs d'imports externes ».

Voici un tableau de liste de sources de données « gratuites » et publiques, par là j'entends

- Option 1 : Il n'y a pas besoin de se créer un compte sur la plateforme pour pouvoir accéder aux données
- Option 2 : Il y a besoin de créer un compte sur la plateforme mais l'accès aux données ne requiert aucun paiement en contrepartie

Source de données :	Accès sans API ?	Accès avec API gratuite ?
AM!TT	Oui	-
AlienVault OTX	Non	Oui
Abuse.ch URL haus	Oui	-
CAPE	Oui	-
CVE	Oui	-
Cryptolaemus	Oui	-
CyberThreatCoalition	Oui	-
Cybercrime-Tracker	Oui	-
MITRE ATT&CK	Oui	-
Malpedia	Oui	-
MalwareBazaar	Oui	-
URLHaus Recent Payloads	Oui	-
VX Vault URL List	Oui	-

Remarque : bien évidemment si vous êtes dans un cercle de personnes qui partagent des données CTI via des instances privées MISP, YETI, OpenCTI ou autre il est tout à fait possible d'accéder aux données si les accès ont été accordés par le gestionnaire.

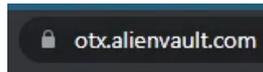
## 7.1 AlienVault OTX

Nous allons voir en détails comment créer un compte sur la plateforme AlivenVault OTX afin d'obtenir une clé API dans le but d'alimenter notre plateforme OpenCTI.

### 7.1.1 SIGN UP

Se rendre à l'adresse suivante :

- <https://otx.alienvault.com/>



Cliquer sur « Sign Up » et remplir les champs :

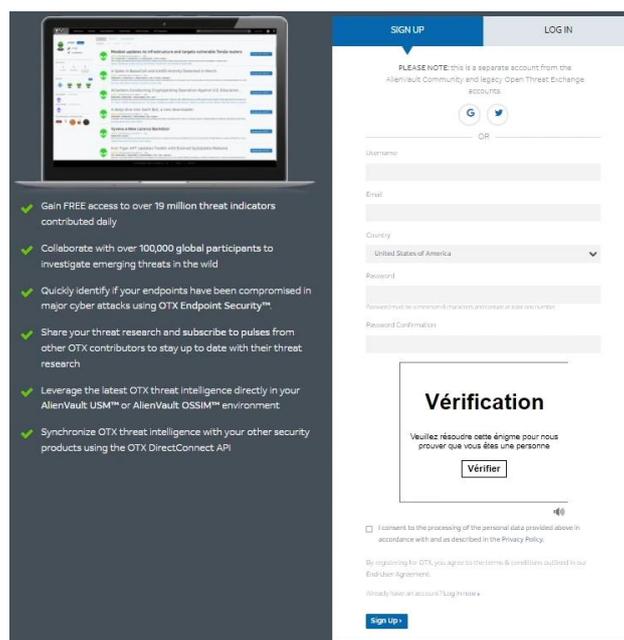
- Username : par un pseudonyme contenant entre 8 à 30 caractères
- Email : une adresse email valide pour confirmer la création de votre compte
- Country : par votre pays
- Password : un mot de passe robuste
- Password Confirmation : saisir à nouveau le mot de passe pour être certain
- Vérifier : cliquer sur le captcha à résoudre

Cocher la case

- « I consent to the processing of the personal data provided above in accordance with and as described in the Privacy Policy. »

Cliquer sur

- Sign Up



### 7.1.2 Welcome to AlienVault OTX

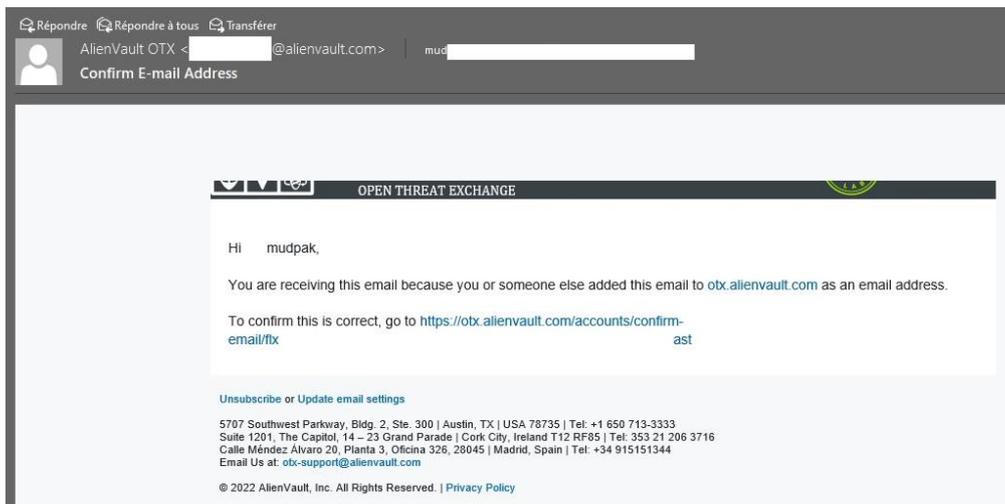
Un message s'affiche vous informant qu'un email de vérification a été envoyé et qu'il faut suivre le lien pour confirmer votre compte :

#### Welcome to AlienVault OTX



Thanks for signing up for OTX! We have sent an e-mail to you for verification. Follow the link provided to finalize the signup process. Please contact us if you do not receive it within a few minutes.

Voici un exemple de mail que vous recevez et il faut cliquer sur le lien fourni pour procéder à la vérification du compte :



Cliquer sur

- Confirm Email

#### Confirm your email



Please confirm that mud is an e-mail address for user mudpak.

Confirm Email

Le compte est désormais confirmé et nous pouvons nous connecter :



### 7.1.3 LOG IN

Cliquer sur

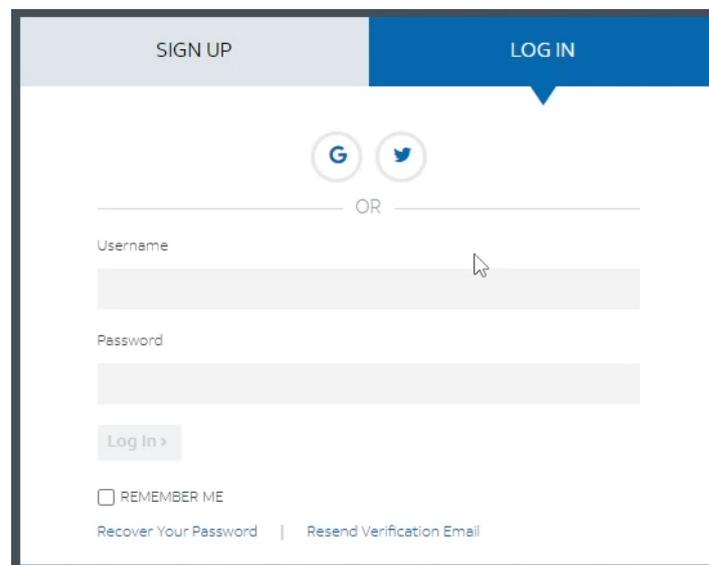
- Log In

Remplir les champs

- Username
- Password

Cliquer sur

- Log In

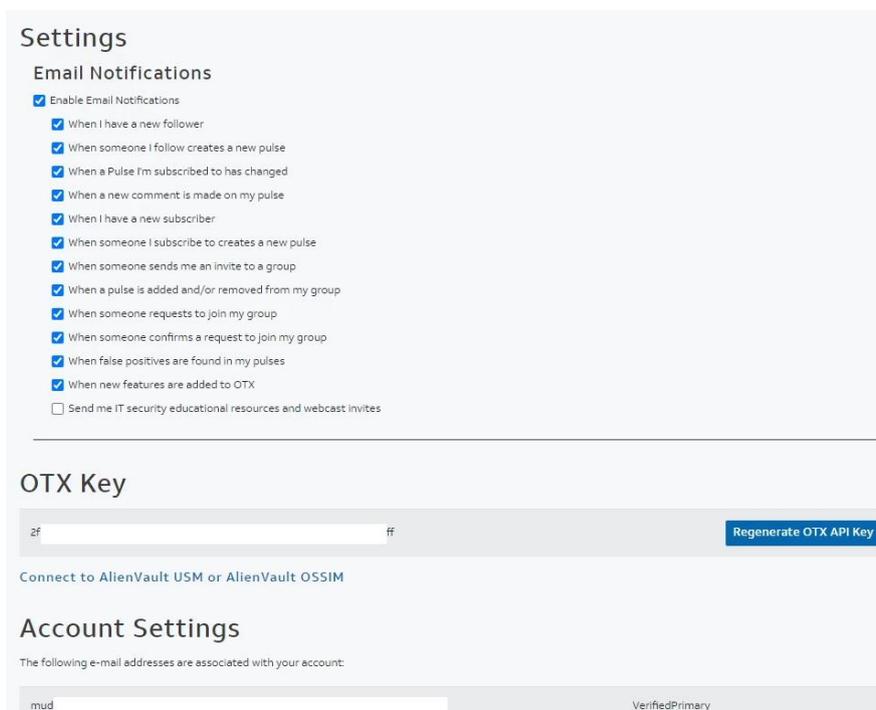


The screenshot shows a login interface with a dark blue header containing two tabs: 'SIGN UP' and 'LOG IN'. The 'LOG IN' tab is active. Below the header, there are two circular social media icons (Google and Twitter) with the text 'OR' between them. Underneath are two input fields labeled 'Username' and 'Password'. A 'Log In >' button is positioned below the password field. At the bottom, there is a 'REMEMBER ME' checkbox and two links: 'Recover Your Password' and 'Resend Verification Email'.

La page d'accueil nous affiche les paramètres du compte :

- Email Notifications : choisir quand être notifié par email
- OTX Key :
  - Le champ qui nous intéresse !
  - Vous pouvez voir la clé API liée à votre compte et à ne surtout pas partager
  - Il est possible de générer une autre clé API en cliquant sur « Regenerate OTX API Key », ce qui aura pour effet de révoquer la clé précédente et vous en délivrer une nouvelle
- Account Settings : paramètres notamment d'adresse email principale, secondaire

A ce stade je vous invite à copier la clé API dans un endroit sûr car par la suite nous allons en avoir besoin.



The screenshot displays the 'Settings' page of OpenCTI, organized into three main sections:

- Email Notifications:** A list of 14 notification events, each with a checked checkbox. The events include: 'When I have a new follower', 'When someone I follow creates a new pulse', 'When a Pulse I'm subscribed to has changed', 'When a new comment is made on my pulse', 'When I have a new subscriber', 'When someone I subscribe to creates a new pulse', 'When someone sends me an invite to a group', 'When a pulse is added and/or removed from my group', 'When someone requests to join my group', 'When someone confirms a request to join my group', 'When false positives are found in my pulses', and 'When new features are added to OTX'. There is also an unchecked checkbox for 'Send me IT security educational resources and webcast invites'.
- OTX Key:** A text input field containing the characters 'zf' followed by a masked field 'ff'. To the right of the field is a blue button labeled 'Regenerate OTX API Key'.
- Account Settings:** A section titled 'Connect to AlienVault USM or AlienVault OSSIM'. Below this, it states 'The following e-mail addresses are associated with your account:' followed by a text input field containing 'mud' and the status 'VerifiedPrimary'.

### 7.1.4 Ajout du connecteur

Voici la configuration par défaut du connecteur AlienVault OTX :

```
version: '3'
services:
  connector-alienvault:
    image: opencti/connector-alienvault:5.1.4
    environment:
      - OPENCTI_URL=http://localhost:8080
      - OPENCTI_TOKEN=ChangeMe
      - CONNECTOR_ID=ChangeMe
      - CONNECTOR_TYPE=EXTERNAL_IMPORT
      - CONNECTOR_NAME=AlienVault
      - CONNECTOR_SCOPE=alienvault
      - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
      - CONNECTOR_UPDATE_EXISTING_DATA=false
      - CONNECTOR_LOG_LEVEL=info
      - ALIENVAULT_BASE_URL=https://otx.alienvault.com
      - ALIENVAULT_API_KEY=ChangeMe
      - ALIENVAULT_TLP=white
      - ALIENVAULT_CREATE_OBSERVABLES=true
      - ALIENVAULT_CREATE_INDICATORS=true
      - ALIENVAULT_PULSE_START_TIMESTAMP=2020-05-01T00:00:00 # BEWARE! Could be a lot of pulses!
      - ALIENVAULT_REPORT_TYPE=threat-report
      - ALIENVAULT_REPORT_STATUS=New
      - ALIENVAULT_GUESS_MALWARE=false # Use tags to guess malware.
      - ALIENVAULT_GUESS_CVE=false # Use tags to guess CVE.
      - ALIENVAULT_EXCLUDED_PULSE_INDICATOR_TYPES=FileHash-MD5,FileHash-SHA1 # Excluded Pulse indicator types.
      - ALIENVAULT_ENABLE_RELATIONSHIPS=true # Enable/Disable relationship creation between SDOs.
      - ALIENVAULT_ENABLE_ATTACK_PATTERNS_INDICATES=true # Enable/Disable "indicates" relationships between indicators and attack patterns
      - ALIENVAULT_INTERVAL_SEC=1800
    restart: always
```

A ce stade si vous ajoutons cette configuration dans le fichier « docker-compose.yml », le connecteur ne fonctionnera pas en effet comme nous pouvons l'observer à certaines lignes il faut modifier la configuration pour ajouter nos paramètres personnalisés.

Pour que les nouveaux éléments soient pris en compte il faudra arrêter la stack en cours d'utilisation, appliquer les changements et relancer la stack pour que la prise en compte des changements soit effective, si ces étapes ne sont pas réalisées alors les changements ne seront pas appliqués notamment dans la partie « docker network ».

Dans le cas présent nous devons modifier trois champs :

- OPENCTI\_TOKEN=ChangeMe
  - Créer une variable et saisir sa valeur UUID v4 dans le fichier « .env »
- CONNECTOR\_ID=ChangeMe
  - Créer une variable et saisir sa valeur UUID v4 dans le fichier « .env »
- ALIENVAULT\_API\_KEY=ChangeMe
  - Créer une variable et saisir sa valeur dans le fichier « .env »

```
7 - OPENCTI_TOKEN=ChangeMe
8 - CONNECTOR_ID=ChangeMe
9 - CONNECTOR_TYPE=EXTERNAL_IMPORT
10 - CONNECTOR_NAME=AlienVault
11 - CONNECTOR_SCOPE=alienvault
12 - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
13 - CONNECTOR_UPDATE_EXISTING_DATA=false
14 - CONNECTOR_LOG_LEVEL=info
15 - ALIENVAULT_BASE_URL=https://otx.alienvault.com
16 - ALIENVAULT_API_KEY=ChangeMe
```

Voici un exemple de résultat qu'on peut obtenir dans le fichier « .env » :

```
ALIENVAULT_OTX_CONNECTOR_ID=XXXXXXXX-XXXX-4XXXX-XXXX-XXXXXXXXXXXX
ALIENVAULT_OTX_API_KEY=2fXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXff
```

Voici un exemple de résultat qu'on peut obtenir dans le fichier « docker-compose.yml » :

```
connector-alienvault:
  image: opencti/connector-alienvault:5.1.3
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${ALIENVAULT_OTX_CONNECTOR_ID}
    - CONNECTOR_TYPE=EXTERNAL_IMPORT
    - CONNECTOR_NAME=AlienVault
    - CONNECTOR_SCOPE=alienvault
    - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_UPDATE_EXISTING_DATA=false
    - CONNECTOR_LOG_LEVEL=info
    - ALIENVAULT_BASE_URL=https://otx.alienvault.com
    - ALIENVAULT_API_KEY=${ALIENVAULT_OTX_API_KEY}
    - ALIENVAULT_TLP=White
    - ALIENVAULT_CREATE_OBSERVABLES=true
    - ALIENVAULT_CREATE_INDICATORS=true
    - ALIENVAULT_PULSE_START_TIMESTAMP=2022-01-01T00:00:00 # BEWARE! Could be a lot of pulses!
    - ALIENVAULT_REPORT_TYPE=threat-report
    - ALIENVAULT_REPORT_STATUS=New
    - ALIENVAULT_GUESS_MALWARE=false # Use tags to guess malware.
    - ALIENVAULT_GUESS_CVE=false # Use tags to guess CVE.
    - ALIENVAULT_EXCLUDED_PULSE_INDICATOR_TYPES=FileHash-MD5,FileHash-SHA1 # Excluded Pulse indicator types.
    - ALIENVAULT_ENABLE_RELATIONSHIPS=true # Enable/Disable relationship creation between SDOs.
    - ALIENVAULT_ENABLE_ATTACK_PATTERNS_INDICATES=true # Enable/Disable "indicates" relationships between indicators and attack patterns
    - ALIENVAULT_INTERVAL_SEC=1800
  restart: always
```

## 7.2 CVE

Contrairement au connecteur précédent, la configuration du connecteur CVE est beaucoup plus courte et simple !

En effet il ne requiert aucun compte, les seuls éléments dont nous aurons besoins seront :

- Un token OpenCTI
- Un ID (UUID v4) pour le connecteur

```
1 version: '3'
2 services:
3   connector-cve:
4     image: opencti/connector-cve:5.1.4
5     environment:
6       - OPENCTI_URL=http://localhost:8080
7       - OPENCTI_TOKEN=ChangeMe
8       - CONNECTOR_ID=ChangeMe
9       - CONNECTOR_TYPE=EXTERNAL_IMPORT
10      - CONNECTOR_NAME=Common Vulnerabilities and Exposures
11      - CONNECTOR_SCOPE=identity,vulnerability
12      - CONNECTOR_CONFIDENCE_LEVEL=75 # From 0 (Unknown) to 100 (Fully trusted)
13      - CONNECTOR_UPDATE_EXISTING_DATA=true
14      - CONNECTOR_RUN_AND_TERMINATE=false
15      - CONNECTOR_LOG_LEVEL=info
16      - CVE_IMPORT_HISTORY=true # Import history at the first run (after only recent), reset the connector state if you want to re-import
17      - CVE_MVD_DATA_FEED=https://nvd.nist.gov/feeds/json/cve/1.1/nvdcve-1.1-recent.json.gz
18      - CVE_HISTORY_DATA_FEED=https://nvd.nist.gov/feeds/json/cve/1.1/
19      - CVE_INTERVAL=7 # In days, must be strictly greater than 1
20     restart: always
```

Il faut procéder de la même façon qu'avec le connecteur AlienVault, c'est-à-dire

- Modifier les valeurs « ChangeMe » par des variables
- Ajouter les variables dans le fichier « .env » et insérer leur valeur

Voici un exemple de résultat obtenu dans le fichier « .env » pour le connecteur CVE :

```
CVE_CONNECTOR_ID=[redacted]-[redacted]-4-[redacted]-[redacted]
```

Voici un exemple de résultat obtenu dans le fichier « docker-compose » pour le connecteur CVE :

```
connector-cve:
  image: opencti/connector-cve:5.1.3
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${CVE_CONNECTOR_ID}
    - CONNECTOR_TYPE=EXTERNAL_IMPORT
    - CONNECTOR_NAME=Common Vulnerabilities and Exposures
    - CONNECTOR_SCOPE=identity,vulnerability
    - CONNECTOR_CONFIDENCE_LEVEL=75 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_UPDATE_EXISTING_DATA=true
    - CONNECTOR_RUN_AND_TERMINATE=false
    - CONNECTOR_LOG_LEVEL=info
    - CVE_IMPORT_HISTORY=true # Import history at the first run (after only recent), reset the connector state if you want to re-import
    - CVE_NVD_DATA_FEED=https://nvd.nist.gov/feeds/json/cve/1.1/nvdcve-1.1-recent.json.gz
    - CVE_HISTORY_DATA_FEED=https://nvd.nist.gov/feeds/json/cve/1.1/
    - CVE_INTERVAL=7 # In days, must be strictly greater than 1
  restart: always
```

## 8. Sources de données payantes

Il faut considérer les autres plateformes que listées dans le chapitre précédent comme étant « payantes ».

Remarque : je ne rentre pas dans la subtilité de savoir si l'accès à une instance distante par exemple MISP est gratuit ou payant, car la solution a beau être open-source, le détenteur peut selon les personnes accorder ou refuser l'accès ou faire payer l'accès.

## 9. Docker Compose – Part 2

Maintenant que nous avons vu comment ajouter des connecteurs et effectué la configuration dans les fichiers « .env » et « docker-compose.yml » il faut faire appliquer ces changements !

En effet la stack étant en cours d'exécution nous devons la stopper, lui dire de recharger le fichier de configuration et relancer la stack.

Remarque : vous pouvez également exécuter la commande suivante pour aller plus rapidement « `sudo docker-compose up -d` » ce qui aura pour effet de relancer la stack avec la prise en compte des changements, cependant cela peut engendrer des erreurs auquel cas je vous conseille d'utiliser la méthode ci-dessous.

Si vous souhaitez procéder par différentes étapes vous pouvez suivre les étapes suivantes :

Pour faire cela saisir la commande suivante :

- `sudo docker-compose stop`

L'arrêt des containers peut prendre un peu de temps :

```
mudpak@CTI:~/opencti/docker$ sudo docker-compose stop
[sudo] password for mudpak:
WARNING: Some services (worker) use the 'deploy' key, which will be ignored. Compose does not support 'deploy' configuration - use 'docker stack deploy' to deploy to a swarm.
Stopping docker_connector-urllhaus_1 ... done
Stopping docker_connector-amitt_1 ... done
Stopping docker_connector-cve_1 ... done
Stopping docker_connector-cape_1 ... done
Stopping docker_connector-export-file-stix_1 ... done
Stopping docker_connector-history_1 ... done
Stopping docker_connector-import-document_1 ... done
Stopping docker_connector-export-file-txt_1 ... done
Stopping docker_connector-import-file-stix_1 ... done
Stopping docker_connector-export-file-csv_1 ... done
Stopping docker_worker_1 ... done
Stopping docker_redis_1 ... done
Stopping docker_rabbitmq_1 ... done
Stopping docker_elasticsearch_1 ... done
Stopping docker_minio_1 ... done
Stopping docker_connector-alienvault_1 ... done
Stopping docker_connector-opencti_1 ... done
```

Pour recharger la configuration et obtenir les nouveaux containers, saisir la commande suivante :

- `sudo docker-compose pull`

Comme nous pouvons le constater docker-compose télécharge et extrait les containers qui n'étaient jusqu'ici pas présents :

```
mudpak@CTI:~/opencti/docker$ sudo docker-compose pull
WARNING: Some services (worker) use the 'deploy' key, which will be ignored. Compose does not support 'deploy' configuration - use 'docker stack deploy' to deploy to a swarm.
Pulling redis ... done
Pulling elasticsearch ... done
Pulling minio ... done
Pulling rabbitmq ... done
Pulling opencti ... done
Pulling worker ... done
e for o..nconnector-history ... done
Pulling connector-export-file-stix ... done
Pulling connector-export-file-csv ... done
Pulling connector-export-file-txt ... done
Pulling connector-import-file-stix ... done
Pulling connector-import-document ... done
Pulling connector-opencti ... done
Pulling connector-alienvault ... done
Pulling connector-amitt ... done
Pulling connector-cape ... done
Pulling connector-cve ... done
Pulling connector-urllhaus ... done
Pulling connector-cryptolaemus ... download complete
Pulling connector-cyber-threat-coalition ... done
Pulling connector-cybercrimetracker ... done
Pulling connector-malpedia ... extracting (100.0%)
Pulling connector-malware-bazaar-recent-additions ... already exists
Pulling connector-mitre ... already exists
Pulling connector-urllhaus-recent-payloads ... pull complete
Pulling connector-vxvault ... done
```

Pour démarrer la stack saisir la commande suivante :

- `sudo docker-compose up -d`

```
mudpak@CTI:~/opencti/docker$ sudo docker-compose up -d
WARNING: Some services (worker) use the 'deploy' key, which will be ignored. Compose does not support 'deploy' configuration - use 'docker stack deploy' to deploy to a swarm.
Starting docker_connector-amitt_1 ... done
Creating docker_connector-malpedia_1 ... done
Starting docker_connector-opencti_1 ... done
Creating docker_connector-malware-bazaar-recent-additions_1 ... done
Starting docker_minio_1 ... done
Creating docker_connector-cyber-threat-coalition_1 ... done
Creating docker_connector-mitre_1 ... done
Starting docker_connector-cape_1 ... done
Creating docker_connector-cryptolaemus_1 ... done
Creating docker_connector-cybercrimetracker_1 ... done
Starting docker_connector-cve_1 ... done
Starting docker_connector-alienvault_1 ... done
Creating docker_connector-urlhaus-recent-payloads_1 ... done
Starting docker_connector-urlhaus_1 ... done
Starting docker_redis_1 ... done
Starting docker_rabbitmq_1 ... done
Starting docker_elasticsearch_1 ... done
Creating docker_connector-vxvault_1 ... done
Starting docker_opencti_1 ... done
Starting docker_connector-history_1 ... done
Starting docker_connector-export-file-txt_1 ... done
Starting docker_connector-import-document_1 ... done
Starting docker_connector-import-file-stix_1 ... done
Starting docker_worker_1 ... done
Starting docker_connector-export-file-stix_1 ... done
Starting docker_connector-export-file-csv_1 ... done
```

## 10. OpenCTI – Découverte de l'interface web

Après avoir réalisé toutes les étapes précédentes votre plateforme OpenCTI devrait être fonctionnelle et les données devraient commencer à s'ajouter.

Nous pouvons enfin partir à la découverte de la plateforme !

### 10.1 Connexion à l'interface web

Se rendre à l'adresse suivante :

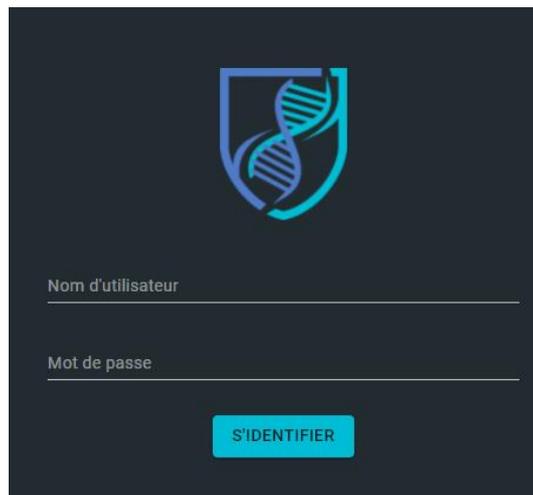
- <http://IP-Instance:8080/dashboard>

Une page similaire à ci-dessous s'affiche, remplir les champs :

- Nom d'utilisateur : par l'adresse email renseignée dans le fichier « .env »
- Mot de passe : par le mot de passe renseigné dans le fichier « .env »

Cliquer sur

- S'IDENTIFIER



Nom d'utilisateur

Mot de passe

S'IDENTIFIER

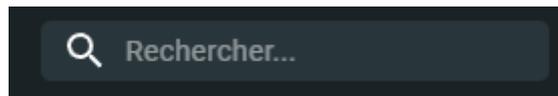
## 10.2 Tableau de bord

Commençons par le tableau de bord :

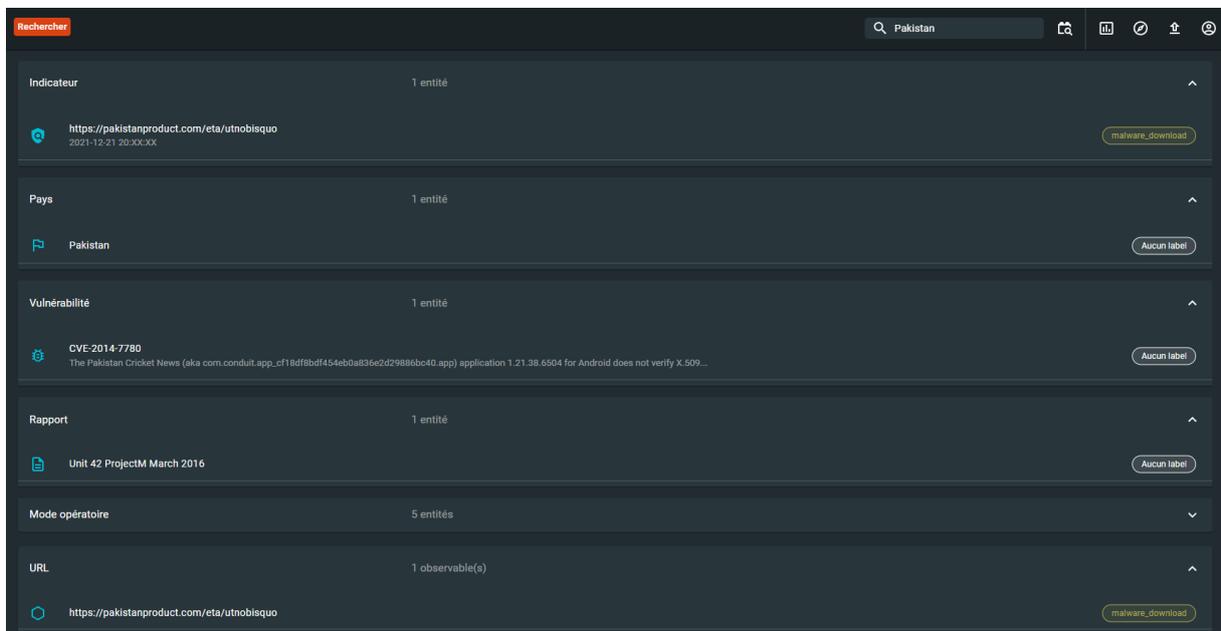


### 10.2.1 Recherche

Comme son nom l'indique, ce champ permet de faire des recherches :

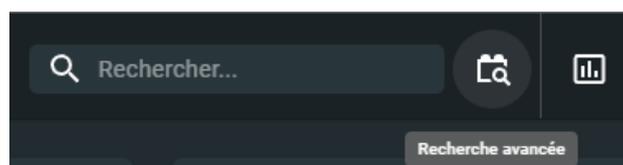


L'avantage de ce menu c'est qu'on peut chercher tous types d'éléments sans avoir à préciser de paramètres spécifiques :



### 10.2.2 Recherche avancée

La recherche avancée située à droite de la recherche « simple » :



Nous pouvons chercher les éléments via les critères suivants :

- Mot-clé global : n'importe quel élément à chercher
- Type d'entité :
- Label : on peut comparer ce système à un tag
- Confiance supérieure à : le niveau de confiance qu'on a en la source qui nous fournit l'information
- Créé après : élément après une certaine date
- Ingéré après : ingestion par la plateforme après une certaine date
- Marquage : le niveau de rapport au format « TLP »
- Auteur : auteur du rapport
- Type d'organisation :
- Créé avant : rapport crée avant une certaine date
- Ingéré avant : ingestion dans la plateforme avant une certaine date

**Recherche avancée**

Mot-clé global

Type d'entité ▼ Marquage ▼

Label ▼ Auteur ▼

Confiance supérieure à ▼ Type d'organisation ▼

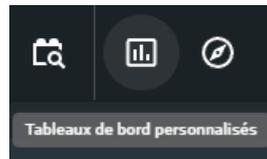
Créé après  Créé avant 

Ingéré après  Ingéré avant 

ANNULER RECHERCHER

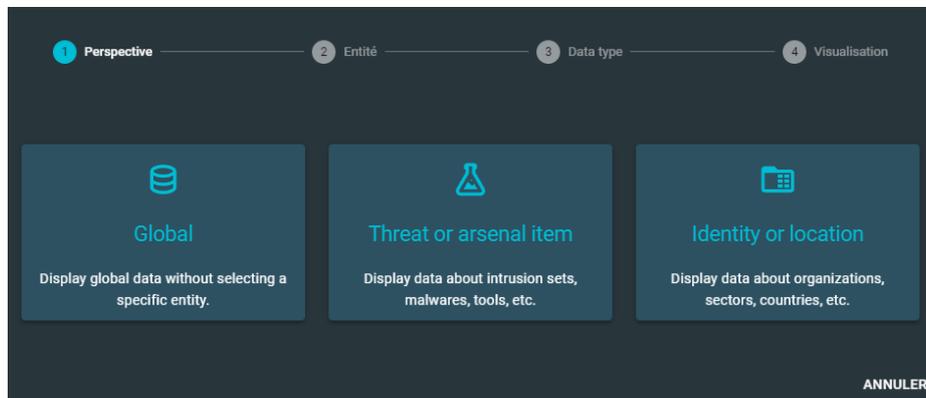
### 10.2.3 Tableaux de bords personnalisés

Par défaut il n'y a pas de tableaux de bords personnalisés, nous pouvons en créer en accédant dans ce menu :

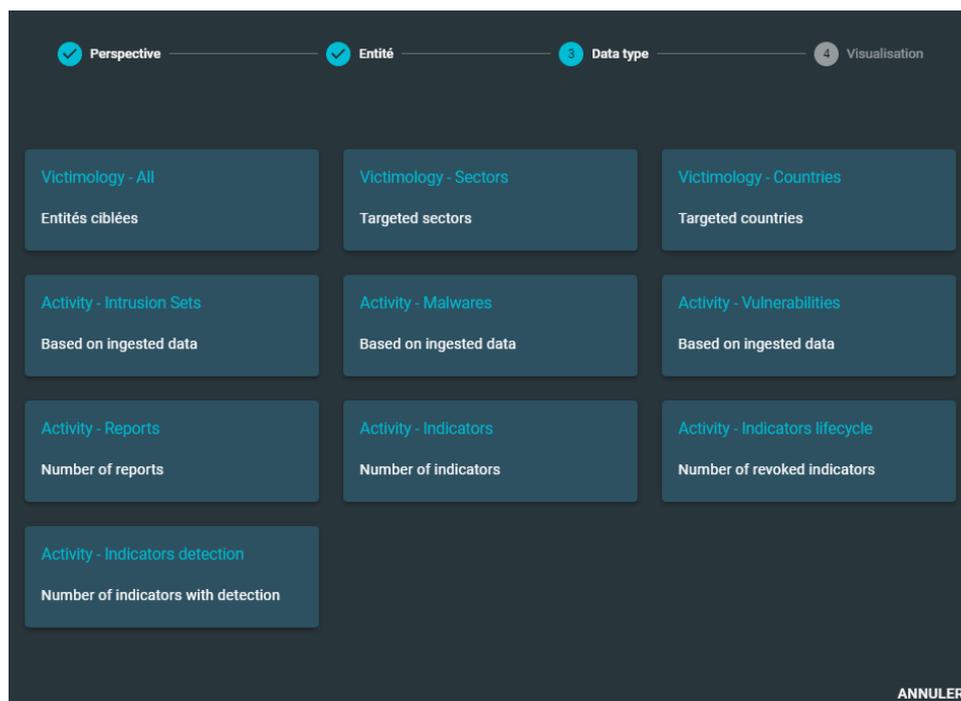


Il est possible de créer des tableaux de bords via différents critères tels que :

- Global : avoir un visuel général
- Threat or arsenal item : avoir des informations sur un élément spécifique
- Identity or location : avoir des informations sur une entité ou pays spécifique

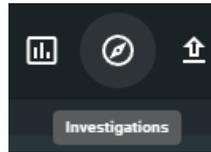


Selon le choix précédent, les données pourront être représentées sous différentes formes :



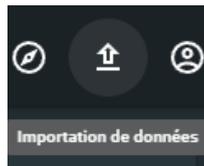
### 10.2.4 Investigations

Le but est de parcourir les graphes pour découvrir les relations.



### 10.2.5 Importation de données

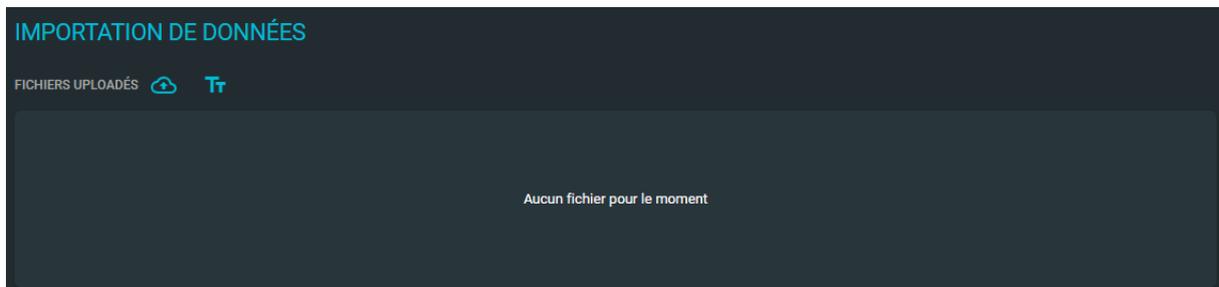
Nous pouvons importer des données manuellement :



#### 10.2.5.1 Fichiers uploadés

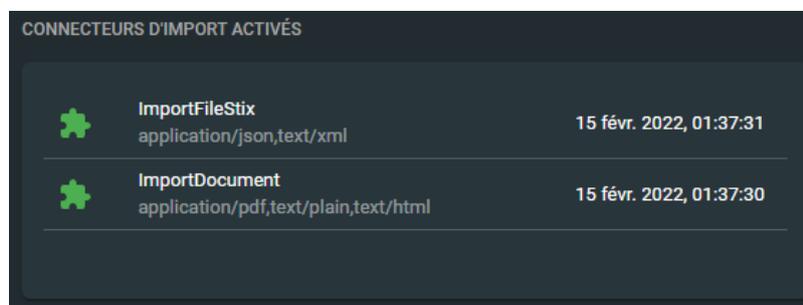
Nous pouvons uploader des fichiers :

- Soit en cliquant sur le logo du nuage pour sélectionner un fichier
- Soit en cliquant sur le logo du texte et saisir les informations en texte brute



#### 10.2.5.2 Connecteurs d'import activés

Nous pouvons voir que les connecteurs sont bien actifs :



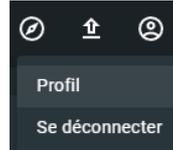
### 10.2.5.3 Fichiers en attente

Si des fichiers sont en attente ils seront listés ici :



### 10.2.6 Profil

Ce menu permet d'avoir les informations du compte utilisateur :

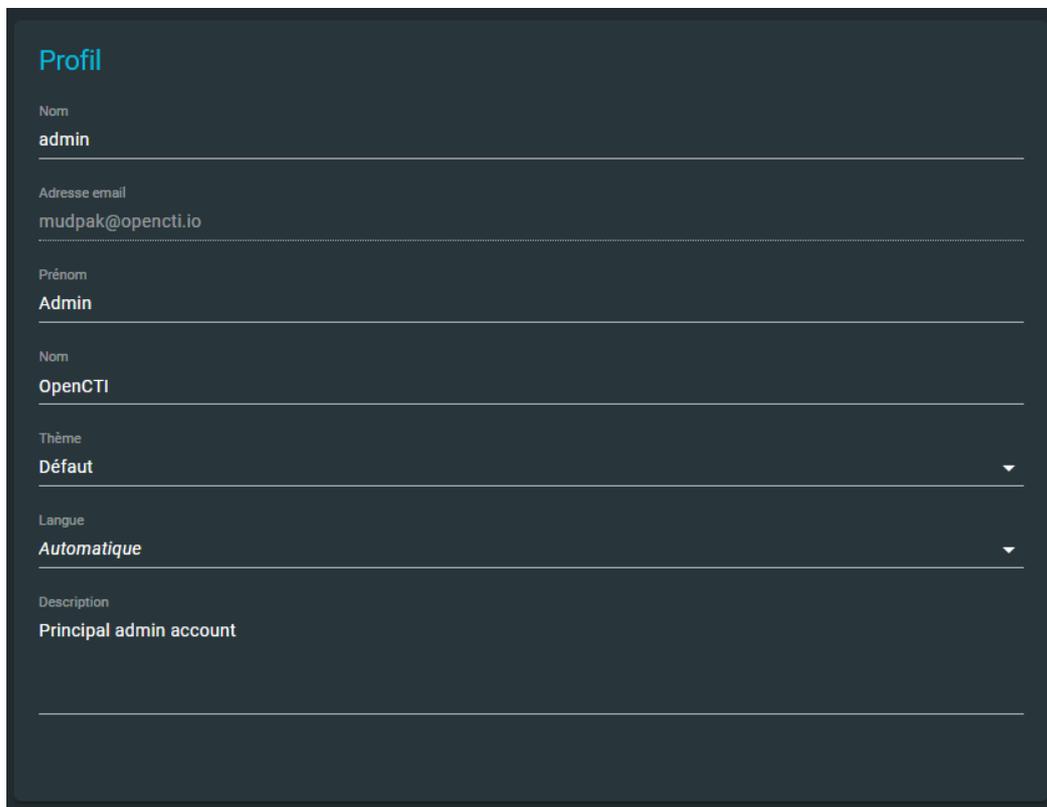


#### 10.2.6.1 Profil

Nous pouvons voir et configurer les paramètres de votre compte à cet endroit.

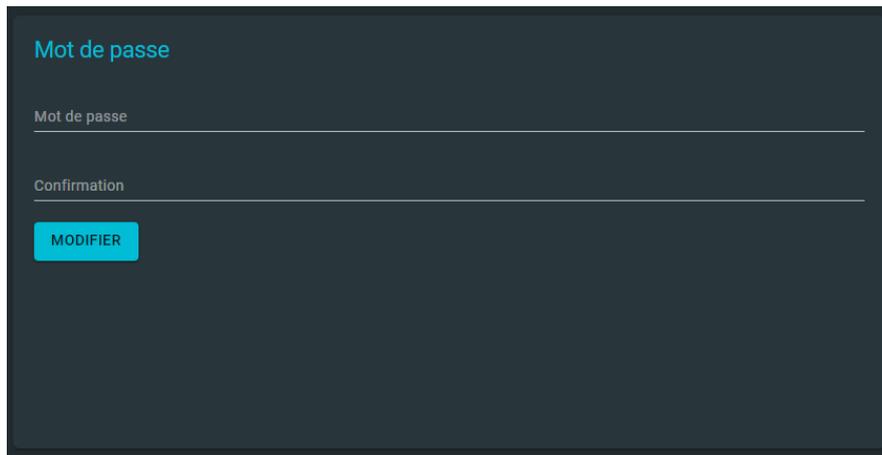
Dans le cas présent nous pouvons constater que le compte actuel :

- Est un compte administrateur
- Est le compte de l'administrateur principal (=compte crée lors de la création de l'instance)
  - L'utilisation d'un compte à hauts privilèges en milieu de production est vivement déconseillée



### 10.2.6.2 Mot de passe

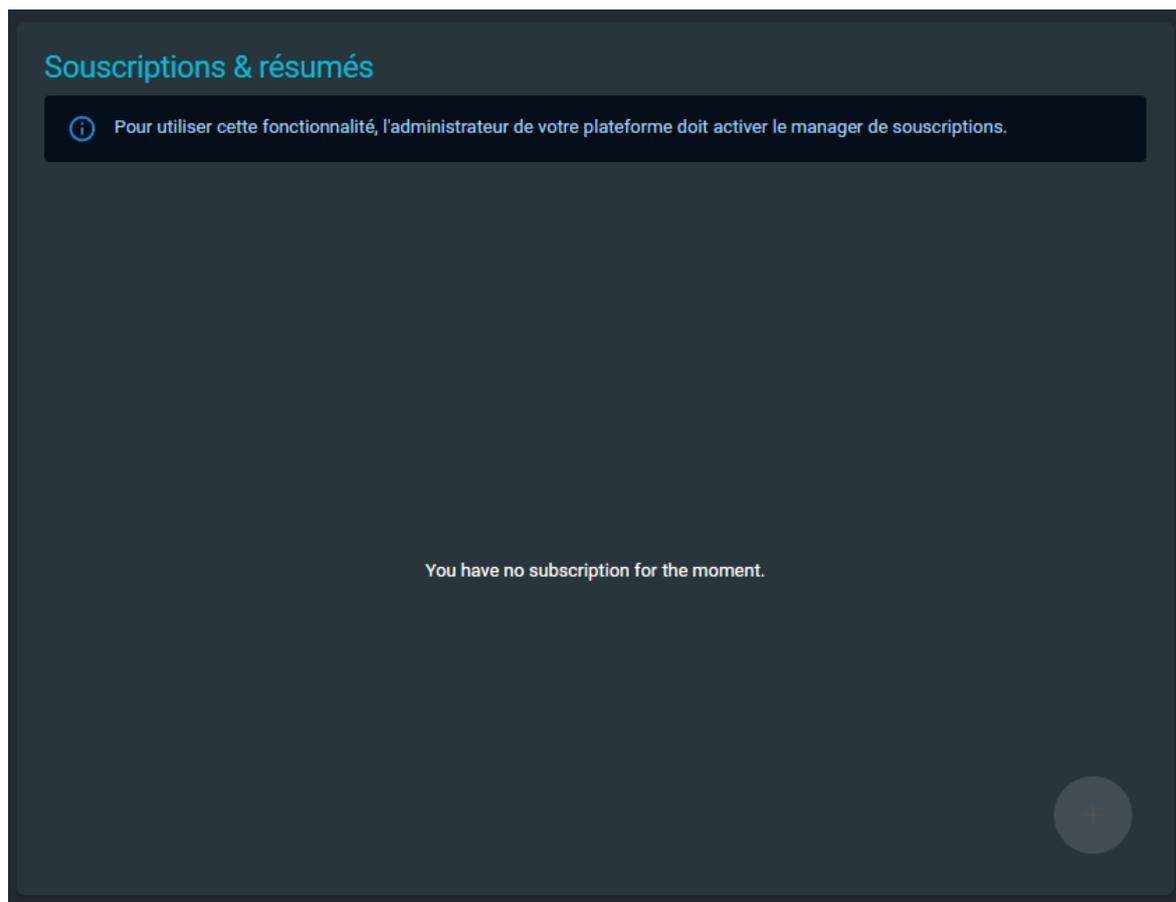
Nous pouvons modifier le mot de passe du compte à cet endroit :



The screenshot shows a dark-themed interface for changing a password. At the top, the title "Mot de passe" is displayed in a light blue font. Below the title, there are two input fields: "Mot de passe" and "Confirmation". A light blue button labeled "MODIFIER" is positioned below the "Confirmation" field.

### 10.2.6.3 Souscriptions & résumés

Feature qui permet de souscrire a des envois de mails concernant certaines informations.

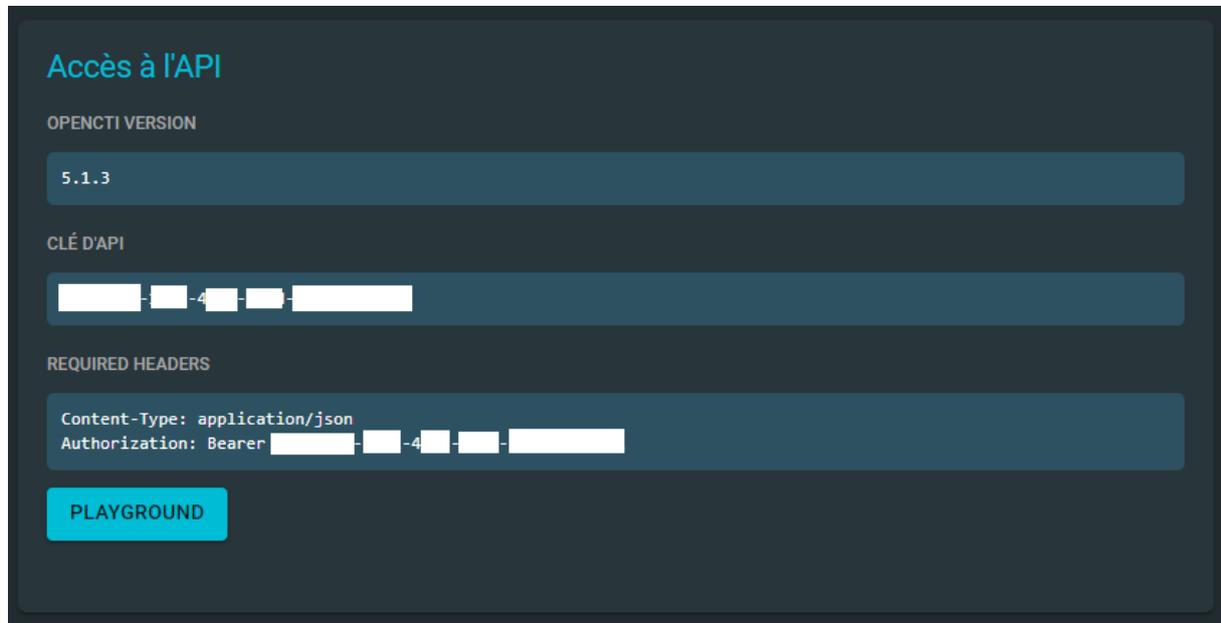


The screenshot shows a dark-themed interface for subscriptions and summaries. The title "Souscriptions & résumés" is displayed in a light blue font. Below the title, there is a dark grey notification box with a light blue information icon and the text: "Pour utiliser cette fonctionnalité, l'administrateur de votre plateforme doit activer le manager de souscriptions." Below the notification box, the text "You have no subscription for the moment." is displayed in a light grey font. A light blue circular button is visible in the bottom right corner.

#### 10.2.6.4 Accès à l'API

Nous avons quelques informations importantes dans cette partie, notamment la version de OpenCTI ainsi que la clé API du compte.

Par ailleurs en cliquant sur « PLAYGROUND » nous sommes redirigés vers une page « GraphQL ».



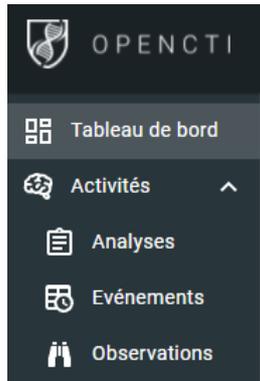
The screenshot shows a dark-themed interface for API access configuration. It features three main sections: 'OPENCTI VERSION' with a value of '5.1.3', 'CLÉ D'API' with a masked key, and 'REQUIRED HEADERS' with 'Content-Type: application/json' and 'Authorization: Bearer' followed by a masked token. A blue 'PLAYGROUND' button is located at the bottom of the configuration area.

#### 10.2.7 Se déconnecter

Comme son nom l'indique, ce paramètre permet de se déconnecter de l'interface web.

## 10.3 Activités

Dans le menu latéral gauche nous allons nous intéresser aux sous-menus de « Activités » :

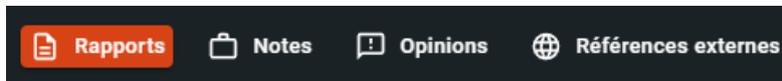


### 10.3.1 Analyses

Voici sans doute l'un des menus qui nous intéresse le plus ! En effet sous forme d'analyses sont représentées les informations issues de différents connecteurs.

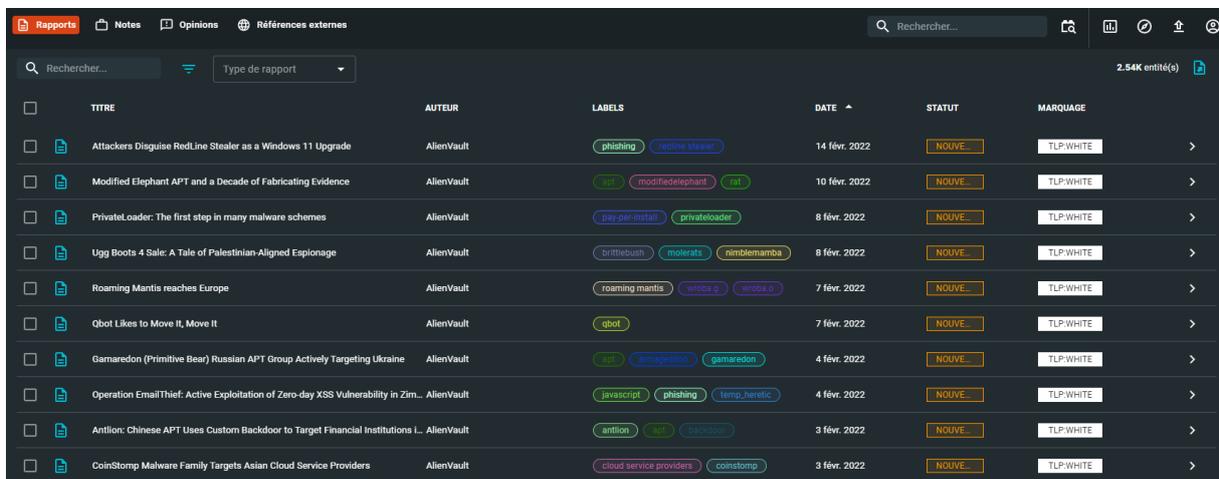
Ce menu est composé de sous-menus :

- Rapports
- Notes
- Opinions
- Références externes



#### 10.3.1.1 Rapports

Nous pouvons voir par exemple ci-dessous des rapports issus du connecteur AlienVault, les dates de création des rapports par le fournisseur, le statut ainsi que le marquage (=TLP).



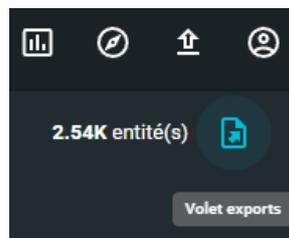
TITRE	AUTEUR	LABELS	DATE	STATUT	MARQUAGE
Attackers Disguise RedLine Stealer as a Windows 11 Upgrade	AlienVault	phishing, redline_stealer	14 févr. 2022	NOUVEAU	TLP:WHITE
Modified Elephant APT and a Decade of Fabricating Evidence	AlienVault	modified_elephant, apt	10 févr. 2022	NOUVEAU	TLP:WHITE
PrivateLoader: The first step in many malware schemes	AlienVault	pay-per-install, private_loader	8 févr. 2022	NOUVEAU	TLP:WHITE
Ugg Boots 4 Sale: A Tale of Palestinian-Aligned Espionage	AlienVault	brittlebush, molerats, nimblemamba	8 févr. 2022	NOUVEAU	TLP:WHITE
Roaming Mantis reaches Europe	AlienVault	roaming_mantis, wroba_g, wroba_b	7 févr. 2022	NOUVEAU	TLP:WHITE
Qbot Likes to Move It, Move It	AlienVault	qbot	7 févr. 2022	NOUVEAU	TLP:WHITE
Gamaredon (Primitive Bear) Russian APT Group Actively Targeting Ukraine	AlienVault	gamaredon, primitive_bear	4 févr. 2022	NOUVEAU	TLP:WHITE
Operation EmailThief: Active Exploitation of Zero-day XSS Vulnerability in Zimbra	AlienVault	javascript, phishing, temp_heretic	4 févr. 2022	NOUVEAU	TLP:WHITE
Antlion: Chinese APT Uses Custom Backdoor to Target Financial Institutions	AlienVault	antlion, backdoor	3 févr. 2022	NOUVEAU	TLP:WHITE
CoinStomp Malware Family Targets Asian Cloud Service Providers	AlienVault	cloud_service_providers, coinstomp	3 févr. 2022	NOUVEAU	TLP:WHITE

Deux types de filtres sont présents :

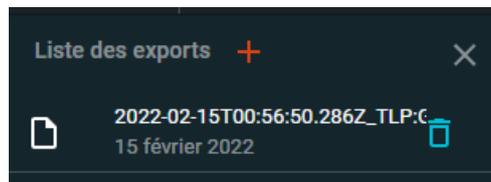
- Recherche
- Type de rapport



Depuis ce menu et plus globalement tous les menus suivants il nous sera possible d'exporter les éléments sous différents formats (CSV, TXT, PDF ...) effectuer cette opération il faut sélectionner un ou plusieurs éléments et cliquer sur le volet d'exports situé dans la zone supérieur droite de la fenêtre :

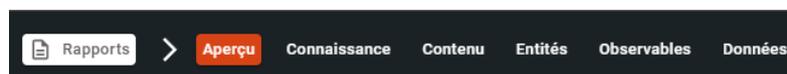


Voici un exemple d'export qui est prêt à être consulté :



Pour visualiser la puissance de OpenCTI et ses fonctionnalités nous allons prendre le rapport « UNIT 42 PROJECTM MARCH 2016 » comme exemple.

Dans le menu général nous avons accès à différents sous-menus où se trouvent les informations sous différentes formes :



Dans la partie « Informations de base » nous pouvons voir les informations suivantes :

- STIX ID standard : l'identifiant STIX donné au rapport
- Auteur : source qui a fourni le rapport
- Distribution des opinions : système de vote pour juger de la pertinence du rapport
- Date de création : date à laquelle la source a créé le rapport
- Date de modification :
- Révoqué : est-ce que le rapport est toujours applicable ou non
- Labels : si des labels sont applicables
- Niveau de confiance : le niveau de confiance en ce rapport / fournisseur
- Date de création (dans la plateforme) : date à laquelle le rapport a été créé sur notre plateforme OpenCTI
- Créateur : le compte qui a été utilisé pour créer le rapport
  - C'est bien évidemment une mauvaise pratique que d'utiliser un compte de type administrateur pour créer des rapports
  - Un rôle existe sur la plateforme pour les comptes de type « connecteur » ce qui est préférable dans ce type d'usage, nous verrons par la suite

The screenshot shows the 'Informations de base' (Basic Information) page for a report in OpenCTI. The page is titled 'UNIT 42 PROJECTM MARCH 2016' and has a 'TLP:WHITE' classification. The report's STIX ID standard is 'report--a[redacted]-4-1[redacted]3-5[redacted]6-9[redacted]d-2[redacted]3'. The author is 'PALO ALTO NETWORKS'. The report is not revoked ('NON'). The confidence level is 'FAIBLE'. The creation date is '25 mars 2016, 01:00:00' and the modification date is '7 février 2022, 00:11:25'. The creator is 'ADMIN'. A distribution of opinions chart is shown, with 'strongly-disagree' at the top, 'disagree' on the right, 'neutral' at the bottom, 'agree' on the left, and 'strongly-agree' at the top-left. The chart shows a score of approximately 1.5 out of 5.

UNIT 42 PROJECTM MARCH 2016 TLP:WHITE

INFORMATIONS DE BASE

STIX ID standard ⓘ  
report--a[redacted]-4-1[redacted]3-5[redacted]6-9[redacted]d-2[redacted]3

Autres IDs STIX ⓘ  
-

Auteur  
PALO ALTO NETWORKS

Révoqué  
NON

Distribution des opinions ⓘ

Labels +

Niveau de confiance  
FAIBLE

Date de création (dans la plateforme)  
16 janvier 2022, 22:33:12

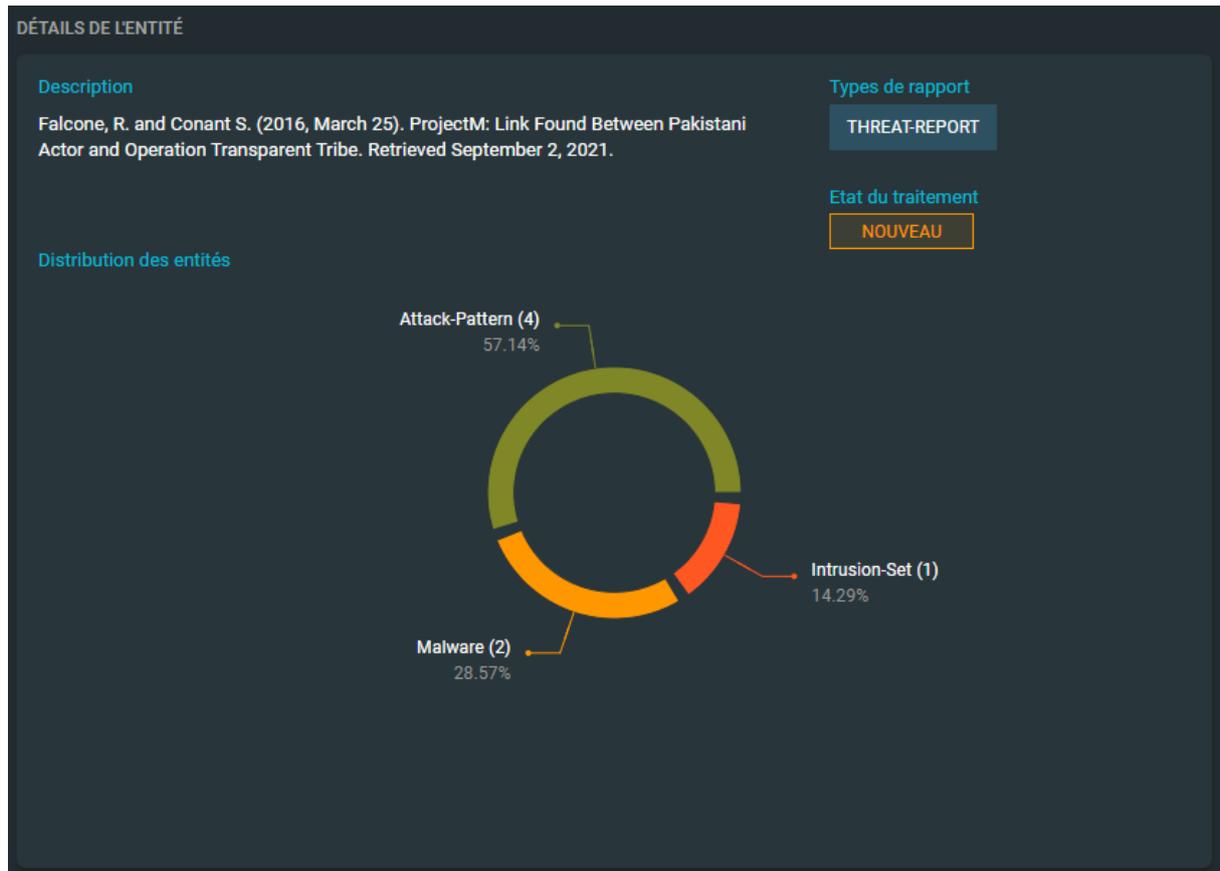
Date de création  
25 mars 2016, 01:00:00

Créateur  
ADMIN

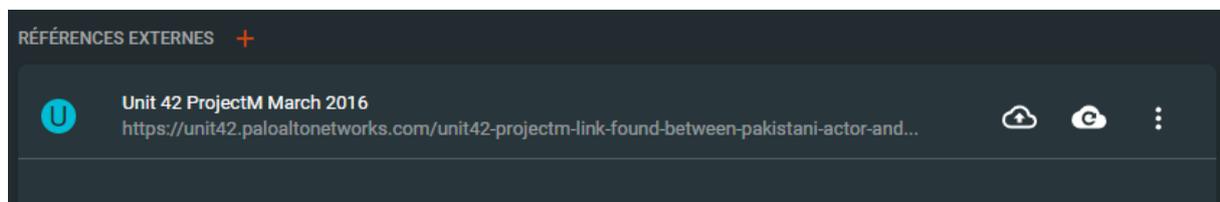
Date de modification  
7 février 2022, 00:11:25

Dans la partie « Détails de l'identité » nous pouvons voir différentes informations :

- Description : un résumé rapide du rapport, ce qui peut être pertinent pour des membres de type RSSI ou personnes souhaitant avoir une information globale du rapport
- Distribution des entités : quels types de données composent le rapport
- Types de rapport : est-ce que c'est un rapport de threat ou un rapport interne
- Etat du traitement : Lié au système de workflow du concept.
  - Pour en savoir plus je vous invite à regarder la démo en live : <https://demo.opencti.io/dashboard/settings/workflow?>

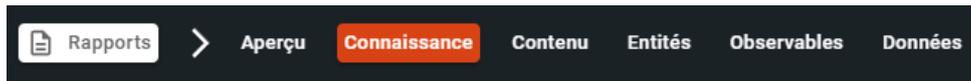


Dans la partie « Références externes » nous pouvons consulter des éléments pour compléter notre étude du rapport :





Explorons désormais la partie « Connaissances » du rapport :

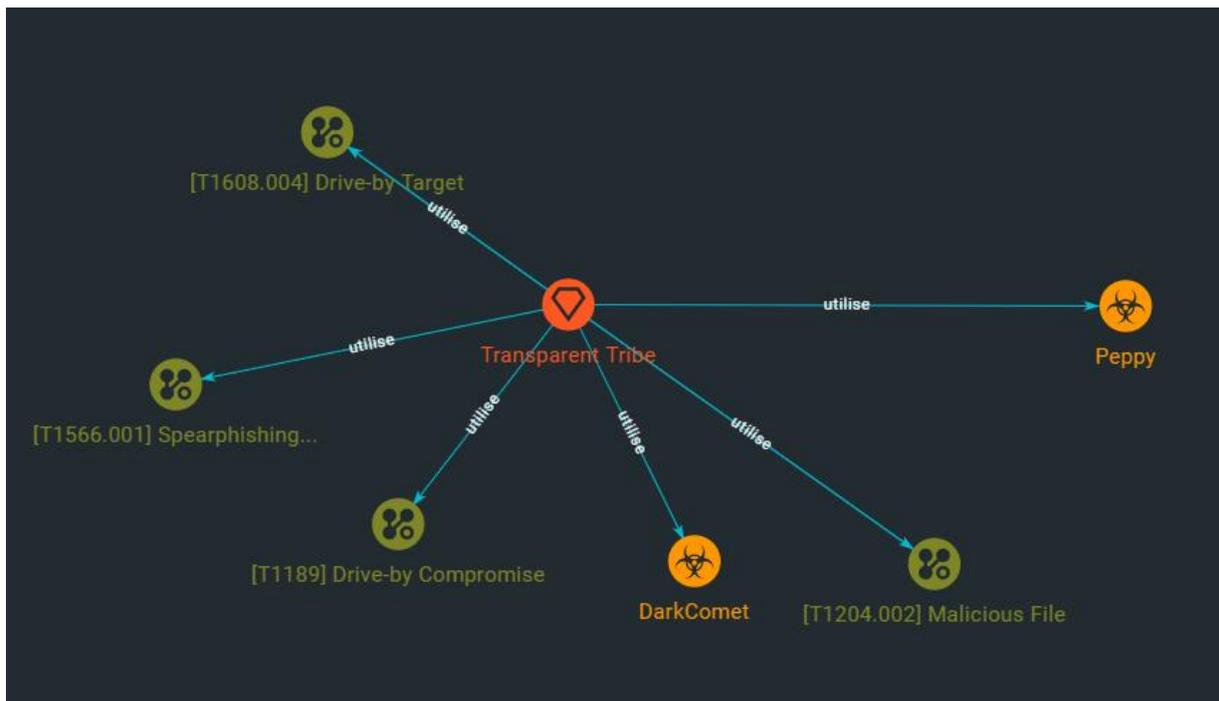


Nous pouvons voir un affichage sous forme de graphe et relations entre les éléments, c'est une manière de représenter les éléments du rapport notamment les IOCs (=Indicator Of Compromise = Indicateurs de compromissions).

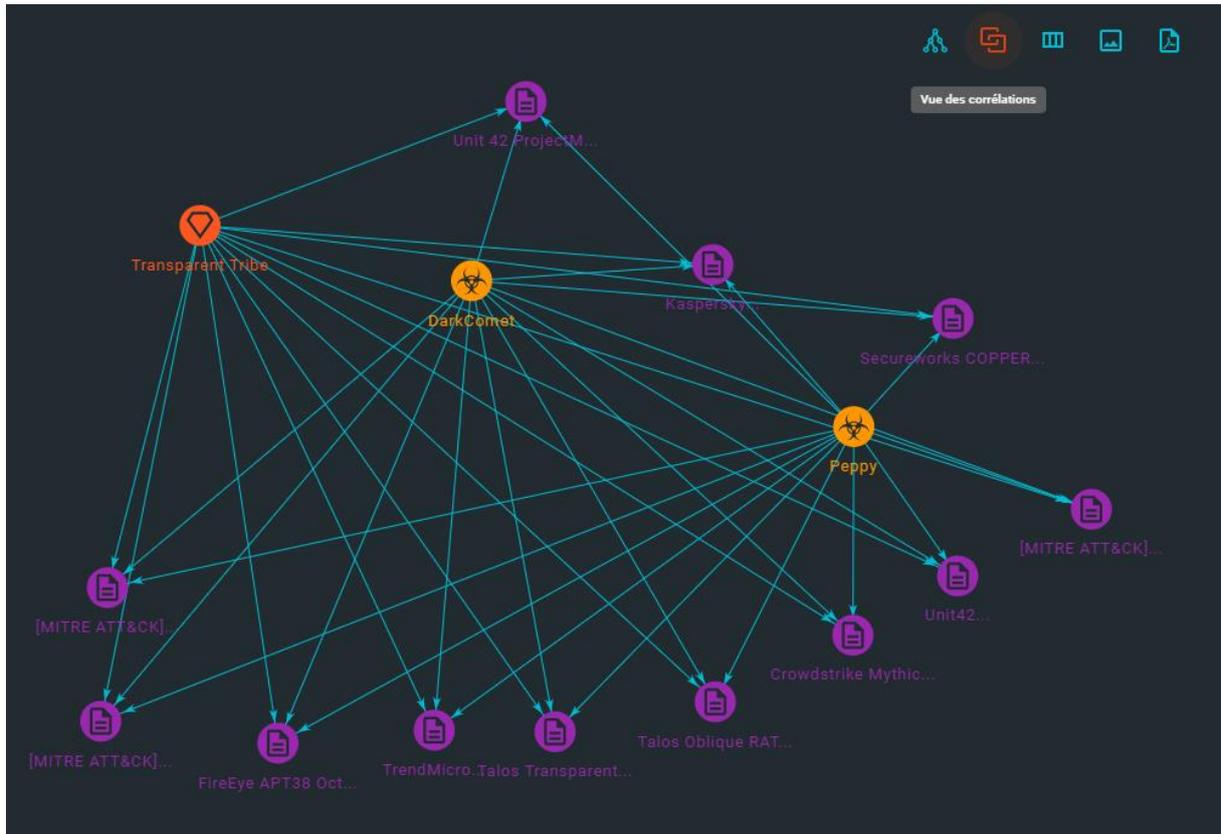
Parmi les éléments présents dans le graphe se trouve « DarkComet », c'est le moment idéal de saluer le bro Jean-Pierre LESUEUR (@darkcodersc) ! You The Best !! ;)



Le graphe étant tout à fait personnalisable, si nous avons du mal à visualiser certains éléments on peut les déplacer à souhait :



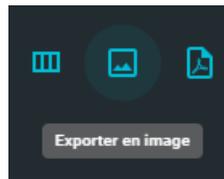
D'autres types de vues permettent d'avoir un visuel des relations de d'autres manières, comme c'est le cas de la « vue des corrélations » ci-dessous :



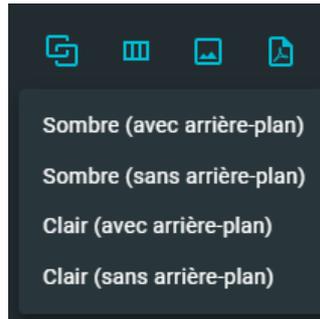
D'un point de vue Blue Team si nous souhaitons avoir comme base la MITRE & ATT&CK nous pouvons avoir le visuel « Tactics matrix view » ainsi les méthodes utilisées sont mises en avant via une couleur différente :

Process	collection 17 techniques	discovery 23 techniques	lateral-movement 11 techniques	command-and-control... 18 techniques	resource-developme... 7 techniques	execution 16 techniques	reconnaissance 10 techniques	exfiltration 9 techniques	initial-access 9 techniques	Tactics matrix view 13 techniques
Adversary-in-the-Middle	Archive Collected Data	Account Discovery	Component Object Model and Distributed COM	Application Layer Protocol	Acquire Infrastructure	Command and Scripting Interpreter	Active Scanning	Automated Exfiltration	Drive-by Compromise	Account Access Removal
Audio Capture	Automated Collection	Application Window Discovery	Exploitation of Remote Services	Commonly Used Port	Compromise Accounts	Component Object Model and Distributed COM	Gather Victim Host Information	Data Transfer Size Limits	Exploit Public-Facing Application	Data Destruction
Browser Bookmark Discovery	Browser Session Hijacking	Browser Bookmark Discovery	Internal Spearphishing	Communication Through Removable Media	Compromise Infrastructure	Container Administration Command	Gather Victim Identity Information	Exfiltration Over Alternative Protocol	External Remote Services	Data Encrypted for Impact
Clipboard Data	Cloud Infrastructure Discovery	Cloud Infrastructure Discovery	Lateral Tool Transfer	Data Encoding	Develop Capabilities	Deploy Container	Gather Victim Network Information	Exfiltration Over C2 Channel	Hardware Additions	Data Manipulation
Data Staged	Cloud Service Dashboard	Cloud Service Dashboard	Remote Service Session Hijacking	Data Obfuscation	Establish Accounts	Graphical User Interface	Gather Victim Org Information	Exfiltration Over Other Network Medium	Phishing	Defacement
Data from Cloud Storage Object	Cloud Storage Object Discovery	Cloud Storage Object Discovery	Remote Services	Dynamic Resolution	Obtain Capabilities	Inter-Process Communication	Phishing for Information	Exfiltration Over Physical Medium	Replication Through Removable Media	Disk Wipe
Data from Configuration Repository	Container and Resource Discovery	Container and Resource Discovery	Shared Webroot	Encrypted Channel	Stage Capabilities	Native API	Search Closed Sources	Exfiltration Over Web Service	Supply Chain Compromise	Endpoint Denial of Service
Data from Information Repositories	Domain Trust Discovery	Domain Trust Discovery	Software Deployment Tools	Fallback Channels	Establish Capabilities	Scheduled Task/Job	Search Open Technical Databases	Scheduled Transfer	Tainted Relationship	Firmware Corruption
Data from Local System	File and Directory Discovery	File and Directory Discovery	Taint Shared Content	Ingress Tool Transfer	Non-Application Layer Protocol	Scripting	Search Open Websites/Domains	Transfer Data to Cloud Account	Valid Accounts	Inhibit System Recovery
Data from Network Shared Drive	Group Policy Discovery	Group Policy Discovery	Use Alternate Authentication Material	Multi-Stage Channels	Non-Standard Port	Shared Modules	Search Victim Owned Websites			Network Denial of Service
Data from Removable Media	Network Service Scanning	Network Service Scanning		Multi-Band Communication	Protocol Tunneling	Software Deployment Tools				Resource Hijacking
Email Collection	Network Share Discovery	Network Share Discovery		Multi-Band Communication	Proxy	Source				Service Stop
Input Capture	Network Sniffing	Network Sniffing		Non-Application Layer Protocol	Remote Access Software	System Services				System Shutdown/Reboot
Screen Capture	Password Policy Discovery	Password Policy Discovery		Protocol Tunneling	Traffic Signaling	User Execution				
	Peripheral Device Discovery	Peripheral Device Discovery		Traffic Signaling	Web Service	Windows Management Instrumentation				

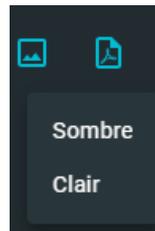
Quel que soit le visuel choisi nous pouvons exporter l'affichage en image :



Nous pouvons choisir parmi les différents types d'exports :

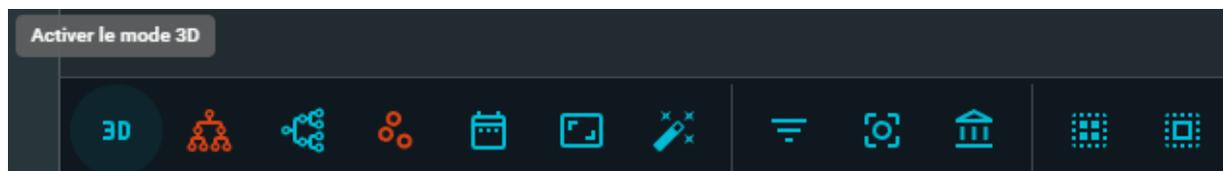


Il est également possible d'exporter le rapport au format PDF :

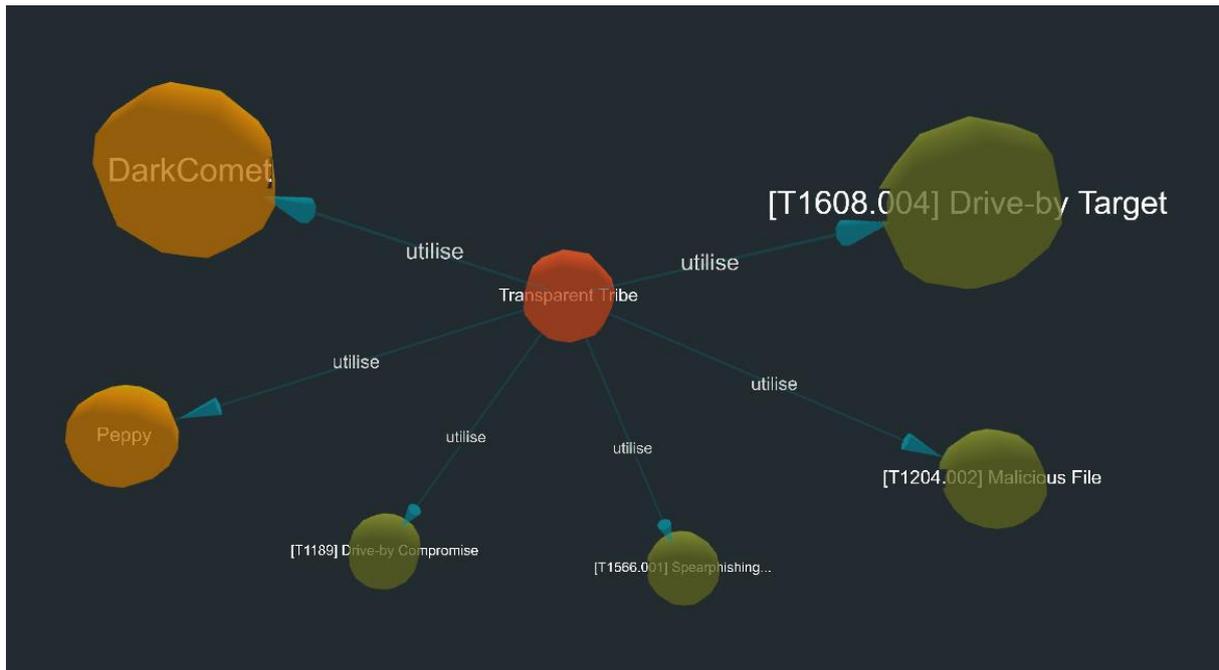


En plus du menu dans la zone supérieure, nous avons le menu de la zone inférieure qui permet d'effectuer d'autres opérations.

Nous pouvons afficher les relations sous forme 3D :



Voici un exemple de résultat qu'on peut obtenir :



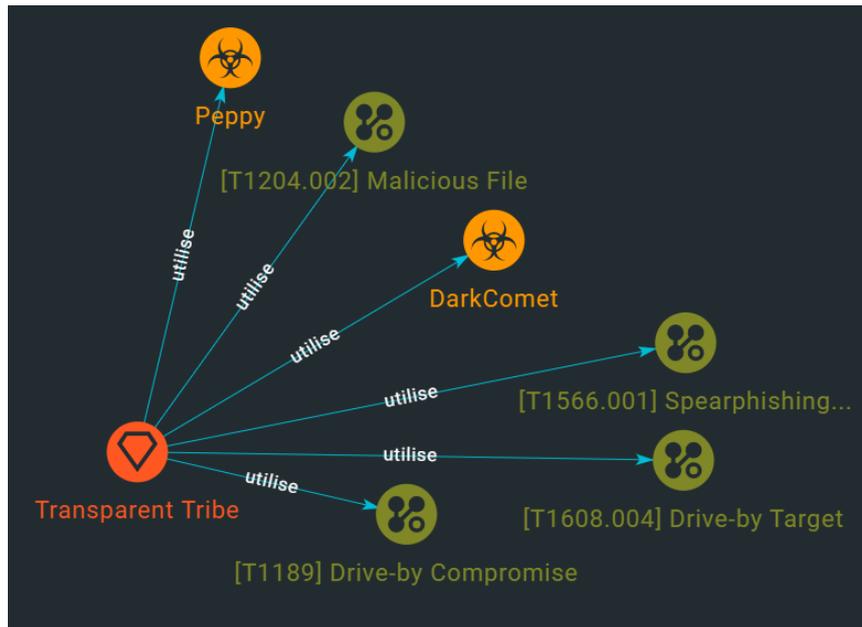
Par défaut le mode « tree » est activé sur les relations mais comme nous l'avons vu plus haut il est possible de changer pour un format plus adapté au besoin.



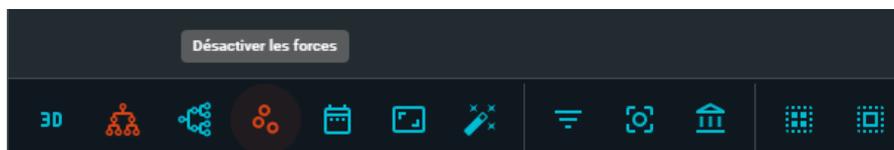
Nous pouvons visualiser les relations avec un modèle vertical :



Voici un exemple de résultat obtenu :



Il est possible de « désactiver les forces » chose que je vous déconseille car si vous déplacez les relations vous risquez de la superposer et puisque cette fonctionnalité n'est pas activée vous risquez de masquer des éléments :

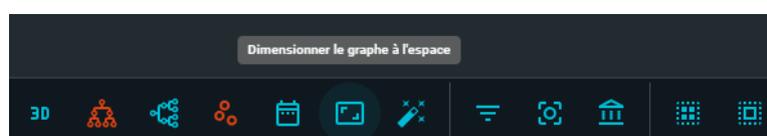


Vous pouvez « Afficher le sélecteur d'intervalle de temps » qui permet de connaître la date exacte d'ajout de chaque élément au rapport !

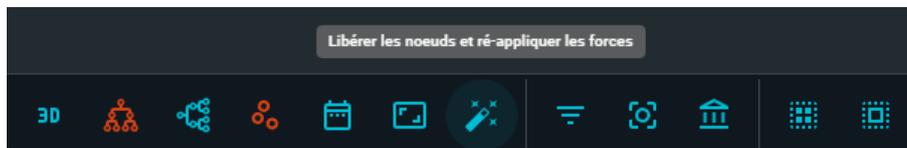
En réalité il est possible de connaître cette date en sélectionnant un élément, mais l'avantage du sélecteur est qu'il affiche un cercle de taille proportionnelle aux changements effectués comme nous pouvons le voir ci-dessous :



Pour adapter l'affichage du graphe sur la fenêtre, on peut opter pour « Dimensionner le graphe à l'espace » ainsi le graphe sera affiché sur toute la fenêtre :

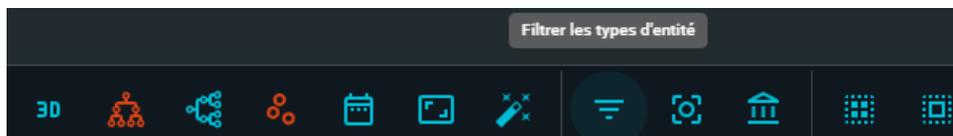


Si vous faites des opérations sur les relations, il se peut que l'affichage de celles-ci ne soit plus à celui d'origine, pour remettre à l'état d'origine les relations nous pouvons choisir d'utiliser la fonctionnalité « Libérer les nœuds et réappliquer les forces » :



Nous pouvons « Filtrer les types d'entité » via ce filtre, voici les trois filtres proposés :

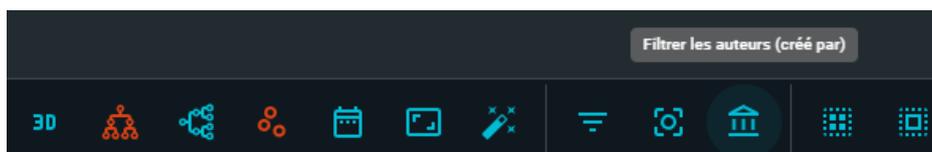
- Code malveillant
- Mode opératoire
- Motif d'attaque



Si vous souhaitez « Filtrer les marquages » vous pouvez le faire via ce filtre, selon les types de marquages du rapport il vous sera possible de ne pas les afficher :

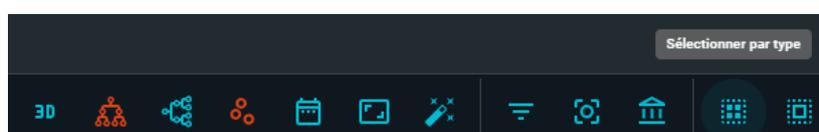


De la même manière que les précédents filtres, il est possible de « Filtrer les auteurs (créé par) » pour afficher ou non les auteurs du rapport :



Il est possible de « Sélectionner par type » les relations, voici les différents types :

- Code malveillant
- Mode opératoire
- Motif d'attaque



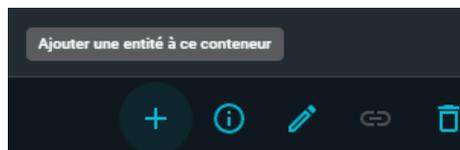
Pour ne pas avoir à sélectionner tous les nœuds un à un ou par types, nous pouvons tous les sélectionner via cette fonctionnalité :



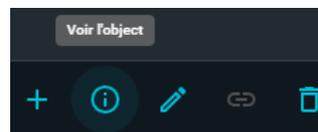
Sur cette page nous avons vu quasiment tous les éléments, il reste les options disponibles dans la zone inférieur droite de la fenêtre lorsque nous sélectionnant un élément du rapport :



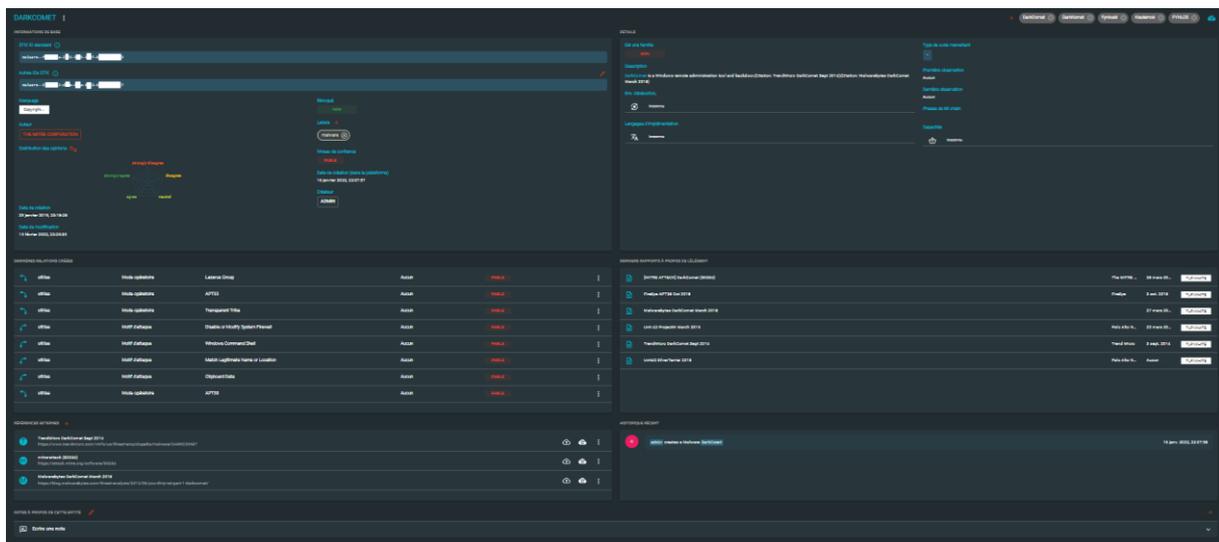
La première option permet d' « Ajouter une entité à ce conteneur » :



La seconde option permet de « Voir l'objet », c'est-à-dire que nous serons redirigés vers une page avec tous les détails de l'élément sélectionné :



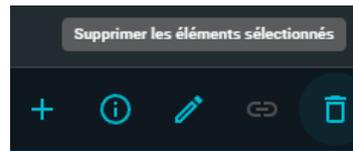
De la même manière qu'un « rapport » nous avons toutes les informations que l'élément :



Si vous sélectionnez au moins deux éléments il vous sera possible de « Créer une relation » entre ces éléments :



La dernière option permet de supprimer un ou plusieurs éléments sélectionnés :

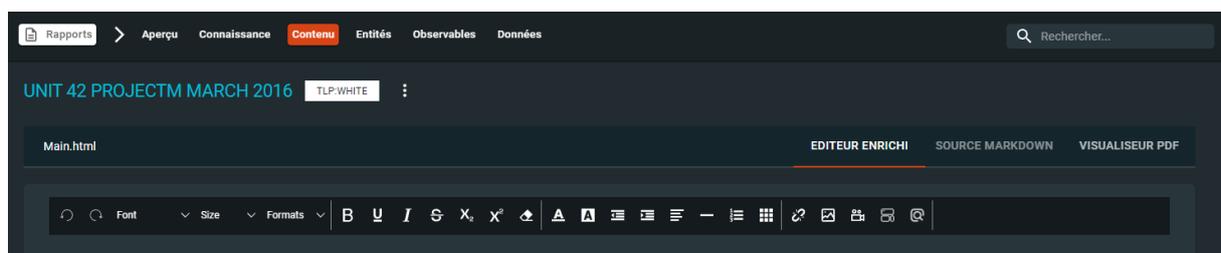


Jusqu'à ce stade nous n'avons parcouru « que » deux sous menus de la partie « Analyses », avec ces éléments nous avons déjà beaucoup d'éléments qui nous permettent de faire notre CTI.

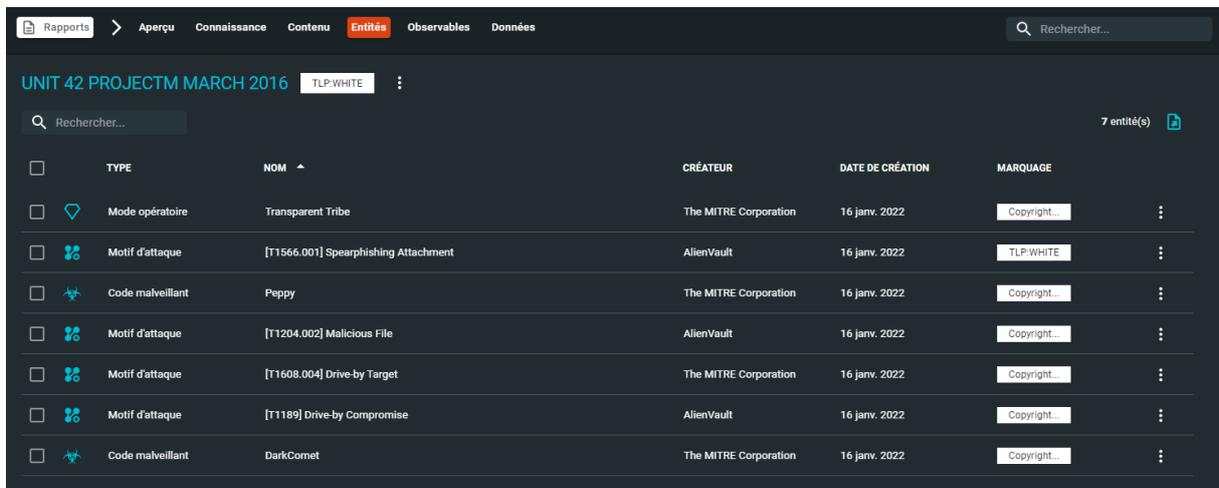
Mais pour compléter notre travail d'autres sous-menus vont nous aider.

Dans le menu « Contenu » nous avons la possibilité d'ajouter du contenu au rapport par différentes méthodes :

- EDITEUR ENRICHI : un éditeur de texte pour ajouter des éléments
- SOURCE MARKDOWN : non actif à cet instant
- VISUALISEUR PDF : non fonctionnel à cet instant

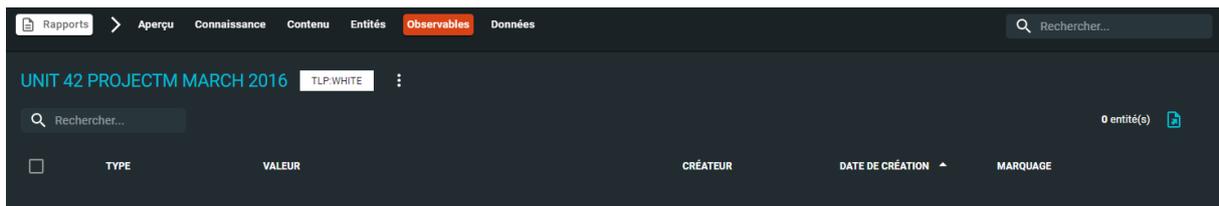


Dans le menu « Entités » nous retrouvons les mêmes informations que précédemment depuis la matrice MITRE ATT&CK ou d'autres visuels des relations car les données sont les mêmes mais représentées différemment :



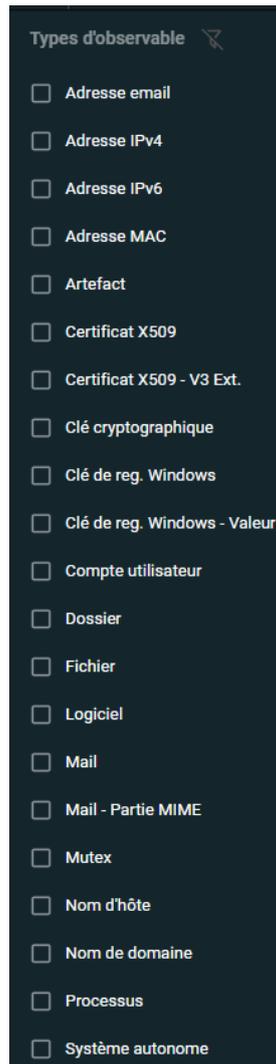
TYPE	NOM	CRÉATEUR	DATE DE CRÉATION	MARQUAGE
Mode opératoire	Transparent Tribe	The MITRE Corporation	16 janv. 2022	Copyright...
Motif d'attaque	[T1566.001] Spearphishing Attachment	AlienVault	16 janv. 2022	TLP-WHITE
Code malveillant	Peppy	The MITRE Corporation	16 janv. 2022	Copyright...
Motif d'attaque	[T1204.002] Malicious File	AlienVault	16 janv. 2022	Copyright...
Motif d'attaque	[T1608.004] Drive-by Target	The MITRE Corporation	16 janv. 2022	Copyright...
Motif d'attaque	[T1189] Drive-by Compromise	AlienVault	16 janv. 2022	Copyright...
Code malveillant	DarkComet	The MITRE Corporation	16 janv. 2022	Copyright...

Dans la partie « Observables » doivent apparaître les éléments en relation avec le rapport :

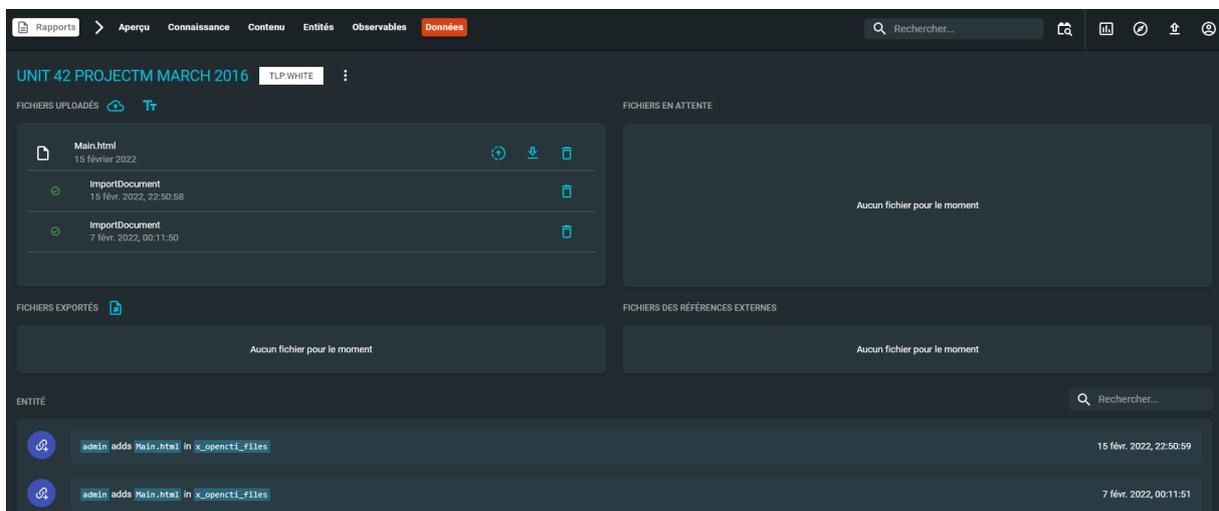


TYPE	VALEUR	CRÉATEUR	DATE DE CRÉATION	MARQUAGE
------	--------	----------	------------------	----------

Ces observables peuvent être de différents types, voici une liste réduite de types d'observables :



Dans le dernier menu « Données » nous pouvons voir les dates des mises à jour des données du rapport :



Au vu des éléments que nous fournissent les rapports de différents types de ressources, si le résultat ne vous satisfait pas il est également possible de créer des rapports manuellement.

Tout comme pour les rapports existants vous pouvez appliquer les mêmes changements sur ces rapports.

Pour cela il faut renseigner les champs suivants :

- Nom : le nom qui sera affiché
- Date de publication : date à laquelle publier le rapport
- Type de rapport : est-ce que c'est un rapport interne ou sur une menace ?
- Confiance : le niveau de confiance accordé entre (aucun, faible, modéré, bon et fort)
- Description : détails qu'on souhaite ajouter au rapport
- Auteur :
  - Quelle entité est à l'origine de ce rapport ?
  - Vous pouvez créer des entités personnalisées comme nous le verrons par la suite
- Labels : labels qui correspondent au rapport
- Marquage : sur quel niveau de du protocole TLP (White, Green, Amber ou Red) se situe la criticité de ce rapport
- Références externes : si vous souhaitez ajouter des références externes pour compléter le rapport

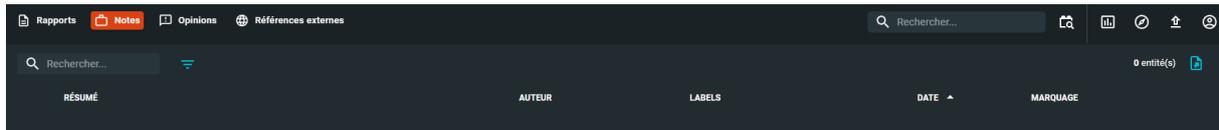
The screenshot shows a dark-themed form titled "Créer un rapport". The form contains the following fields and controls:

- Nom**: A text input field.
- Date de publication**: A date picker showing "2022-02-15" with a calendar icon.
- Type de rapport**: A dropdown menu.
- Confiance**: A dropdown menu with "Faible" selected.
- Description**: A rich text editor with a toolbar containing icons for "Ecrire", "Aperçu", bold (H), italic (I), link, quote, code, list, and table.
- Auteur**: A dropdown menu with a "+" icon.
- Labels**: A dropdown menu with a "+" icon.
- Marquage**: A dropdown menu.
- Références externes**: A dropdown menu with a "+" icon.

At the bottom right, there are two buttons: "ANNULER" (grey) and "CRÉER" (blue).

### 10.3.1.2 Notes

Si vous revenons dans le menu « Notes » nous pouvons visualiser les notes s'il y en a :



Nous pouvons créer des notes en renseignant les champs suivants :

- Date : date de création de la note
- Résumé : descriptif rapide de la note
- Contenu : détails de la note
- Confiance
- Auteur
- Labels
- Marquage

Créer une note

Date  
2022-02-15

Résumé

Contenu

Ecrire Aperçu H B I  $\text{↻}$   $\text{↵}$   $\text{↶}$   $\text{↷}$   $\text{☰}$   $\text{☷}$   $\text{☰☷}$

Confiance  
Faible

Auteur +

Labels +

Marquage

ANNULER CRÉER

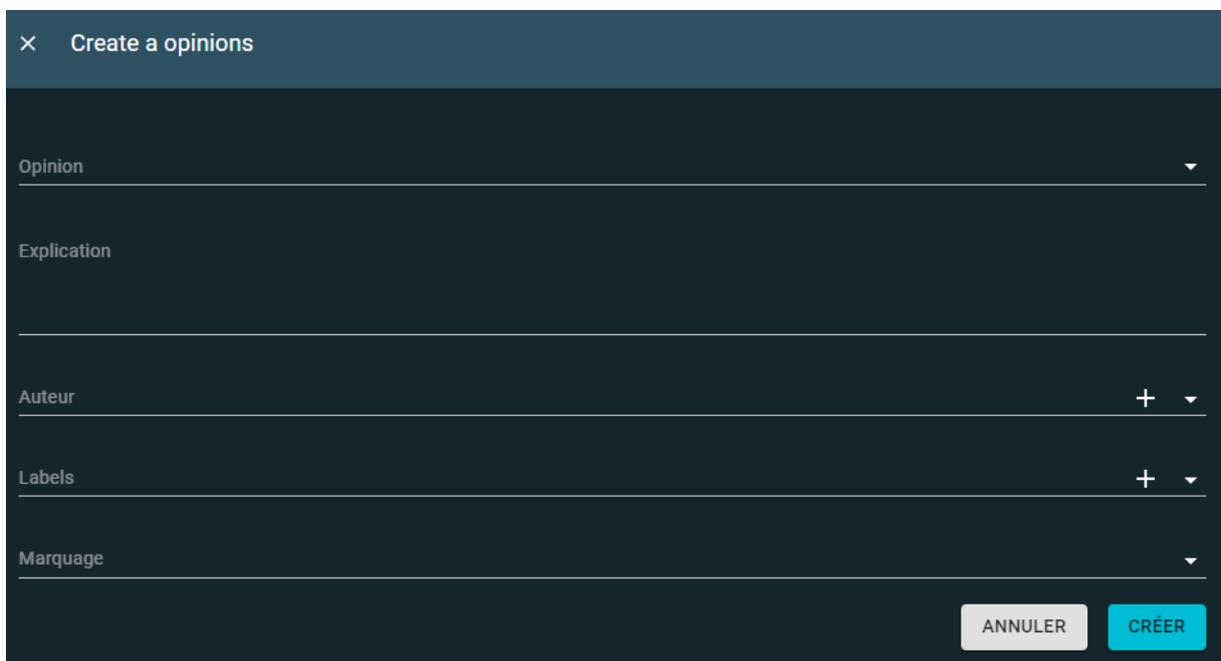
### 10.3.1.3 Opinions

De la même manière que les notes nous pouvons visualiser les « Opinions » dans ce menu :



S'il n'en existe pas nous pouvons en créer en remplissant les champs suivants :

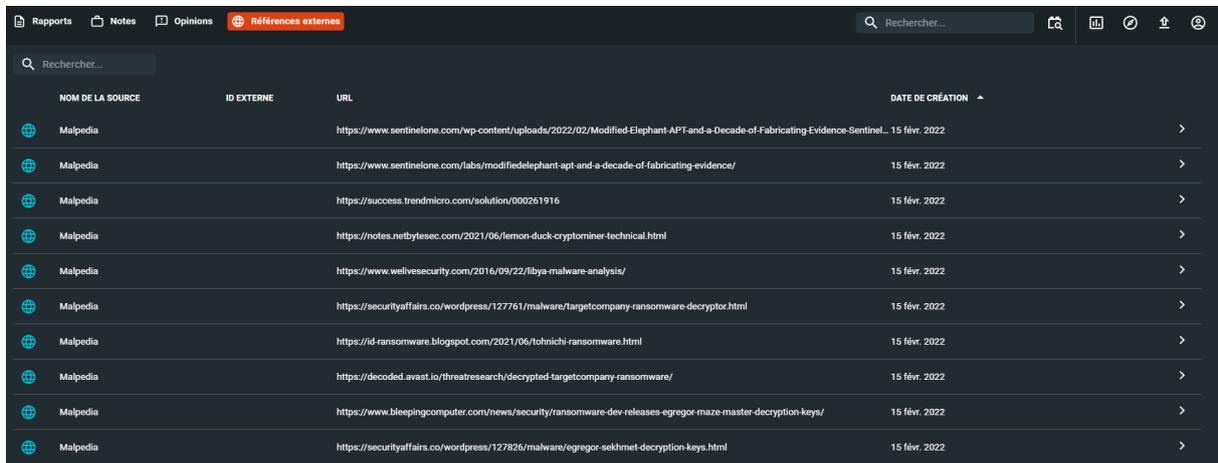
- Opinion : type d'opinion (strongly-disagree, disagree, neutral, agree, strongly-agree)
- Explication : raisons de l'opinion
- Auteur
- Labels
- Marquage

A screenshot of the 'Create a opinions' form in the OpenCTI interface. The form has a dark background and a title bar with a close button and the text 'Create a opinions'. It contains five input fields: 'Opinion' (a dropdown menu), 'Explication' (a text area), 'Auteur' (a text field with a '+' icon and a dropdown arrow), 'Labels' (a text field with a '+' icon and a dropdown arrow), and 'Marquage' (a dropdown menu). At the bottom right, there are two buttons: 'ANNULER' (grey) and 'CRÉER' (blue).

### 10.3.1.4 Références externes

Comme nous l'avons vu précédemment dans les rapports une partie « Références externes » permet de rassembler des liens qui mènent à des ressources pour compléter notre analyse ou servent de sources.

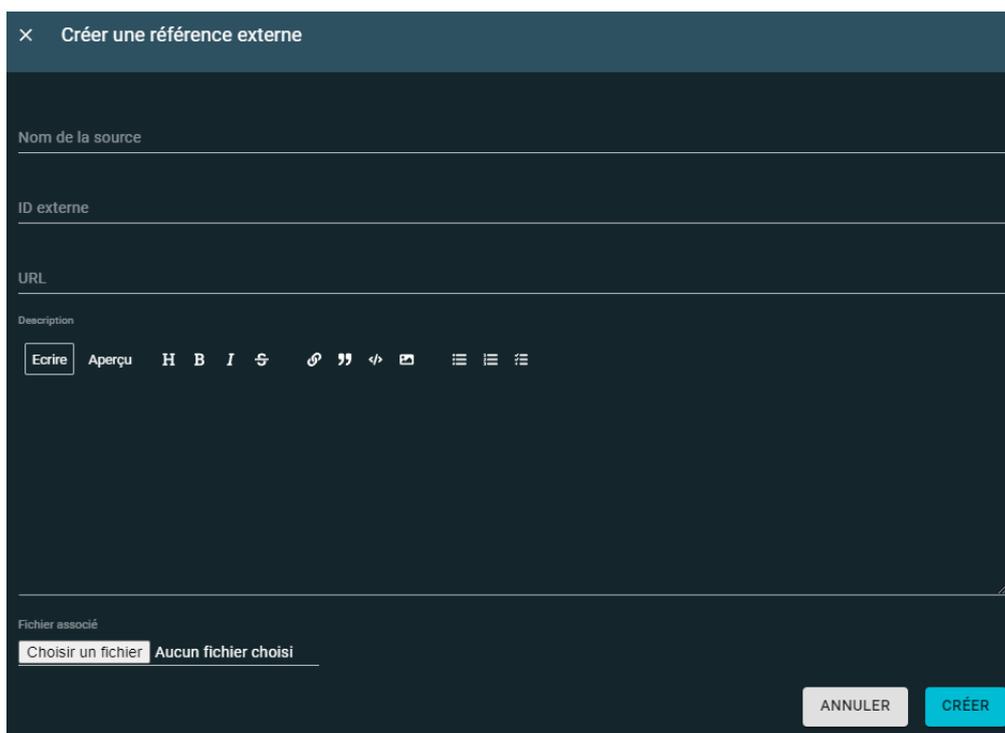
Nous pouvons retrouver ces éléments dans ce menu :



NOM DE LA SOURCE	ID EXTERNE	URL	DATE DE CRÉATION
Malpedia		https://www.sentinelone.com/wp-content/uploads/2022/02/Modified-Elephant-APT-and-a-Decade-of-Fabricating-Evidence-Sentinel...	15 févr. 2022
Malpedia		https://www.sentinelone.com/labs/modifiedelephant-apt-and-a-decade-of-fabricating-evidence/	15 févr. 2022
Malpedia		https://success.trendmicro.com/solution/000261916	15 févr. 2022
Malpedia		https://notes.netbytesec.com/2021/06/lemon-duck-cryptominer-technical.html	15 févr. 2022
Malpedia		https://www.welivesecurity.com/2016/09/22/libya-malware-analysis/	15 févr. 2022
Malpedia		https://securityaffairs.co/wordpress/127761/malware/targetcompany-ransomware-decryptor.html	15 févr. 2022
Malpedia		https://id-ransomware.blogspot.com/2021/06/fohnicchi-ransomware.html	15 févr. 2022
Malpedia		https://decoded.avast.io/threatresearch/decrypted-targetcompany-ransomware/	15 févr. 2022
Malpedia		https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/	15 févr. 2022
Malpedia		https://securityaffairs.co/wordpress/127826/malware/egregor-sekhet-decryption-keys.html	15 févr. 2022

Si vous souhaitez créer une référence manuellement il est tout à fait possible en remplissant les champs suivants :

- Nom de la source : le nom que vous souhaitez donner à cette référence
- ID externe : si vous souhaitez attribuer un identifiant à cette référence
- URL : lien qui mène vers la référence
- Description : détails sur la référence
- Choisir un fichier ... : vous pouvez joindre un fichier



Créer une référence externe

Nom de la source

ID externe

URL

Description

Ecrire Aperçu H B I S ↻ ↶ ↷ ↸ ↹

Fichier associé

Choisir un fichier Aucun fichier choisi

ANNULER CRÉER

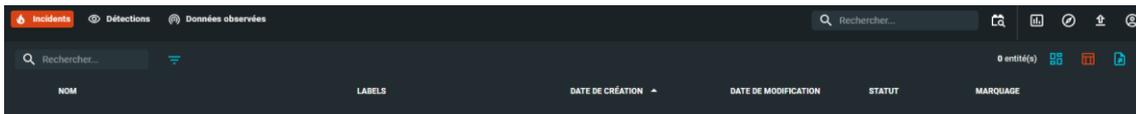
### 10.3.2 Evènements

Les évènements peuvent être de différents types :

- Incidents
- Détections
- Données observées

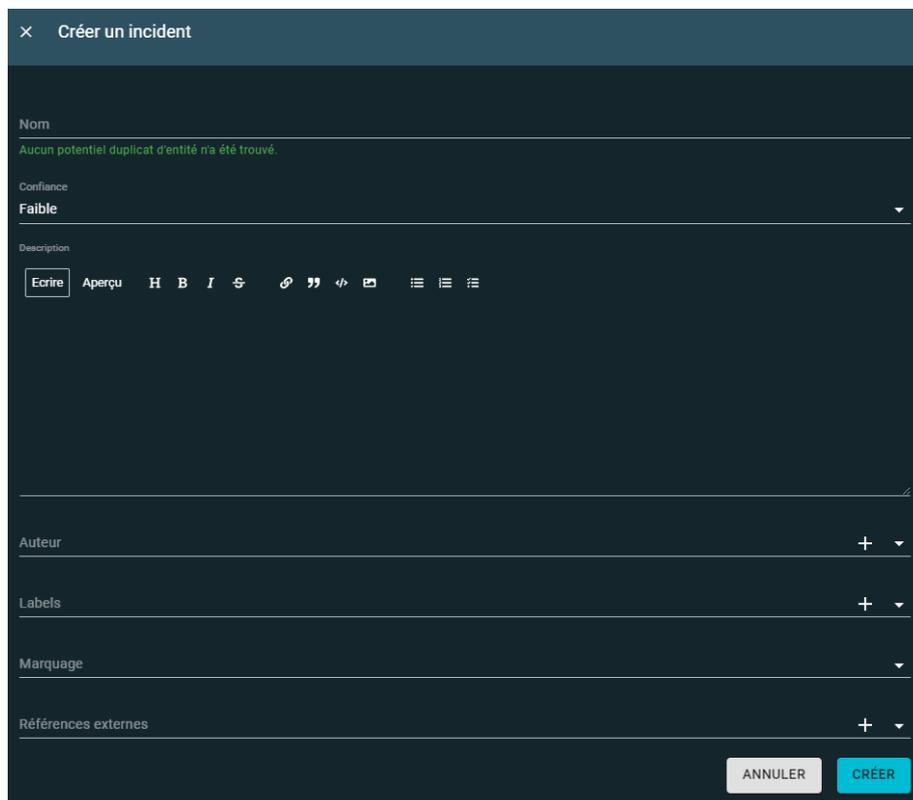


#### 10.3.2.1 Incidents

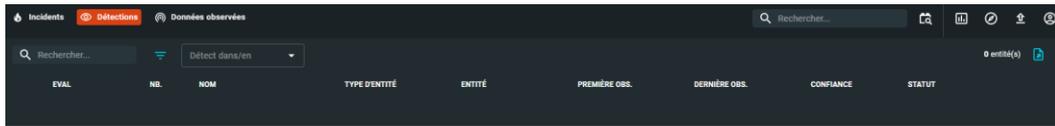


Pour créer un incident il faut remplir les champs suivants :

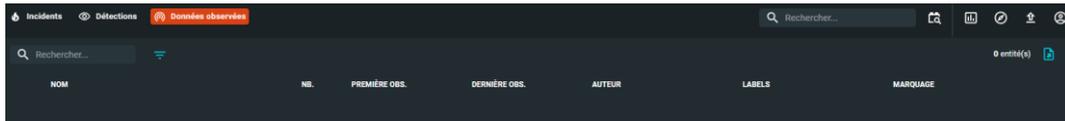
- Nom
- Confiance
- Description
- Auteur
- Labels
- Marquage
- Références externes



### 10.3.2.2 Détections



### 10.3.2.3 Données observées



Pour créer une donnée observée, il faut remplir les champs suivants :

- Entités
- Première observation
- Dernière observation
- Nombre de fois
- Confiance
- Auteur
- Labels
- Marquage
- Références externes

× Créer une donnée observée

Entités ▼

Première observation  
2022-02-15 📅

Dernière observation  
2022-02-15 📅

Nombre de fois  
1

Confiance  
Faible ▼

Auteur + ▼

Labels + ▼

Marquage ▼

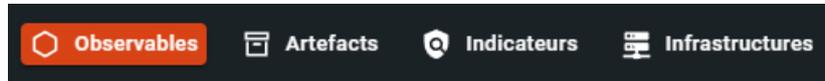
Références externes + ▼

ANNULER CRÉER

### 10.3.3 Observations

Il y a différents types d'observables

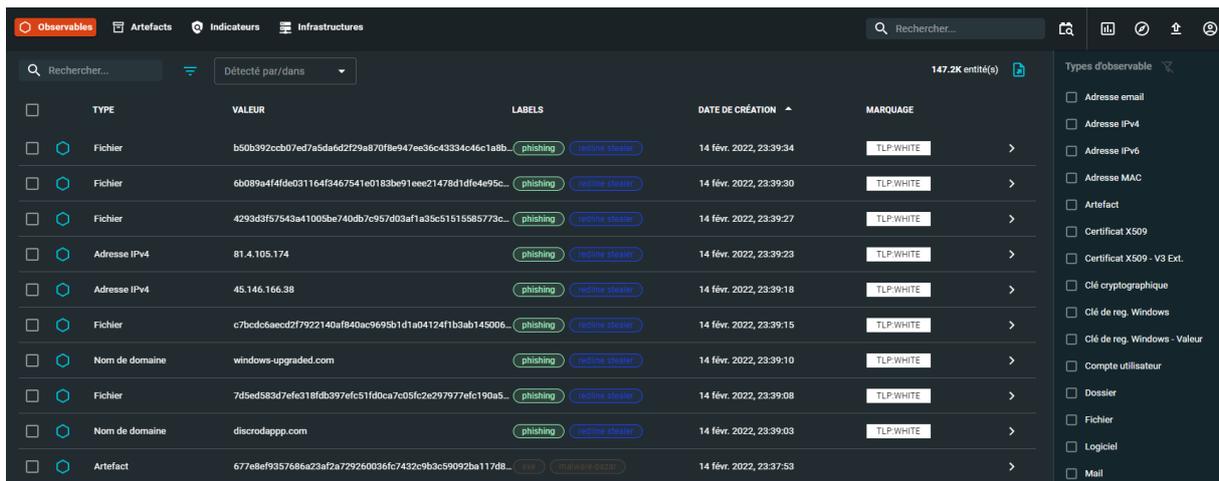
- Observables
- Artefacts
- Indicateurs
- Infrastructures



#### 10.3.3.1 Observables

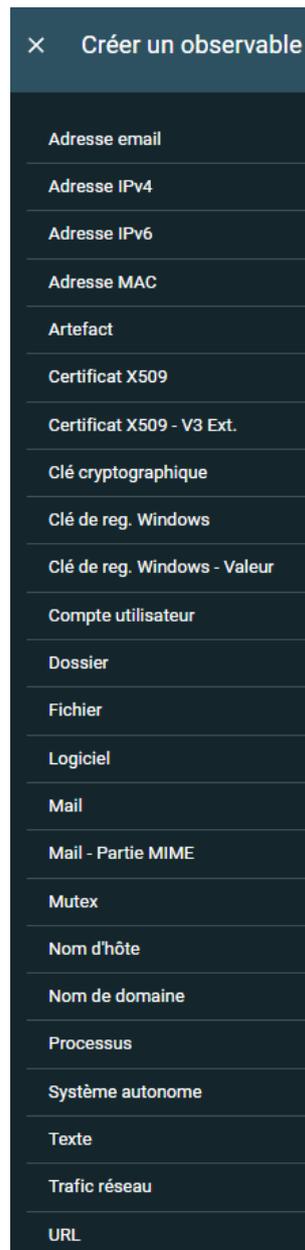
La liste des observables est disponible à cet endroit, on peut les trier via différentes colonnes :

- Type
- Valeur
- Labels
- Date de création
- Marquage



TYPE	VALEUR	LABELS	DATE DE CRÉATION	MARQUAGE
Fichier	b50b392ccb07ed7a5de6d2f29a870f8e947ee96c43334c46c1a8b...	phishing redline stealer	14 fév. 2022, 23:39:34	TLP-WHITE
Fichier	6b089a4f4fde031164f3467541e0183be91eee21478d1dfe4e95c...	phishing redline stealer	14 fév. 2022, 23:39:30	TLP-WHITE
Fichier	4293d3f57543a41005be740db7c957d03af1a35c51515585773c...	phishing redline stealer	14 fév. 2022, 23:39:27	TLP-WHITE
Adresse IPv4	81.4.105.174	phishing redline stealer	14 fév. 2022, 23:39:23	TLP-WHITE
Adresse IPv4	45.146.166.38	phishing redline stealer	14 fév. 2022, 23:39:18	TLP-WHITE
Fichier	c7bcd6aecd2f7922140af840ac9695b1d1a04124f1b3ab145006...	phishing redline stealer	14 fév. 2022, 23:39:15	TLP-WHITE
Nom de domaine	windows-upgraded.com	phishing redline stealer	14 fév. 2022, 23:39:10	TLP-WHITE
Fichier	7d5ed583d7efe318fdb397efc51fd0ca7c05fc2e297977efc190a5...	phishing redline stealer	14 fév. 2022, 23:39:08	TLP-WHITE
Nom de domaine	discrodapp.com	phishing redline stealer	14 fév. 2022, 23:39:03	TLP-WHITE
Artefact	677e8ef9357686a23af2a729260036fc7432c9b3c59092ba117d8...	malware redline stealer	14 fév. 2022, 23:37:53	TLP-WHITE

Voici un extrait de types d'observables :



Pour créer un observable il faut remplir les champs suivants :

- Score
- Description
- Display\_name : nom d'affichage
- Value : la valeur à attribuer
- Auteur
- Labels
- Marquage
- Références externes

× Créer un observable

Score

50

Description

Ecrire Aperçu H B I       

display\_name

value

Auteur + ▾

Labels + ▾

Marquage ▾

Références externes + ▾

Créer un indicateur à partir de cet observable

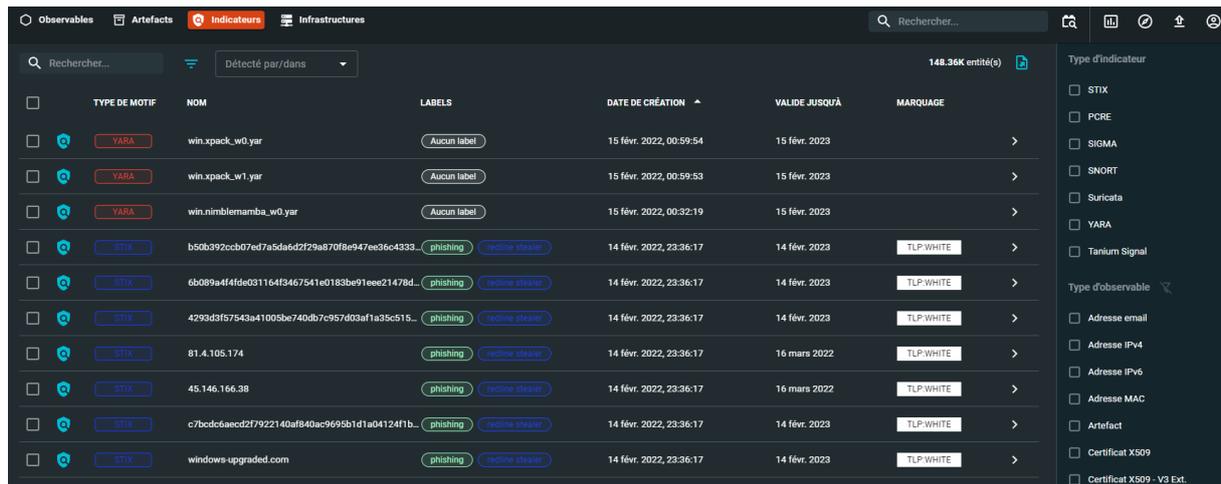
ANNULER CRÉER



### 10.3.3.3 Indicateurs

Les indicateurs peuvent être triés via les colonnes suivantes :

- Type de motif
- Nom
- Labels
- Date de création
- Valide jusqu'à
- Marquage



TYPE DE MOTIF	NOM	LABELS	DATE DE CRÉATION	VALIDE JUSQU'À	MARQUAGE
YARA	win_xpack_w0.yar	Aucun label	15 févr. 2022, 00:59:54	15 févr. 2023	
YARA	win_xpack_w1.yar	Aucun label	15 févr. 2022, 00:59:53	15 févr. 2023	
YARA	win_nimblemamba_w0.yar	Aucun label	15 févr. 2022, 00:32:19	15 févr. 2023	
STIX	b50b392ccb07ed7a5da6d2f29a870f8e947ee35c4333_	phishing, redmine_slack	14 févr. 2022, 23:36:17	14 févr. 2023	TLP:WHITE
STIX	6b089a4f4fde031164f3467541e0183be91eee21478d_	phishing, redmine_slack	14 févr. 2022, 23:36:17	14 févr. 2023	TLP:WHITE
STIX	4293d3f57543a41005be740db7c957d03af1a35c515_	phishing, redmine_slack	14 févr. 2022, 23:36:17	14 févr. 2023	TLP:WHITE
STIX	81.4.105.174	phishing, redmine_slack	14 févr. 2022, 23:36:17	16 mars 2022	TLP:WHITE
STIX	45.146.166.38	phishing, redmine_slack	14 févr. 2022, 23:36:17	16 mars 2022	TLP:WHITE
STIX	c7bcd6aecd27922140af840ac9695b1d1a04124f1b_	phishing, redmine_slack	14 févr. 2022, 23:36:17	14 févr. 2023	TLP:WHITE
STIX	windows-upgraded.com	phishing, redmine_slack	14 févr. 2022, 23:36:17	14 févr. 2023	TLP:WHITE

Il est possible de créer un indicateur en remplissant les champs suivants :

- Nom
- Confiance
- Type de motif
  - STIX
  - PCRE
  - SIGMA
  - SNORT
  - Suricata
  - YARA
  - Tanium Signal
- Type d'observable principal : Parmi une longue liste de choix (adresse email, IPv4, IPv6, Fichier, URL ...)
- Valide depuis
- Valide jusqu'à
- Système d'exploitation
  - Android
  - MacOS
  - Linux
  - Windows

- Description
- Phases de kill chain : sur quelle phase de la cyber kill chain se trouve cet élément
- Auteur
- Labels
- Marquages
- Références externes

× Créer un indicateur

Nom

Confiance  
**Faible**

Type de motif

Motif

Aucun potentiel duplicat d'entité n'a été trouvé.

Type d'observable principal

Valide depuis

Valide jusqu'à

Systèmes d'exploitation

Description

Ecrire Aperçu H B I ↺ ↻ ↶ ↷ ↸ ↹

Phases de kill chain

Auteur +

Labels +

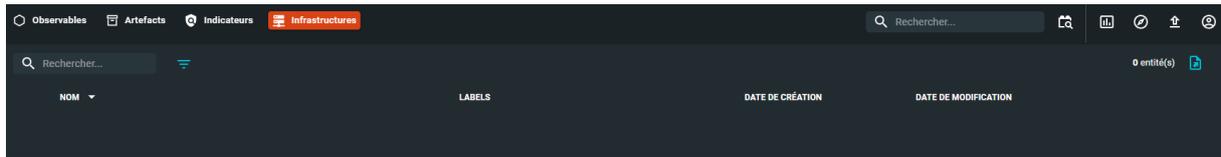
Marquage

Références externes +

Detection

ANNULER CRÉER

### 10.3.3.4 Infrastructures



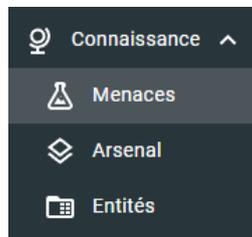
Pour créer une infrastructure il faut remplir les champs suivants :

- Nom
- Description
- Auteur
- Labels
- Marquage
- Références externes

## 10.4 Connaissances

Il y a différents types de connaissances

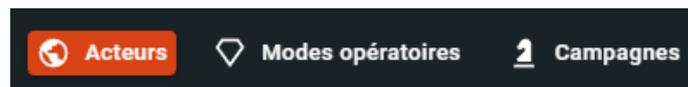
- Menaces
- Arsenal
- Entités



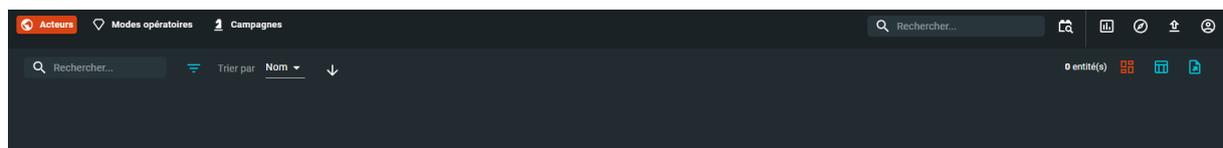
### 10.4.1 Menaces

Il y a différents types de menaces

- Acteurs
- Modes opératoires
- Campagnes



#### 10.4.1.1 Acteurs



Pour créer un acteur il faut remplir les champs suivants :

- Nom
- Type d'acteur : choisir parmi la liste proposée (activiste, concurrent, hacker ...)
- Confiance
- Description
- Auteur
- Labels
- Marquage
- Références externes

✕ Créer un acteur

Nom

Aucun potentiel duplicat d'entité n'a été trouvé.

Type d'acteur

Confiance

Faible

Description

Ecrire Aperçu H B I ↻ 🔗 ” </> 📧 ☰ ☷ ☸

Auteur +

Labels +

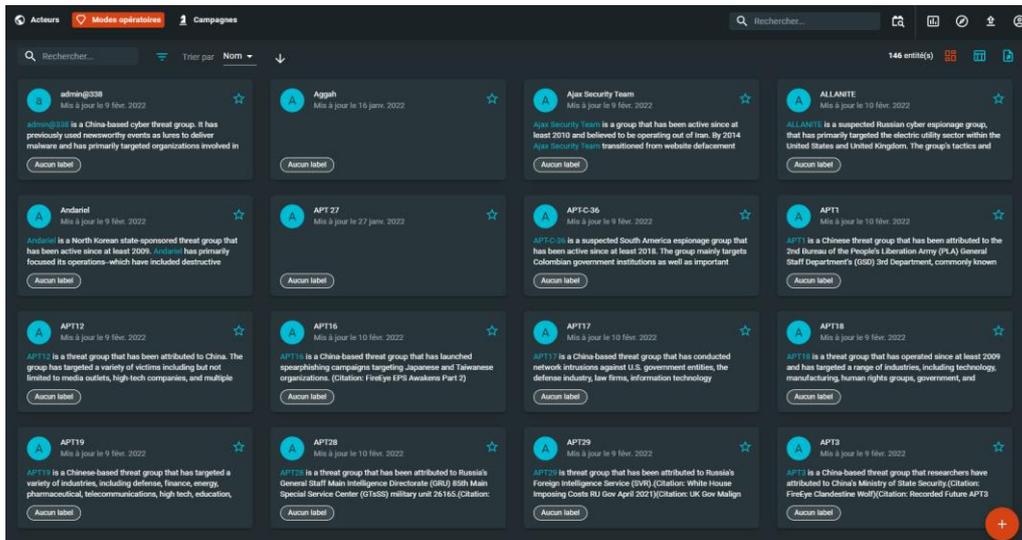
Marquage

Références externes +

ANNULER CRÉER

### 10.4.1.2 Modes opératoires

Les modes opératoires recensent les TTPs utilisés par les différents attaquants, ils sont consultables sous formes de rapports :



Pour créer un mode opératoire il faut remplir les champs suivants :

- Nom
- Confiance
- Description
- Auteur
- Labels
- Marquage
- Références externes

✕ Créer un mode opératoire

Nom

Aucun potentiel duplicat d'entité n'a été trouvé.

Confiance

Faible

Description

Ecrire Aperçu H B I G

Auteur + ▾

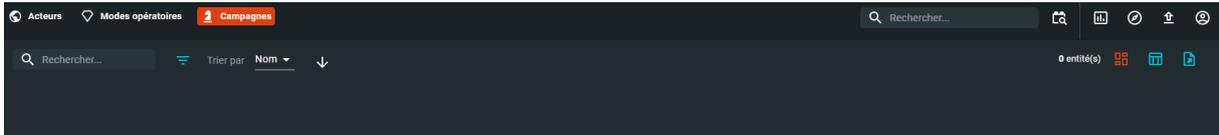
Labels + ▾

Marquage ▾

Références externes + ▾

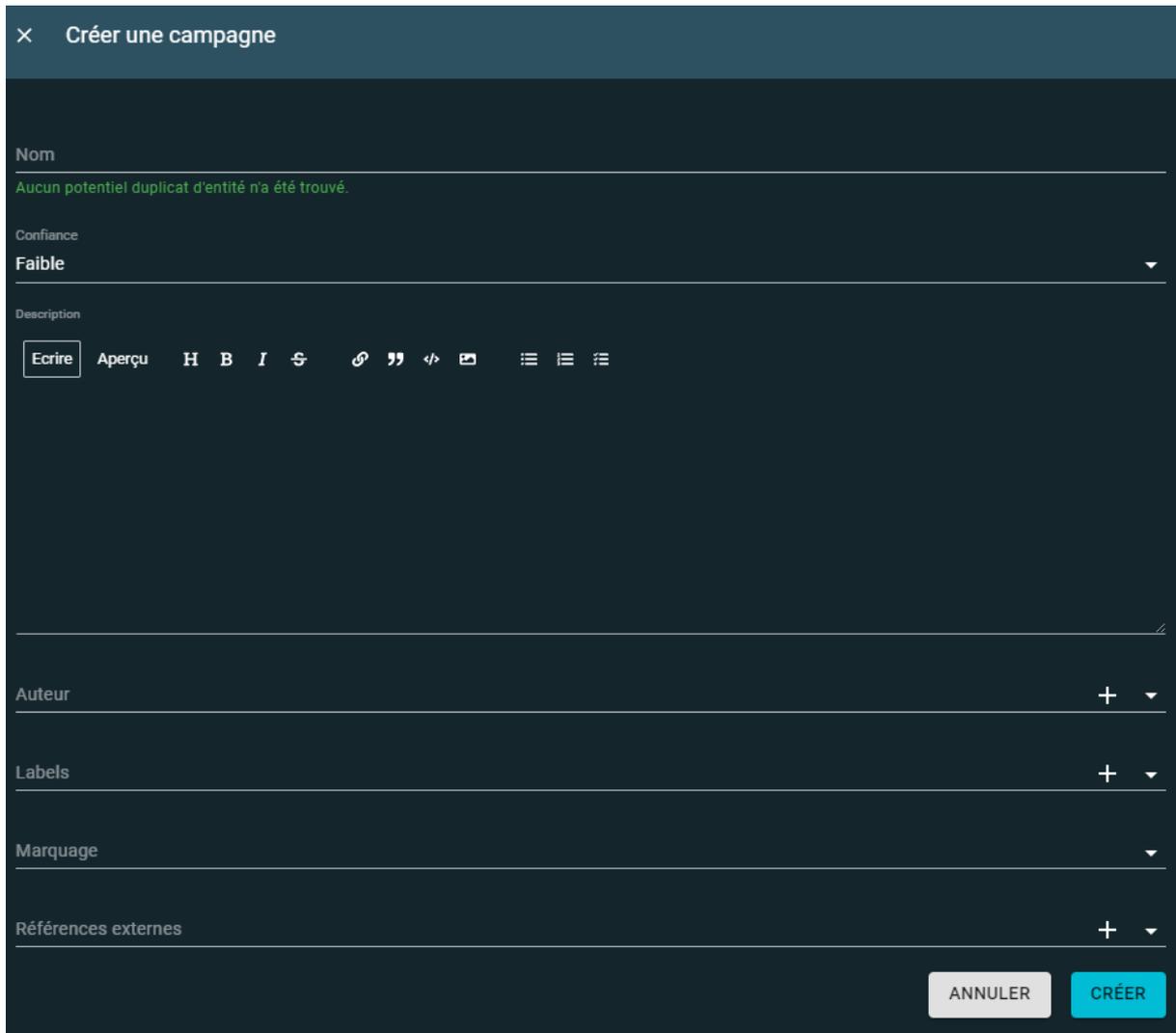
ANNULER
CRÉER

### 10.4.1.3 Campagnes



Pour créer des campagnes il faut remplir les champs suivants :

- Nom
- Confiance
- Description
- Auteur
- Labels
- Marquage
- Références externes



×

## Créer une campagne

Nom

Aucun potentiel duplicat d'entité n'a été trouvé.

Confiance

Faible

Description

Ecrire Aperçu H B I ↺ ↻ ↶ ↷ ↸ ↹

Auteur +

Labels +

Marquage

Références externes +

ANNULER CRÉER

## 10.4.2 Arsenal

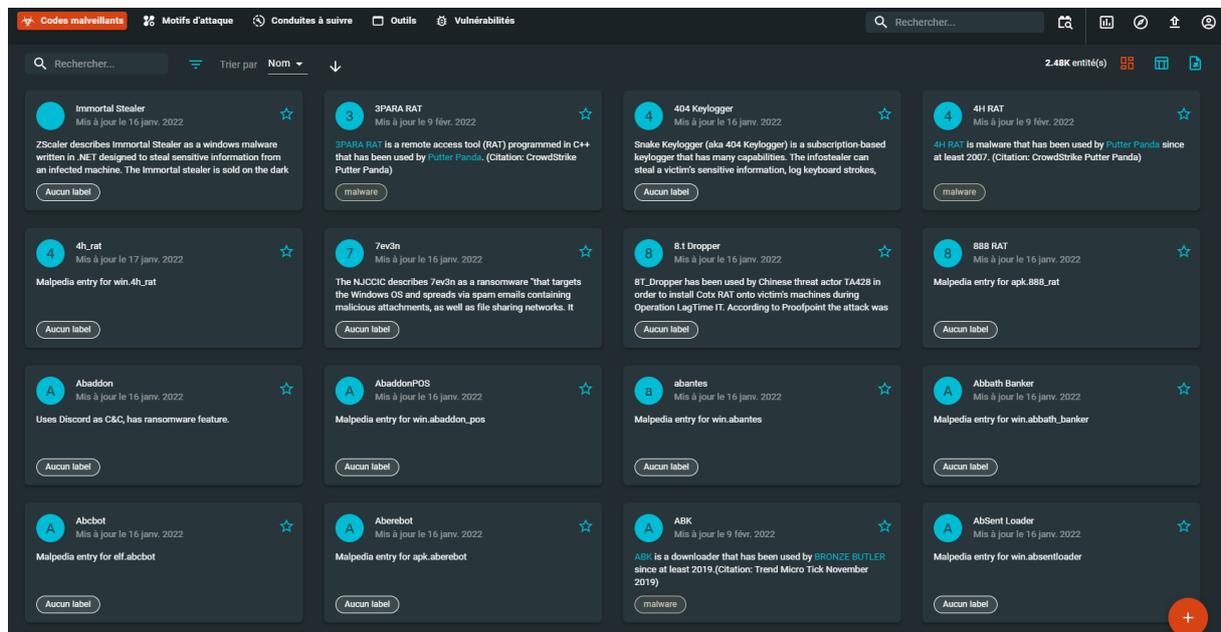
Il y a différents types d'éléments dans la catégorie Arsenal :

- Codes malveillants
- Motifs d'attaque
- Conduites à suivre
- Outils
- Vulnérabilités



### 10.4.2.1 Codes malveillants

Cette catégorie recense les codes utilisés par les acteurs malveillants :



The screenshot displays a grid of 16 malware entries in the OpenCTI interface. Each entry includes a title, a brief description, a source reference, and a date. The entries are:

- Immortal Stealer**: ZScaler describes Immortal Stealer as a windows malware written in .NET designed to steal sensitive information from an infected machine. The Immortal stealer is sold on the dark. (Aucun label)
- 3PARA RAT**: 3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda. (Citation: CrowdStrike Putter Panda) (malware)
- 404 Keylogger**: Snake Keylogger (aka 404 Keylogger) is a subscription-based keylogger that has many capabilities. The info-stealer can steal a victim's sensitive information, log keyboard strokes, (Aucun label)
- 4H RAT**: 4H RAT is malware that has been used by Putter Panda since at least 2007. (Citation: CrowdStrike Putter Panda) (malware)
- 4h\_rat**: Malpedia entry for win.4h\_rat (Aucun label)
- 7ev3n**: The NJCCIC describes 7ev3n as a ransomware "that targets the Windows OS and spreads via spam emails containing malicious attachments, as well as file sharing networks. It (Aucun label)
- 81 Dropper**: 81\_Dropper has been used by Chinese threat actor TA428 in order to install CoR RAT onto victim's machines during Operation LagTime IT. According to Proofpoint the attack was (Aucun label)
- 888 RAT**: Malpedia entry for apk.888\_rat (Aucun label)
- Abaddon**: Uses Discord as C&C, has ransomware feature. (Aucun label)
- AbaddonPOS**: Malpedia entry for win.abaddon\_pos (Aucun label)
- abantes**: Malpedia entry for win.abantes (Aucun label)
- Abbath Banker**: Malpedia entry for win.abbath\_banker (Aucun label)
- Abcbot**: Malpedia entry for elf.abcbot (Aucun label)
- Aberebot**: Malpedia entry for apk.aberebot (Aucun label)
- ABK**: ABK is a downloader that has been used by BRONZE BUTLER since at least 2019. (Citation: Trend Micro Tick November 2019) (malware)
- AbSent Loader**: Malpedia entry for win.absentloader (Aucun label)

Pour ajouter un élément de type code malveillant, il faut remplir les champs suivants :

- Nom
- Type de code malveillant : choisir parmi la liste proposée (adware, backdoor, bot...)
- Confiance
- Description
- Phases de kill chain
- Auteur
- Labels
- Marquage
- Références externes

× Créer un code malveillant

Nom

Aucun potentiel duplicat d'entité n'a été trouvé.

Type de code malveillant

Confiance

Faible

Description

Ecrire Aperçu H B I ↺ ↻ ↶ ↷ ↸ ↹ ↺ ↻ ↶ ↷ ↸ ↹

Phases de kill chain

Auteur +

Labels +

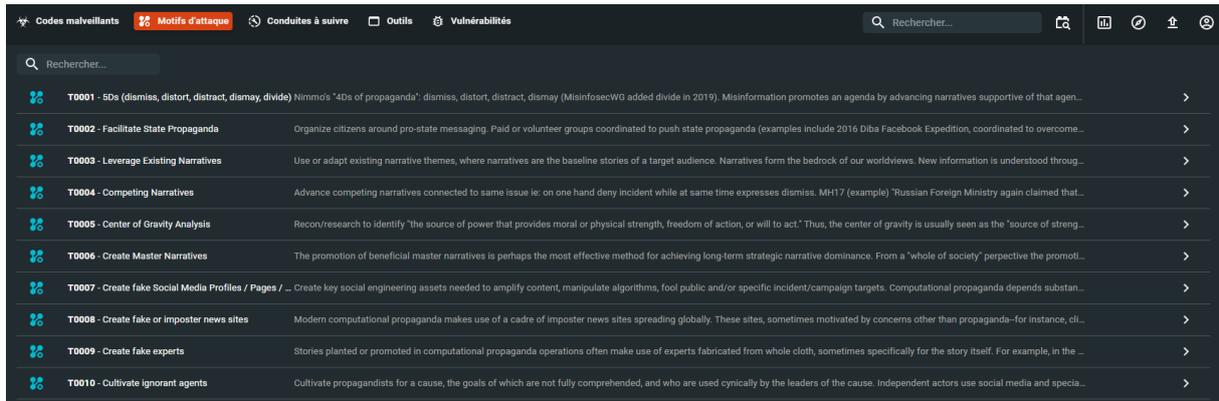
Marquage

Références externes +

ANNULER CRÉER

### 10.4.2.2 Motifs d'attaques

Les motifs d'attaques sont les TTPs présents dans la matrice MITRE ATT&CK :



Pour ajouter un nouveau motif d'attaque il faut remplir les champs suivants :

- Nom
- ID externe : c'est l'identifiant issue de la MITRE ATT&CK de l'élément
  - Par exemple « Active Scanning » correspondant à la référence suivante : <https://attack.mitre.org/techniques/T1595/> et l'ID est « T1595 »
- Description
- Phases de kill chain
- Auteur
- Labels
- Marquage

Créer un motif d'attaque

Nom

Aucun potentiel duplicat d'entité n'a été trouvé.

ID externe

Description

Ecrire Aperçu H B I ↺ ↻ ↶ ↷ ↸ ↹ ↺ ↻ ↶ ↷ ↸ ↹

Phases de kill chain

Auteur + ▾

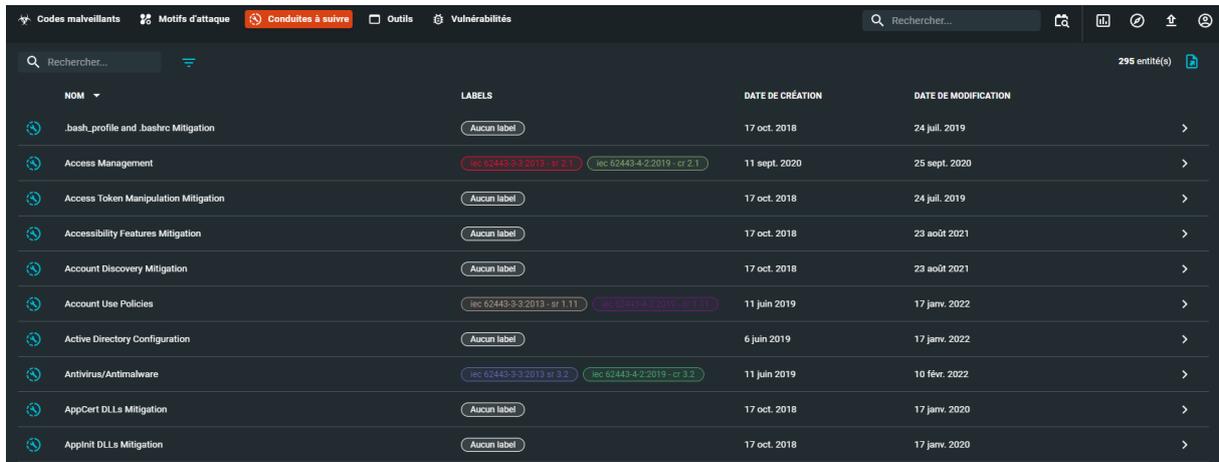
Labels + ▾

Marquage ▾

ANNULER CRÉER

### 10.4.2.3 Conduites à suivre

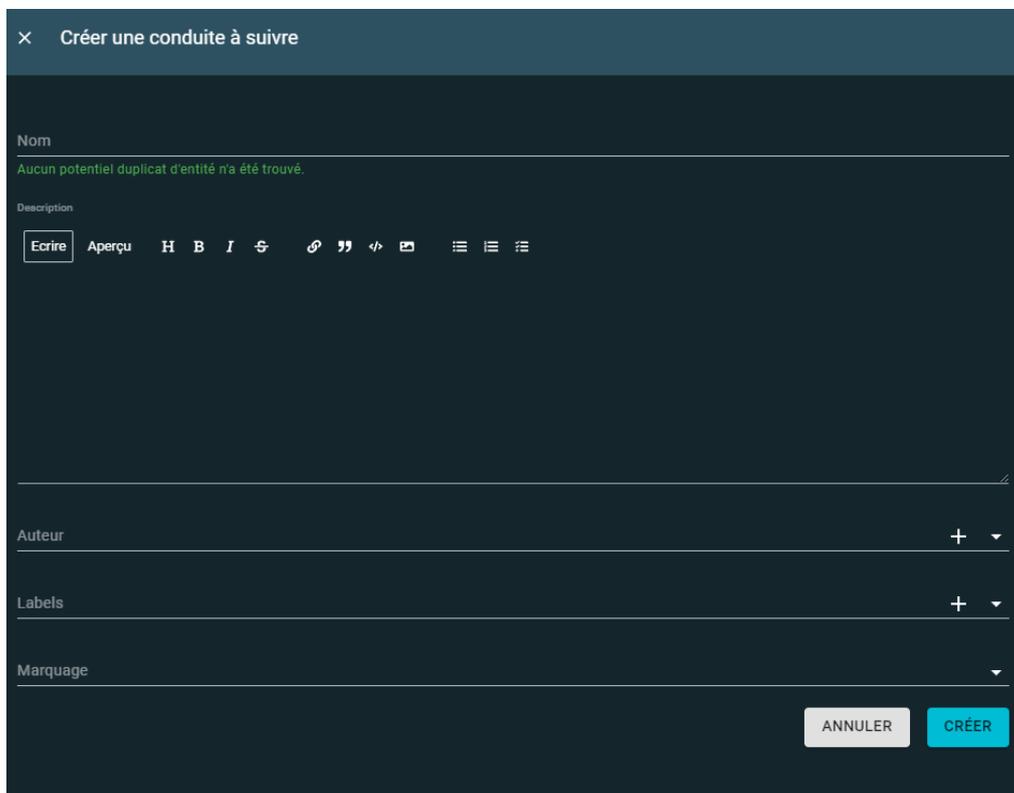
Cette partie très importante pour la partie remédiation permet de proposer des mesures correctives face à des menaces :



NOM	LABELS	DATE DE CRÉATION	DATE DE MODIFICATION
.bash_profile and .bashrc Mitigation	Aucun label	17 oct. 2018	24 juil. 2019
Access Management	lec-62443-3-3-2019 - cr 2.1   lec-62443-4-2-2019 - cr 2.1	11 sept. 2020	25 sept. 2020
Access Token Manipulation Mitigation	Aucun label	17 oct. 2018	24 juil. 2019
Accessibility Features Mitigation	Aucun label	17 oct. 2018	23 août 2021
Account Discovery Mitigation	Aucun label	17 oct. 2018	23 août 2021
Account Use Policies	lec-62443-3-3-2019 - sr 1.11   lec-62443-4-2-2019 - sr 1.11	11 juin 2019	17 janv. 2022
Active Directory Configuration	Aucun label	6 juin 2019	17 janv. 2022
Antivirus/Antimalware	lec-62443-3-3-2019 - cr 3.2   lec-62443-4-2-2019 - cr 3.2	11 juin 2019	10 févr. 2022
AppCert DLLs Mitigation	Aucun label	17 oct. 2018	17 janv. 2020
AppInit DLLs Mitigation	Aucun label	17 oct. 2018	17 janv. 2020

Pour ajouter une conduite à suivre il faut remplir les champs suivants :

- Nom
- Description
- Auteur
- Labels
- Marquage



Créer une conduite à suivre

Nom  
Aucun potentiel duplicat d'entité n'a été trouvé.

Description  
Ecrire Aperçu H B I 

Auteur + ▾

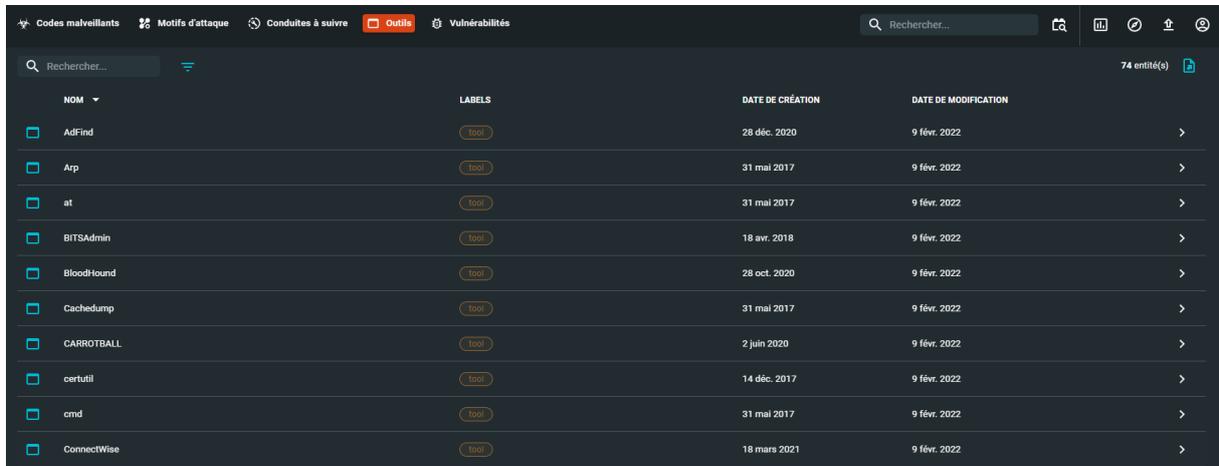
Labels + ▾

Marquage ▾

ANNULER CRÉER

#### 10.4.2.4 Outils

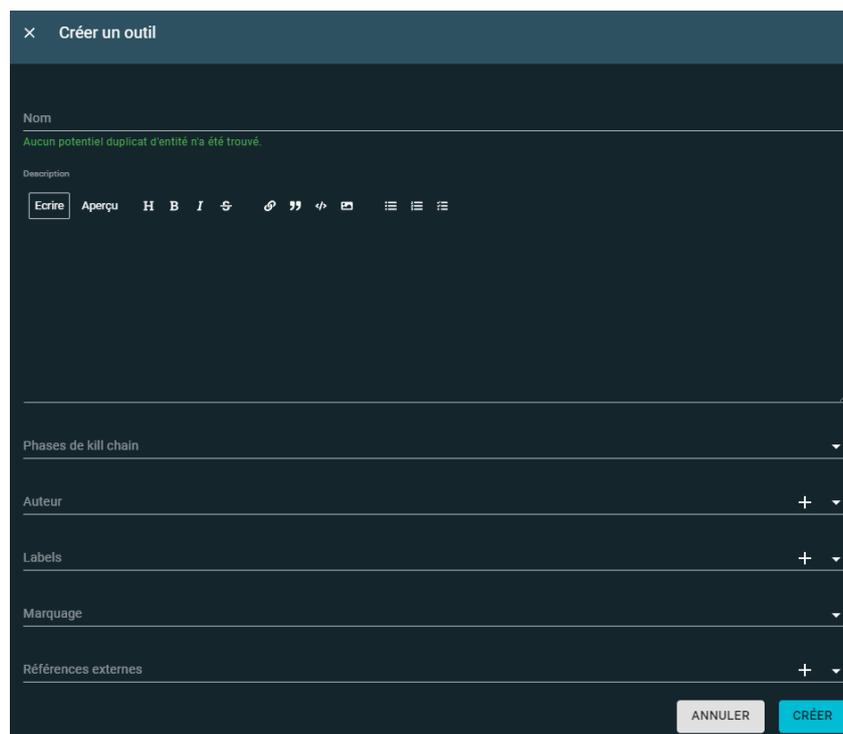
Dans cette partie sont recensés les outils qui ont été trouvés durant les attaques, et une page de rapport leur est dédiée pour donner plus de détails notamment sur les attaques durant lesquels ils ont été détectés / utilisés :



NOM	LABELS	DATE DE CRÉATION	DATE DE MODIFICATION
AdFind	tool	28 déc. 2020	9 févr. 2022
Arp	tool	31 mai 2017	9 févr. 2022
at	tool	31 mai 2017	9 févr. 2022
BITSAdmin	tool	18 avr. 2018	9 févr. 2022
BloodHound	tool	28 oct. 2020	9 févr. 2022
Cachedump	tool	31 mai 2017	9 févr. 2022
CARROTBALL	tool	2 juin 2020	9 févr. 2022
certutil	tool	14 déc. 2017	9 févr. 2022
cmd	tool	31 mai 2017	9 févr. 2022
ConnectWise	tool	18 mars 2021	9 févr. 2022

Pour ajouter un outil il faut remplir les champs suivants :

- Nom
- Description
- Phases de kill chain
- Auteur
- Labels
- Marquage
- Références externes



Créer un outil

Nom

Aucun potentiel duplicat d'entité n'a été trouvé.

Description

Ecrire Aperçu H B I       

Phases de kill chain

Auteur +

Labels +

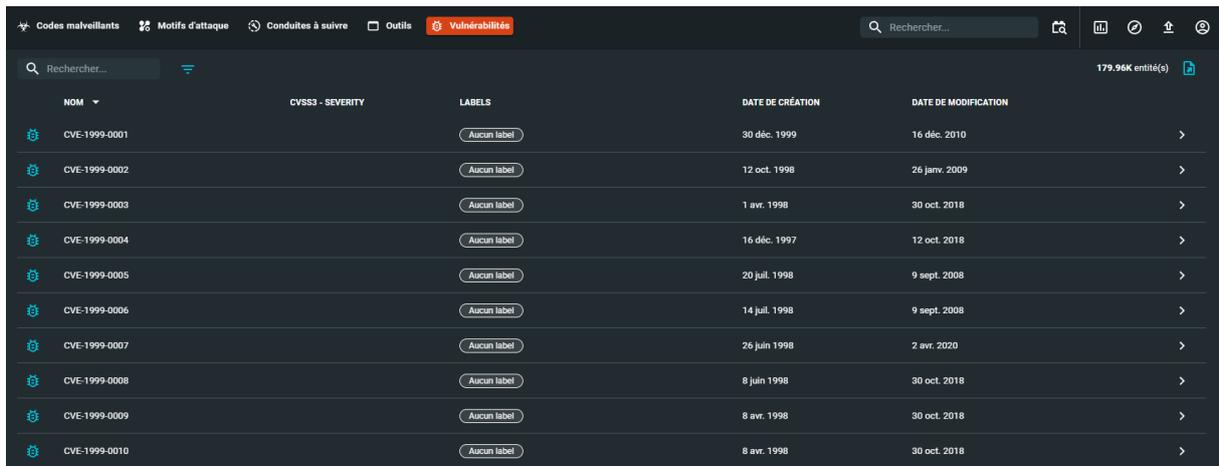
Marquage

Références externes +

ANNULER CRÉER

### 10.4.2.5 Vulnérabilités

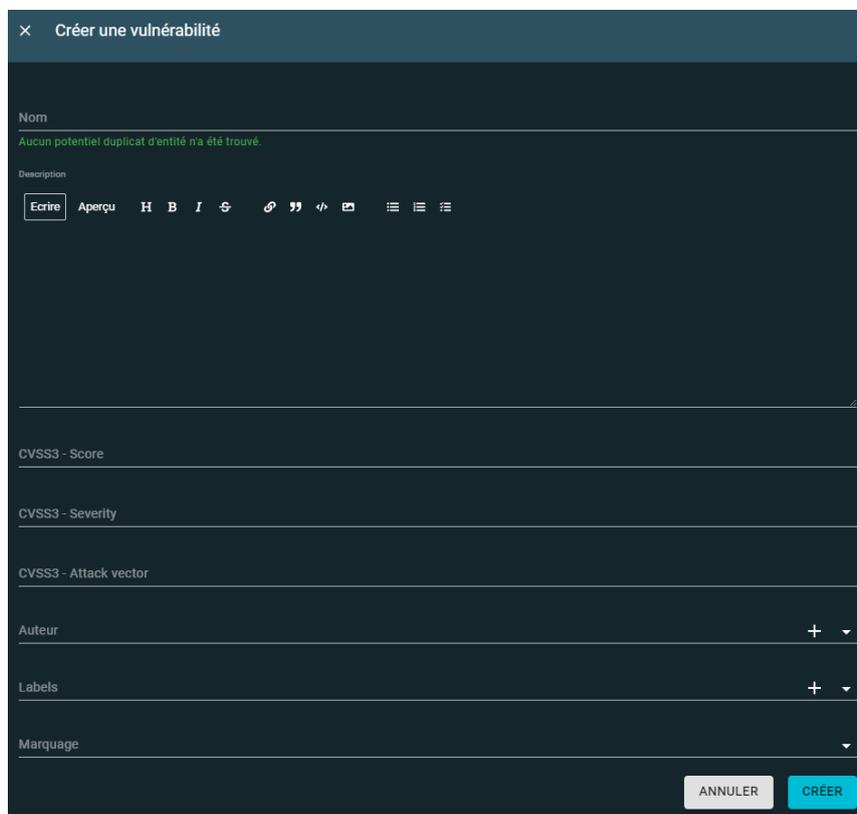
Cette partie recense les vulnérabilités qui ont été exploitées par les attaquants :



NOM	CVSS3 - SEVERITY	LABELS	DATE DE CRÉATION	DATE DE MODIFICATION
CVE-1999-0001		Aucun label	30 déc. 1999	16 déc. 2010
CVE-1999-0002		Aucun label	12 oct. 1998	26 janv. 2009
CVE-1999-0003		Aucun label	1 avr. 1998	30 oct. 2018
CVE-1999-0004		Aucun label	16 déc. 1997	12 oct. 2018
CVE-1999-0005		Aucun label	20 juil. 1998	9 sept. 2008
CVE-1999-0006		Aucun label	14 juil. 1998	9 sept. 2008
CVE-1999-0007		Aucun label	26 juin 1998	2 avr. 2020
CVE-1999-0008		Aucun label	8 juin 1998	30 oct. 2018
CVE-1999-0009		Aucun label	8 avr. 1998	30 oct. 2018
CVE-1999-0010		Aucun label	8 avr. 1998	30 oct. 2018

Pour ajouter une vulnérabilité il faut remplir les champs suivants :

- Nom
- CVSS3 – Score : le score correspondant à la vulnérabilité avec l'échelle CVSS3
- CVSS3 – Severity : le niveau de criticité correspondant à la vulnérabilité avec l'échelle CVSS3
- CVSS3 – Attack vector : le vecteur d'attaque utilisé en se basant sur l'échelle CVSS3
- Auteur
- Labels
- Marquage



Créer une vulnérabilité

Nom

Aucun potentiel duplicat d'entité n'a été trouvé.

Description

Ecrire Aperçu H B I ↺ ↻ ↶ ↷ ↸ ↹

CVSS3 - Score

CVSS3 - Severity

CVSS3 - Attack vector

Auteur + -

Labels + -

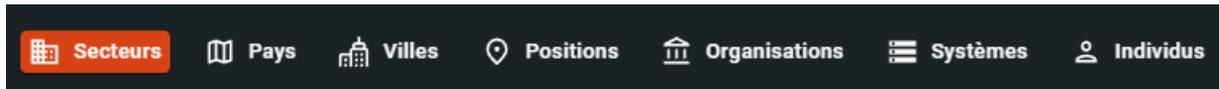
Marquage -

ANNULER CRÉER

### 10.4.3 Entités

Il y a différents types d'entités

- Secteurs
- Pays
- Villes
- Positions
- Organisations
- Systèmes
- Individus



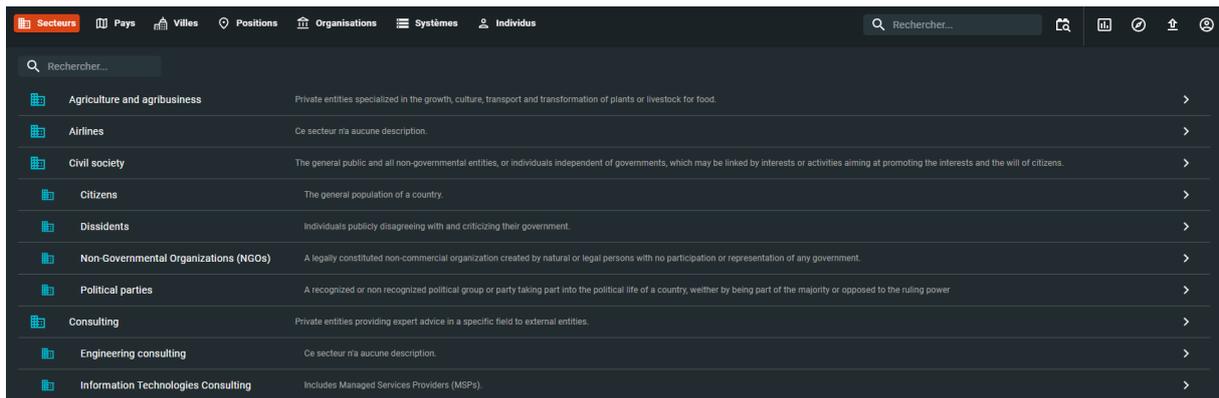
Parmi la liste ci-dessus on peut s'étonner de voir des villes, positions, et mêmes individus !

Tout dépend de votre type de CTI, mais il est tout à fait possible de faire de la veille :

- Sur des villes : si une entreprise possède plusieurs filiales dans le même pays elle peut plus aisément attacher les rapports à chaque ville
- Sur des positions : pour des raisons spécifiques une entreprise peut avoir besoin de localiser de manière précise des positions
- Sur des individus : il n'est pas rare que les équipes cyber / sureté fassent de la veille sur les membres « VIP » d'une entreprise, donc il peut être pertinent de créer dans votre CTI des « individus » et avoir des « rapports » à leur sujet.

#### 10.4.3.1 Secteurs

Une liste de secteurs est par défaut présente dans la plateforme :



Si vous souhaitez ajouter un secteur il faut remplir les champs suivants :

- Nom
- Description
- Auteur
- Marquage
- Références externes

× Créer un secteur

Nom

Aucun potentiel duplicat d'entité n'a été trouvé.

Description

Ecrire Aperçu H B I ↺ ↻ ↵ ↶ ↷ ↸ ↹

Auteur + ▾

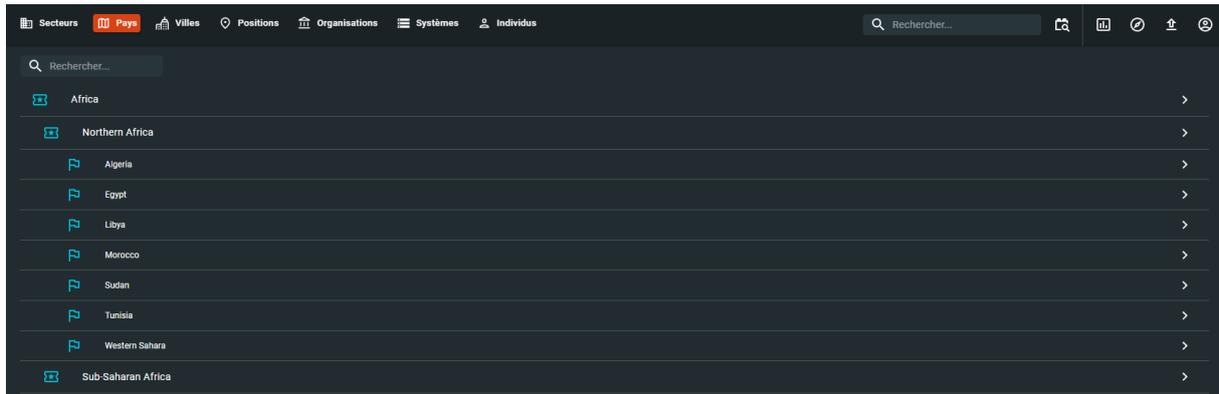
Marquage ▾

Références externes + ▾

ANNULER CRÉER

### 10.4.3.2 Pays

La liste des pays du monde est présente par défaut :



Nous pouvons

- Créer un pays
- Créer une région

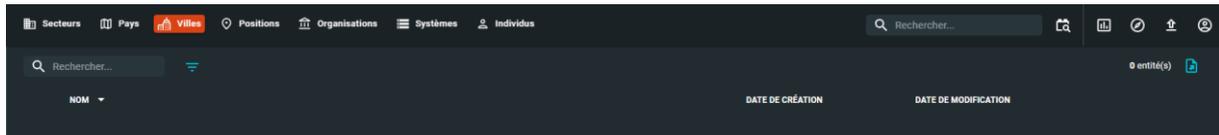


Pour créer un pays il faut remplir les champs suivants :

- Nom
- Description
- Auteur
- Marquage

### 10.4.3.3 Villes

Par défaut il n'y a pas de villes présentes :

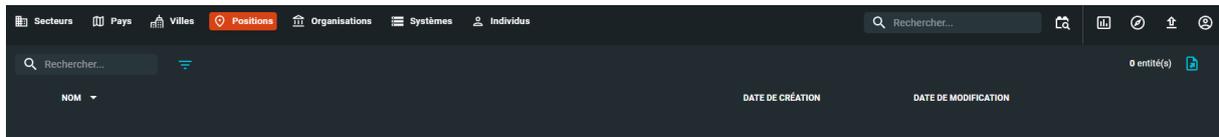


Si vous souhaitez ajouter une ville il faut remplir les champs suivants :

- Nom
- Description
- Latitude
- Longitude
- Auteur
- Marquage
- Références externes

#### 10.4.3.4 Positions

Si ce n'est pas une ville ou un pays alors on peut ajouter une position spécifique via ses coordonnées de latitude et longitude.



Pour ajouter une position il faut remplir les champs suivants :

- Nom
- Latitude
- Longitude
- Auteur
- Marquage
- Références externes

×

### Create a position

Nom

Aucun potentiel duplicat d'entité n'a été trouvé.

Description

Ecrire Aperçu H B I S Link Quote Code List Bulleted List Numbered List

Latitude

Longitude

Auteur + ▾

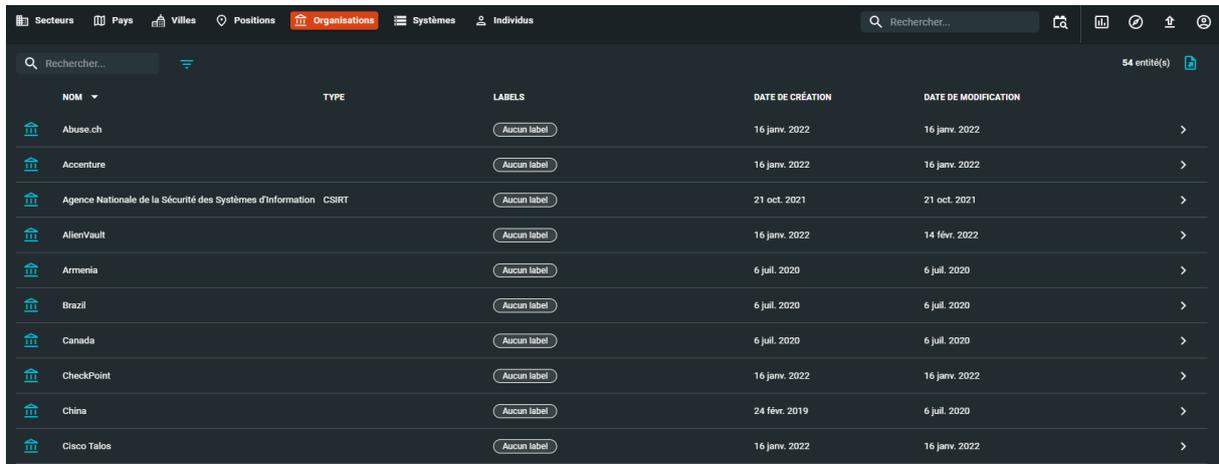
Marquage ▾

Références externes + ▾

ANNULER CRÉER

### 10.4.3.5 Organisations

La liste des organisations s'enrichit en même temps que les autres données lorsque des connecteurs sont ajoutés :

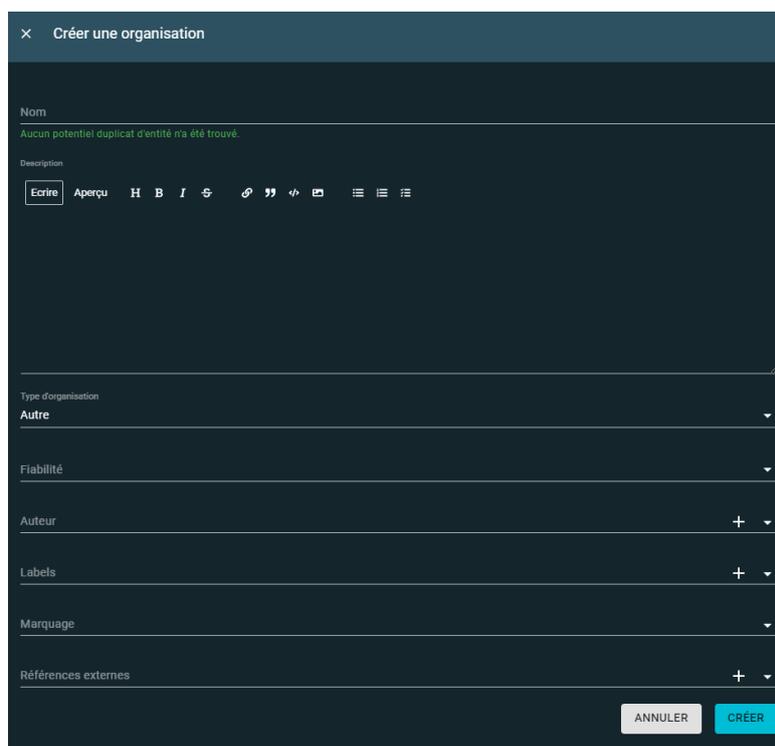


The screenshot shows the OpenCTI interface with the 'Organisations' tab selected. The table displays the following data:

NOM	TYPE	LABELS	DATE DE CRÉATION	DATE DE MODIFICATION
Abuse.ch		Aucun label	16 janv. 2022	16 janv. 2022
Accenture		Aucun label	16 janv. 2022	16 janv. 2022
Agence Nationale de la Sécurité des Systèmes d'Information	CSIRT	Aucun label	21 oct. 2021	21 oct. 2021
AlienVault		Aucun label	16 janv. 2022	14 févr. 2022
Armenia		Aucun label	6 juil. 2020	6 juil. 2020
Brazil		Aucun label	6 juil. 2020	6 juil. 2020
Canada		Aucun label	6 juil. 2020	6 juil. 2020
CheckPoint		Aucun label	16 janv. 2022	16 janv. 2022
China		Aucun label	24 févr. 2019	6 juil. 2020
Cisco Talos		Aucun label	16 janv. 2022	16 janv. 2022

Pour ajouter manuellement une organisation il faut remplir les champs suivants :

- Nom
- Description
- Type d'organisation : choisir parmi la liste proposée (CSIRT, Partenaire, Editeur ...)
- Fiabilité
- Auteur
- Labels
- Marquage
- Références externes

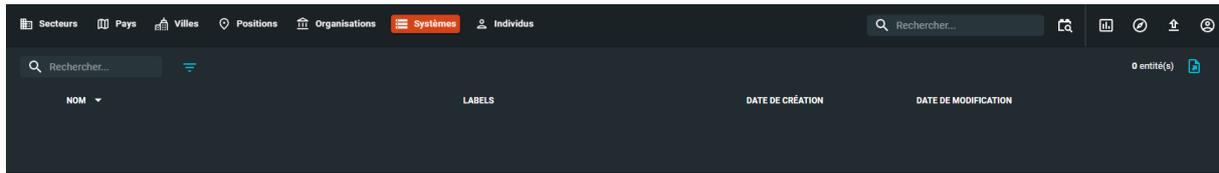


The screenshot shows the 'Créer une organisation' form with the following fields:

- Nom:  (Message: Aucun potentiel duplicat d'entité n'a été trouvé.)
- Description:  (Rich text editor with 'Ecrire' button)
- Type d'organisation:
- Fiabilité:
- Auteur:  (+)
- Labels:  (+)
- Marquage:
- Références externes:  (+)

Buttons: ANNULER, CRÉER

### 10.4.3.6 Systèmes



Pour ajouter un système il faut remplir les champs suivants :

- Nom
- Description
- Auteur
- Labels
- Marquage
- Références externes

Créer un système

Nom

Aucun potentiel duplicat d'entité n'a été trouvé.

Description

Ecrire Aperçu H B I

Auteur + ▾

Labels + ▾

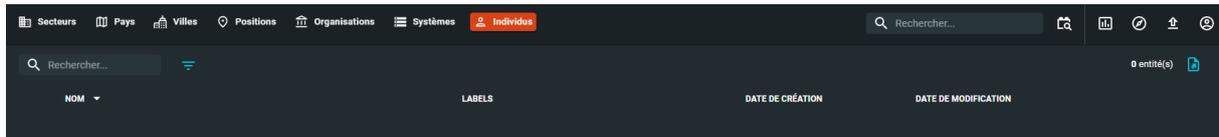
Marquage ▾

Références externes + ▾

ANNULER CRÉER

### 10.4.3.7 Individus

Par défaut il n'y a pas de liste d'individus :



Pour ajouter un individu il faut remplir les champs suivants :

- Nom
- Description
- Auteur
- Labels
- Marquage
- Références externes

## 10.5 Données

Dans ce menu se trouvent différents sous-menus :

- Entités
- Tâches de fond
- Connecteurs
- Synchronisation
- Partage de données
- Collections TAXII



### 10.5.1 Entités

Représente toutes les données de la plateforme sans les relations, afin de pouvoir faire des opérations de masse.

A screenshot of the OpenCTI 'Entités' page. The page shows a table of entities with columns for TYPE, NOM, AUTEUR, LABELS, DATE DE CRÉATION, and MARQUAGE. The table contains 10 rows of data. On the right side, there is a sidebar with 'Types d'entité' and a list of entity types with checkboxes. The top navigation bar shows 'Entités' as the active menu item.

	TYPE	NOM	AUTEUR	LABELS	DATE DE CRÉATION	MARQUAGE
<input type="checkbox"/>	Code malveillant	Incubator	Malpedia	Aucun label	15 févr. 2022	TLP:WHITE
<input type="checkbox"/>	Code malveillant	Lemon Duck	Malpedia	Aucun label	15 févr. 2022	TLP:WHITE
<input type="checkbox"/>	Code malveillant	Book of Eli	Malpedia	Aucun label	15 févr. 2022	TLP:WHITE
<input type="checkbox"/>	Indicateur	win.xpack_w0.yar	Malpedia	Aucun label	15 févr. 2022	
<input type="checkbox"/>	Indicateur	win.xpack_w1.yar	Malpedia	Aucun label	15 févr. 2022	
<input type="checkbox"/>	Code malveillant	TargetCompany	Malpedia	Aucun label	15 févr. 2022	TLP:WHITE
<input type="checkbox"/>	Code malveillant	m0yv	Malpedia	Aucun label	15 févr. 2022	TLP:WHITE
<input type="checkbox"/>	Indicateur	win.nimblemamba_w0.yar	Malpedia	Aucun label	15 févr. 2022	
<input type="checkbox"/>	Rapport	Attackers Disguise RedLine Stealer as a Windows 11 ...	AlienVault	phishing, redline-stealer	14 févr. 2022	TLP:WHITE
<input type="checkbox"/>	Indicateur	b50b392ccb07ed7a5da6d2f29a870f8e947ee36c4333_AlienVault		phishing, redline-stealer	14 févr. 2022	TLP:WHITE

### 10.5.2 Tâches de fond

Les tâches de fond sont consultables depuis ce menu :

A screenshot of the OpenCTI 'Tâches de fond' page. The page shows two sections: 'TÂCHES EN COURS' and 'TÂCHES TERMINÉES'. Both sections display 'Aucune tâche'. The top navigation bar shows 'Tâches de fond' as the active menu item.

TÂCHES EN COURS
Aucune tâche

TÂCHES TERMINÉES
Aucune tâche

### 10.5.3 Connecteurs

Voici un des menus les plus importants de la plateforme ! En effet c'est depuis cet endroit que nous pouvons observer :

- Le nombre de Worker connectés
- Les bundles en attentes
- Les bundles traités
- Les opérations de lecture
- Les opérations d'écriture
- Le nombre total de documents

Mais au-delà de ces informations nous pouvons observer en temps réel la liste et l'état des connecteurs, notamment :

- Les noms des connecteurs
- Le type de connecteur
- Le type de déclenchement
- Le nombre de messages en attente d'import vers notre OpenCTI
- La date de la dernière modification apportée par le connecteur
- Réinitialiser l'état du connecteur
- Supprimer le connecteur

#	NOM	TYPE	DÉCLENCHEMENT AUTOMATIQUE	MESSAGES	MODIFIÉ
1	AMITT	Import de données	NON APPLICAB...	2,66M	15 févr. 2022, 02:19:30
2	Abuse.ch URLhaus	Import de données	NON APPLICAB...	0	15 févr. 2022, 02:19:58
3	AlienVault	Import de données	NON APPLICAB...	0	15 févr. 2022, 02:19:31
4	CAPE	Import de données	NON APPLICAB...	0	15 févr. 2022, 02:19:30
5	Common Vulnerabilities and Exposures	Import de données	NON APPLICAB...	0	15 févr. 2022, 02:19:58
6	Cryptolemus	Import de données	NON APPLICAB...	0	15 févr. 2022, 02:19:30
7	CyberThreatCoalition	Import de données	NON APPLICAB...	0	15 févr. 2022, 02:19:31
8	Cybercrime-Tracker	Import de données	NON APPLICAB...	0	15 févr. 2022, 02:19:58
9	ExportFileCsv	Export de fichiers	NON APPLICAB...	0	15 févr. 2022, 02:19:33
10	ExportFileStix2	Export de fichiers	NON APPLICAB...	0	15 févr. 2022, 02:19:31

Si nous regardons en détails par exemple le connecteur « AlienVault », voici les informations que nous pouvons observer :

- Informations de base :
  - Un état général du connecteur
  - Quel type d'import est effectué ?
  - La date de la dernière mise à jour
- Détails
  - L'état du connecteur avec les paramètres d'horodatage
  - Listen queue : informations techniques liées à rabbitmq
  - Push queue : informations techniques liées à rabbitmq
- Exécution en cours : est-ce que le connecteur est en cours d'exécution ou non, par là il faut comprendre est-ce que le connecteur est en cours d'importation des données vers notre plateforme
- Exécutions terminées :
  - La liste des exécutions
  - Début et fin de l'exécution
  - Le statut
  - Opérations terminées : combien d'éléments ont été importés
  - Nombre total d'opérations : nombre total d'éléments importés
  - Supprimer : si vous souhaitez supprimer la tâche

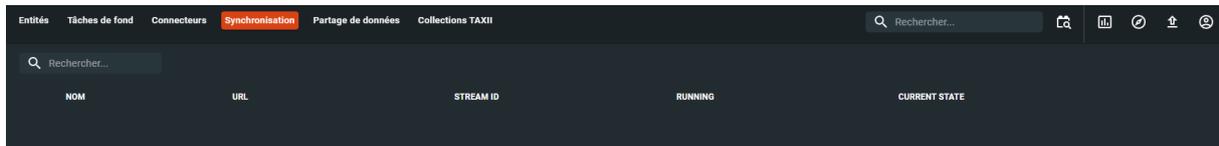
Remarque : en cliquant sur « Erreurs » vous êtes redirigés vers une page qui affichera les détails des erreurs s'il y en a.

The screenshot displays the OpenCTI interface for the AlienVault connector. It is divided into several sections:

- ALIENVAULT ACTIF**: Header indicating the connector's status.
- INFORMATIONS DE BASE**:
  - Type**: EXTERNAL\_IMPORT
  - Dernière mise à jour**: 16 févr. 2022, 01:08:11
  - Seulement contextuel**: NON APPLICAB...
  - Déclenchement automatique**: NON APPLICAB...
  - Paramètre**: alienvault
- DÉTAILS**:
  - Etat**: {"latest\_pulse\_timestamp": "2022-02-15T13:11:0...", "last\_run": "..."} (partially obscured)
  - Listen queue**: listen\_... (partially obscured)
  - Push queue**: push\_... (partially obscured)
- EXÉCUTIONS EN COURS**: Aucune exécution
- EXÉCUTIONS TERMINÉES**:
  - Exécution 1**:
    - Nom: AlienVault run @ 2022-02-15 20:48:10
    - Statut: TERMINE
    - Opérations terminées: 567
    - Nombre total d'opérations: 567
    - 0 ERREURS
    - Début de l'exécution: 15 févr. 2022, 21:48:10
    - Fin de l'exécution: 15 févr. 2022, 22:19:38
    - Progression: [Progress bar]
    - SUPPRIMER
  - Exécution 2**:
    - Nom: AlienVault run @ 2022-02-14 22:36:12
    - Statut: TERMINE
    - Opérations terminées: 95
    - Nombre total d'opérations: 95
    - 0 ERREURS
    - Début de l'exécution: 14 févr. 2022, 23:36:13
    - Fin de l'exécution: 14 févr. 2022, 23:43:02
    - Progression: [Progress bar]
    - SUPPRIMER

### 10.5.4 Synchronisation

Possibilité de se connecter et récupérer des informations en temps réel d'une autre plateforme OpenCTI qui aurait publié un live stream.



Pour créer un synchroniseur il faut remplir les champs suivants :

- Nom
- URL de la plateforme distante
- Token de la plateforme distante
- ID du stream de la plateforme distante

Vous pouvez vérifier si la connexion avec l'hôte distante est fonctionnelle en cliquant sur

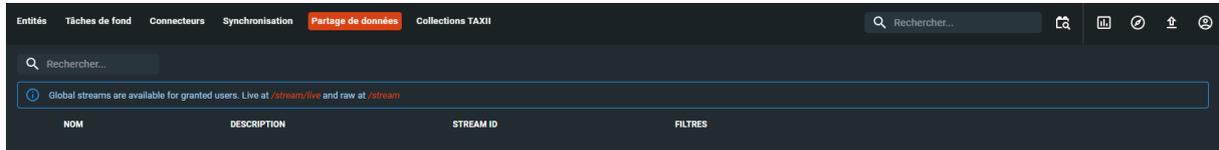
- VÉRIFIER

A screenshot of the 'Créer un synchroniseur' form in the OpenCTI interface. The form has a dark background and a light-colored header with a close button (X) and the title 'Créer un synchroniseur'. The form contains several input fields: 'Nom', 'URL de la plateforme distante', 'Token de la plateforme distante', and 'ID du stream de la plateforme distante'. The 'live' checkbox is checked. There are two toggle switches: 'Vérifier le certificat SSL' (unchecked) and 'Prendre en compte les suppressions' (unchecked). At the bottom right, there are three buttons: 'ANNULER' (disabled), 'VÉRIFIER' (active), and 'CRÉER' (disabled).

### 10.5.5 Partage de données

Par défaut deux types de streams de données sont disponibles :

- `/stream/live` : pour les données « traitées »
- `/stream` : pour les données au format « brute »



Voici un exemple de « stream live » :

```
event: connected
data: {"lastEventId":1 7-0,"firstEventId":1 7-0,"firstEventData": " ", "lastEventData": " ", "streamSize":1977926,"connectionId":d 6-3 6-4 e-8 9-4 1"}

Id: 1 9-0
event: create
data: {"data":{"id":"marking-definition-6 d-4 7-9 a-b 0","definition_type":"tlp","definition":{"tlp":"WHITE"},"x_opencti_color":"#ffffff","x_opencti_order":1,"x_opencti_stix_id":["marking-definition-6 d-4 7-9 a-b 0"],"spec_version":"2.1","created_at":"2021 1","updated_at":"2021 1","created":"2021 1","modified":"2021 1","x_opencti_id":"f 8","type":"marking-definition","x_opencti_type":"Marking-Definition","name":"TLP:WHITE"},"markings":[],"message":"creates a Marking-Definition 'TLP:WHITE'", "version":3}

Id: 1 3-0
event: create
data: {"data":{"id":"marking-definition-3 e-8 f-4 e-8 0-e a","definition_type":"tlp","definition":{"tlp":"GREEN"},"x_opencti_color":"#2e7d32","x_opencti_order":2,"x_opencti_stix_id":["marking-definition-3 e-8 f-4 e-8 0-e a"],"spec_version":"2.1","created_at":"2 1-1 1- 1721:36:29.003Z","updated_at":"2021 2","created":"2021 2","modified":"2021 12","x_opencti_id":"51 9","type":"marking-definition","x_opencti_type":"Marking-Definition","name":"TLP:GREEN"},"markings":[],"message":"creates a Marking-Definition 'TLP:GREEN'", "version":3}

Id: 1 3-0
event: create
data: {"data":{"id":"marking-definition 3","spec_version":"2.1","cr definition","x_opencti_type":"Marking-Definition","name":"TLP:AMBER"},"markings":[],"message":"creates a Marking-Definition 'TLP:AMBER'", "version":3}

Id: 1 3-0
event: create
data: {"data":{"id":"marking-definition- 1","spec_version":"2.1","created_at":" 1","updated_at":" 1","created":" 1","modified" definition","x_opencti_type":"Marking-Definition","name":"TLP:RED"},"markings":[],"message":"creates a Marking-Definition 'TLP:RED'", "version":3}
,"type":"marking-
```

Voici un exemple de « stream brut » :

```
event: connected
data: {"lastEventId":1 7-0,"firstEventId":1 7-0,"firstEventData": " ", "lastEventData": " ", "streamSize":1 6,"connectionId":9- 2-d 1-4 3-9 3-6 e"}

event: heartbeat
data: "2022-02-15T01:22:02.275Z"

event: heartbeat
data: "2022-02-15T01:22:22.277Z"

event: heartbeat
data: "2022-02-15T01:22:42.277Z"

event: heartbeat
data: "2022-02-15T01:23:02.277Z"

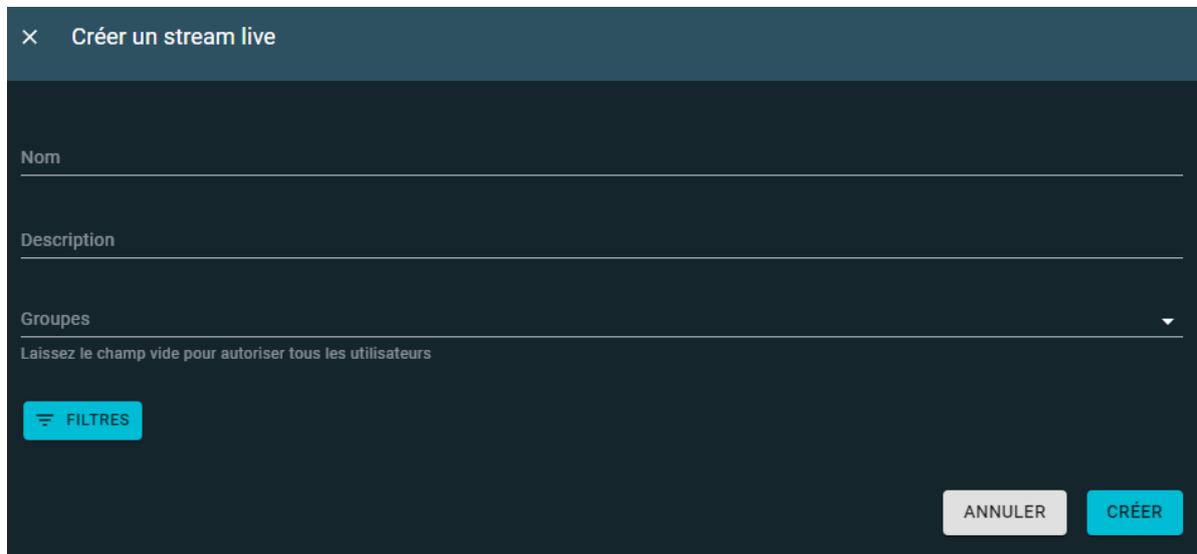
event: heartbeat
data: "2022-02-15T01:23:22.279Z"

event: heartbeat
data: "2022-02-15T01:23:42.279Z"

event: heartbeat
data: "2022-02-15T01:24:02.280Z"
```

Vous pouvez créer un stream personnalisé pour cela il faut remplir les champs suivants :

- Nom
- Description
- Groupes
- Filtres



The screenshot shows a dark-themed modal window titled "Créer un stream live". It contains three input fields: "Nom", "Description", and "Groupes". Below the "Groupes" field, there is a note: "Laissez le champ vide pour autoriser tous les utilisateurs". At the bottom left, there is a cyan button labeled "FILTRES". At the bottom right, there are two buttons: "ANNULER" (grey) and "CRÉER" (cyan).

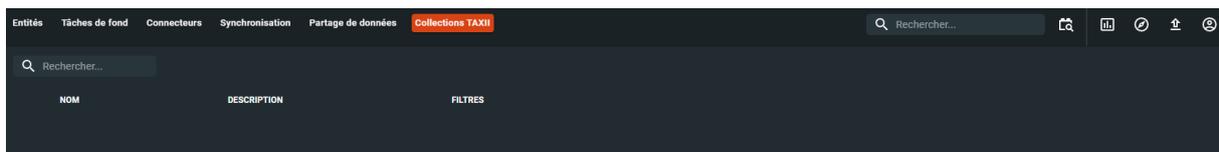
#### 10.5.6 Collections TAXII

Pour exposer un TAXII server je vous invite à regarder la source suivante :

- <https://oasis-open.github.io/cti-documentation/taxii/intro.html>

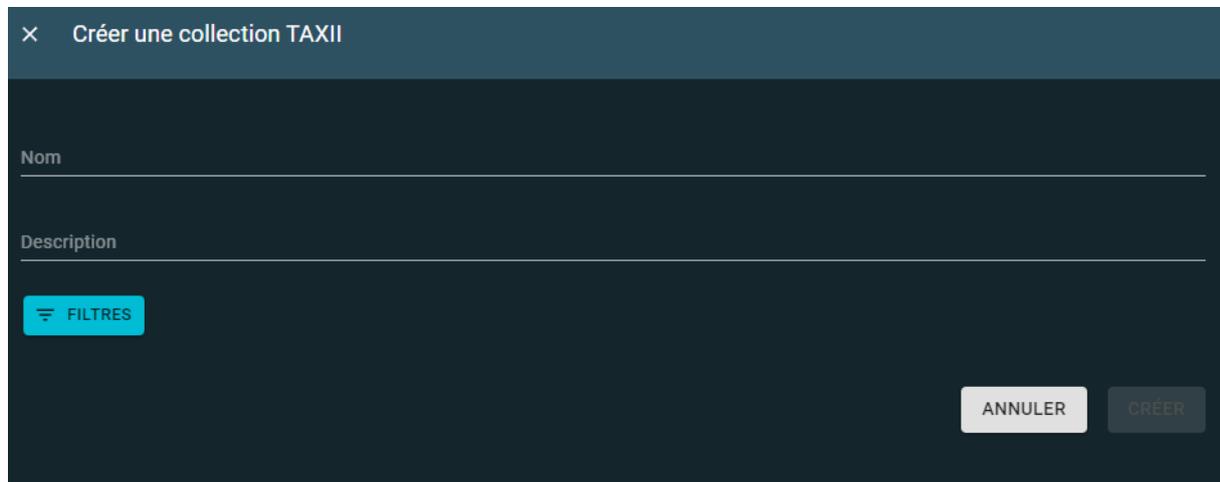
Pour synchroniser TAXII je vous invite à voir la source suivante : OpenCTI data sharing >

- <https://medium.com/luatix/opencti-data-sharing-6da7dc045d14>



Pour créer une collection TAXII il faut remplir les champs suivants :

- Nom
- Description
- Filtres



Créer une collection TAXII

Nom

Description

FILTRES

ANNULER CREER

## 10.6 Paramètres

Cette partie contiens différents menus qui sont les suivants :

- Paramètres
- Accès
- Workflows
- Politiques de rétention
- Moteur de règles
- Labels & Attributs



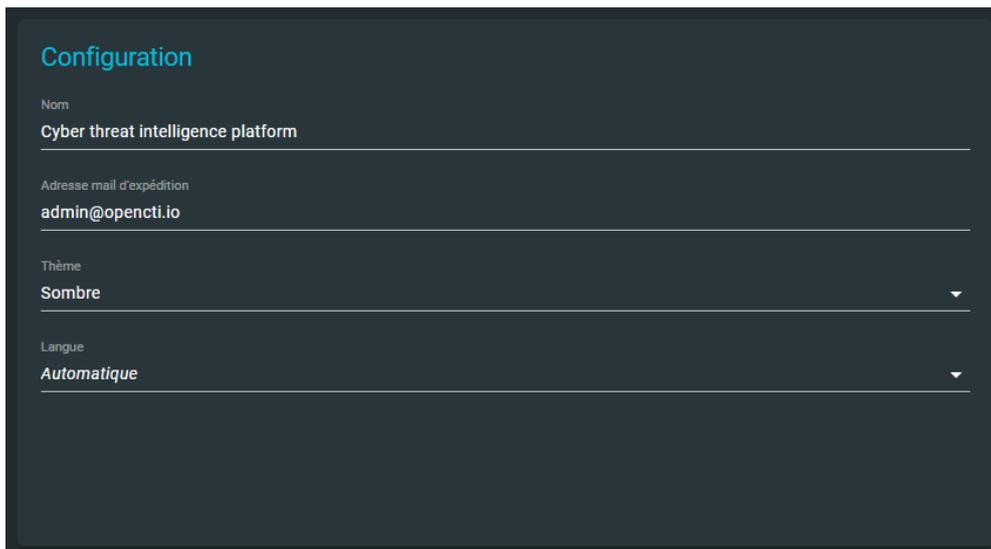
### 10.6.1 Paramètres

Le menu paramètre contiens différentes parties.

### 10.6.1.1 Configuration

Dans cette partie nous avons les champs suivants :

- Nom : nom sur s'affiche sur l'onglet du navigateur
- Adresse mail d'expédition : adresse email à utiliser pour les envois de mail
- Thème : nous pouvons choisir un thème clair ou sombre ou même en créer un !
- Langue : la langue de la plateforme
  - Par défaut le paramètre « automatique » est utilisé ainsi selon la langue du système la plateforme s'adapte entre le Français et l'Anglais.

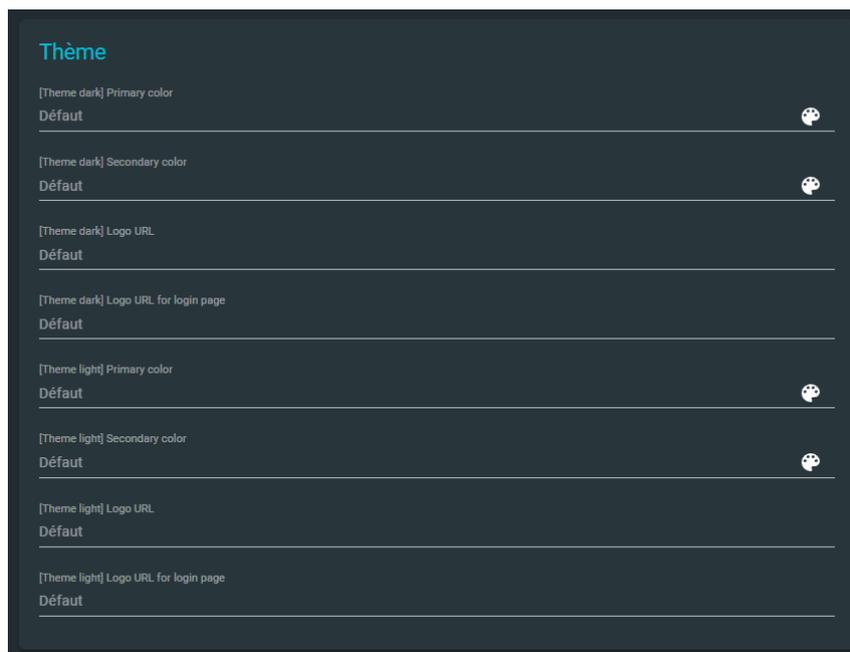


The screenshot shows the 'Configuration' page in OpenCTI. It features a dark background with white text. The title 'Configuration' is at the top left. Below it, there are four settings:

- Nom**: Cyber threat intelligence platform
- Adresse mail d'expédition**: admin@opencti.io
- Thème**: Sombre (with a dropdown arrow)
- Langue**: Automatique (with a dropdown arrow)

### 10.6.1.2 Thème

Il est tout à fait possible de créer un thème personnalisé qui vous corresponde mieux :

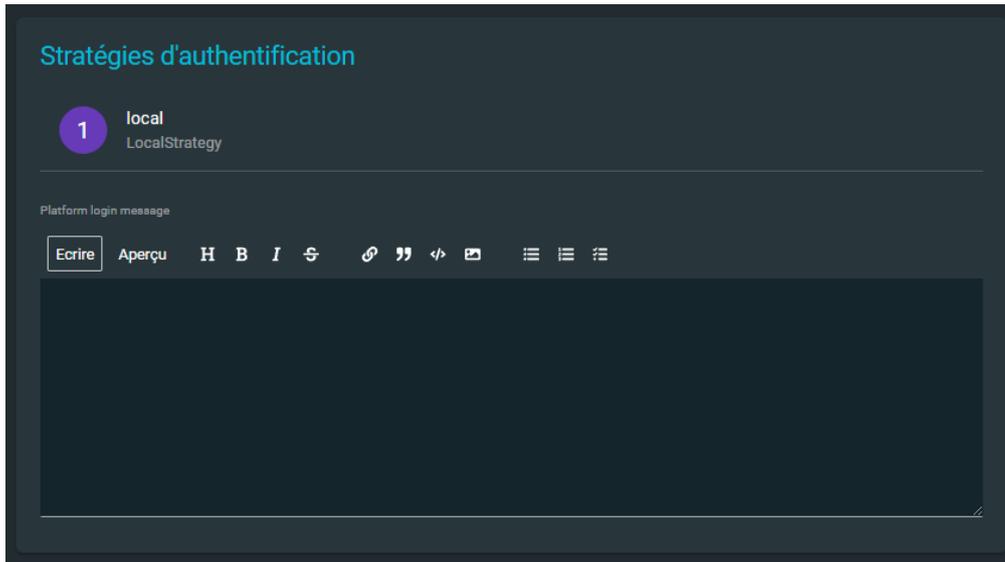


The screenshot shows the 'Thème' (Theme) configuration page in OpenCTI. It features a dark background with white text. The title 'Thème' is at the top left. Below it, there are eight settings for customizing themes:

- [Theme dark] Primary color**: Défait (with a color picker icon)
- [Theme dark] Secondary color**: Défait (with a color picker icon)
- [Theme dark] Logo URL**: Défait
- [Theme dark] Logo URL for login page**: Défait
- [Theme light] Primary color**: Défait (with a color picker icon)
- [Theme light] Secondary color**: Défait (with a color picker icon)
- [Theme light] Logo URL**: Défait
- [Theme light] Logo URL for login page**: Défait

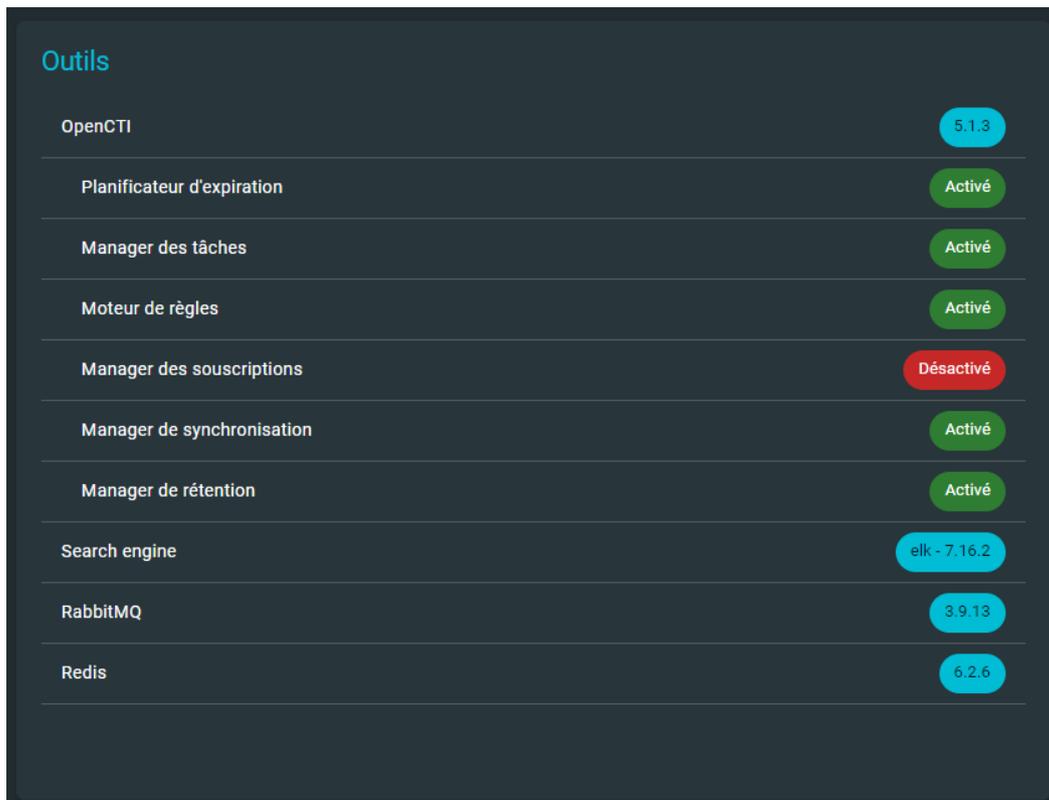
### 10.6.1.3 Stratégies d'authentification

Nous pouvons définir un message à afficher lorsqu'on arrive sur la page d'authentification :



### 10.6.1.4 Outils

La liste des outils et leur état est affiché :

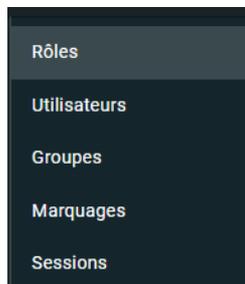


## 10.6.2 Accès



Le menu « Accès » est composé de différentes parties :

- Rôles
- Utilisateurs
- Groupes
- Marquages
- Sessions



### 10.6.2.1 Rôles

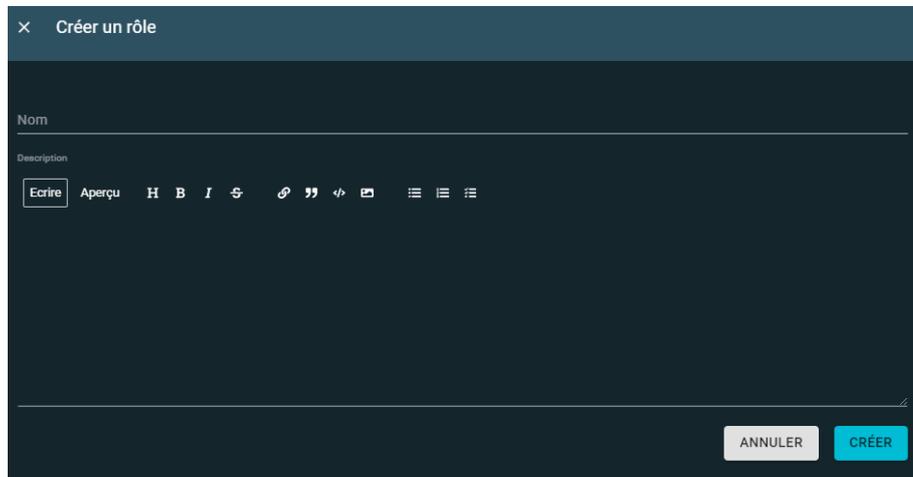
Différents types de rôles sont par défaut existants :

- Administrateur : un compte avec tous les privilèges sur la plateforme
- Connector :
  - Le fameux rôle dont j'ai parlé à plusieurs reprises plus haut dans le document !
  - Je vous conseille vivement de créer un compte utilisateur et de lui appliquer ce rôle, ainsi le Token / clé API de ce compte sera utilisé pour les connecteurs
  - Pour aller plus loin je dirais même qu'il faut un compte par connecteur pour séparer les connecteurs
- Default

NOM	ALLOUÉ PAR DÉFAUT	DATE DE CRÉATION	DATE DE MODIFICATION
Administrator	-	31 oct. 2021	31 oct. 2021
Connector	-	31 oct. 2021	31 oct. 2021
Default	✓	31 oct. 2021	31 oct. 2021

Il est possible de créer un nouveau rôle pour cela il faut remplir les champs suivants :

- Nom
- Description



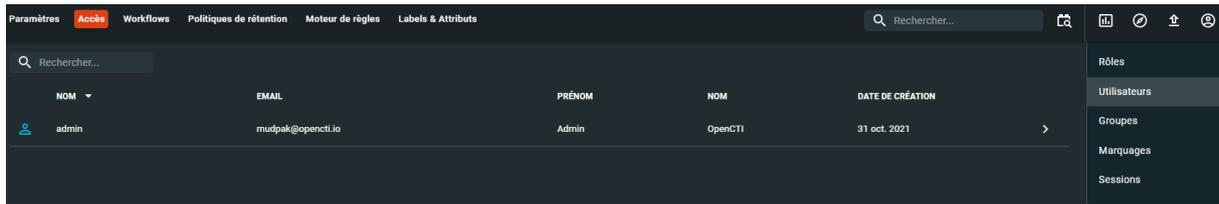
Une fois que le rôle est créé, il faut lui attribuer des droits, voici la liste des droits qu'on peut attribuer :



Capacité	Statut
Bypass all capabilities	<input type="checkbox"/>
Access knowledge	<input type="checkbox"/>
Create / Update knowledge	<input type="checkbox"/>
Delete knowledge	<input type="checkbox"/>
Upload knowledge files	<input type="checkbox"/>
Import knowledge	<input type="checkbox"/>
Download knowledge export	<input type="checkbox"/>
Generate knowledge export	<input type="checkbox"/>
Ask for knowledge enrichment	<input type="checkbox"/>
Access exploration	<input type="checkbox"/>
Create / Update exploration	<input type="checkbox"/>
Delete exploration	<input type="checkbox"/>
Access connectors	<input type="checkbox"/>
Manage connector state	<input type="checkbox"/>
Access Taxii feed	<input type="checkbox"/>
Manage Taxii collections	<input type="checkbox"/>
Access administration	<input type="checkbox"/>
Manage credentials	<input type="checkbox"/>
Manage marking definitions	<input type="checkbox"/>
Manage labels & Attributes	<input type="checkbox"/>
Connectors API usage: register, ping, export push ...	<input type="checkbox"/>
Connect and consume the platform streams (/stream, /stream/live)	<input type="checkbox"/>
Bypass mandatory references if any	<input type="checkbox"/>

### 10.6.2.2 Utilisateurs

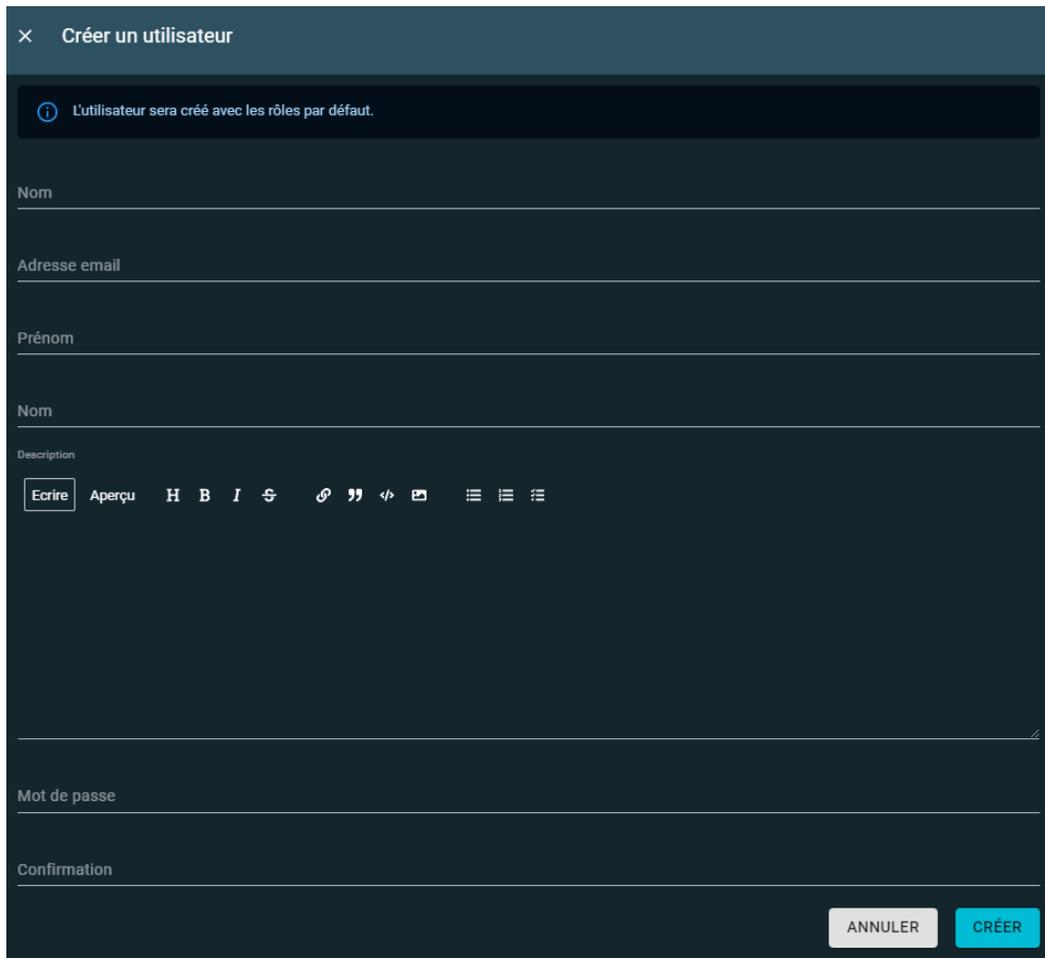
Par défaut un compte de type administrateur est présent :



NOM	EMAIL	PRÉNOM	NOM	DATE DE CRÉATION
admin	mudpak@opencti.io	Admin	OpenCTI	31 oct. 2021

Pour créer un nouveau compte il faut remplir les champs suivants :

- Nom
- Adresse email
  - Il est important de noter que nous n'avons pas traité la partie emailing, ainsi l'utilisateur aura beau se connecter avec une adresse email aucun email ne lui sera envoyé puisque nous n'avons pas mis en place un serveur de messagerie.
- Prénom
- Nom
- Description
- Mot de passe
- Confirmation



×

Créer un utilisateur

*i* L'utilisateur sera créé avec les rôles par défaut.

Nom

Adresse email

Prénom

Nom

Description

Ecrire Aperçu H B I ↻ ↺ ↻ ↻

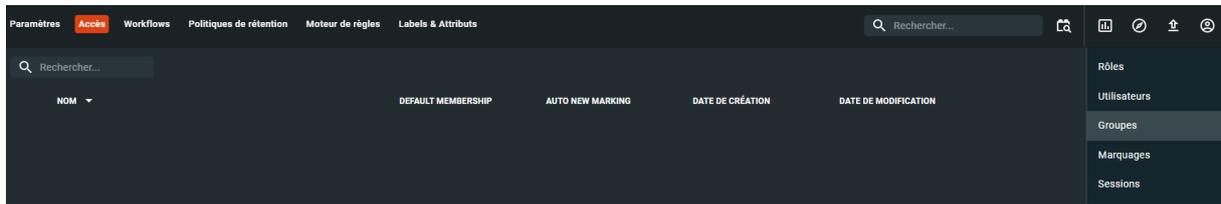
Mot de passe

Confirmation

ANNULER CRÉER

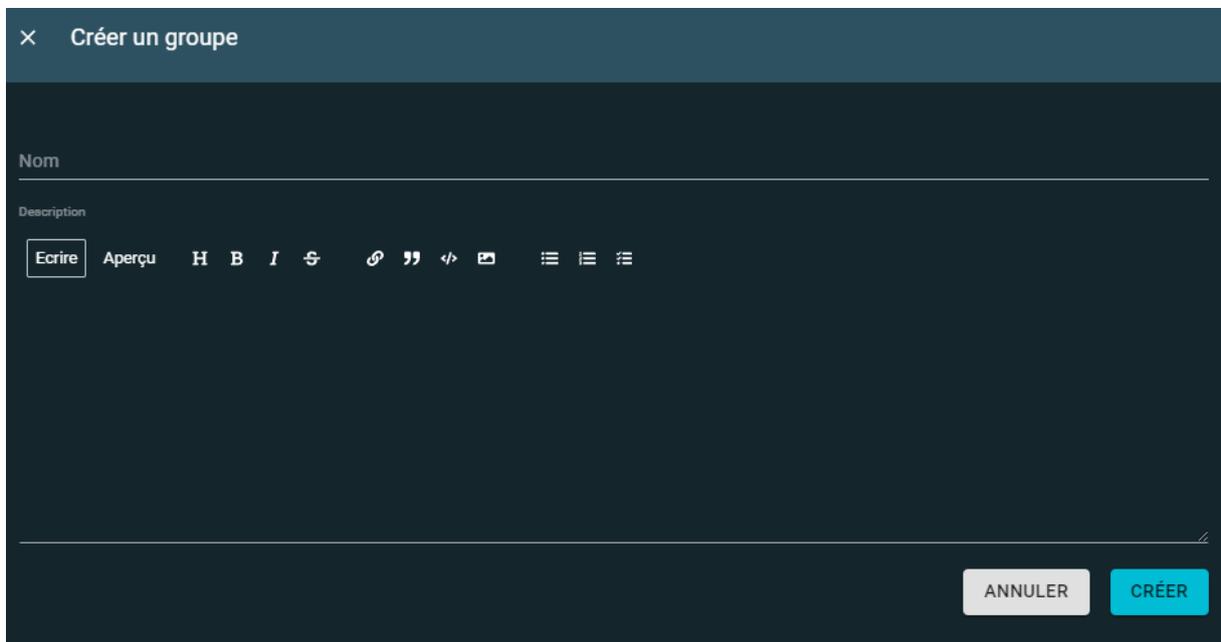
### 10.6.2.3 Groupes

Par défaut il n'y a pas de groupes, pour des raisons de sécurité et de bonnes pratiques il est recommandé de créer des groupes :



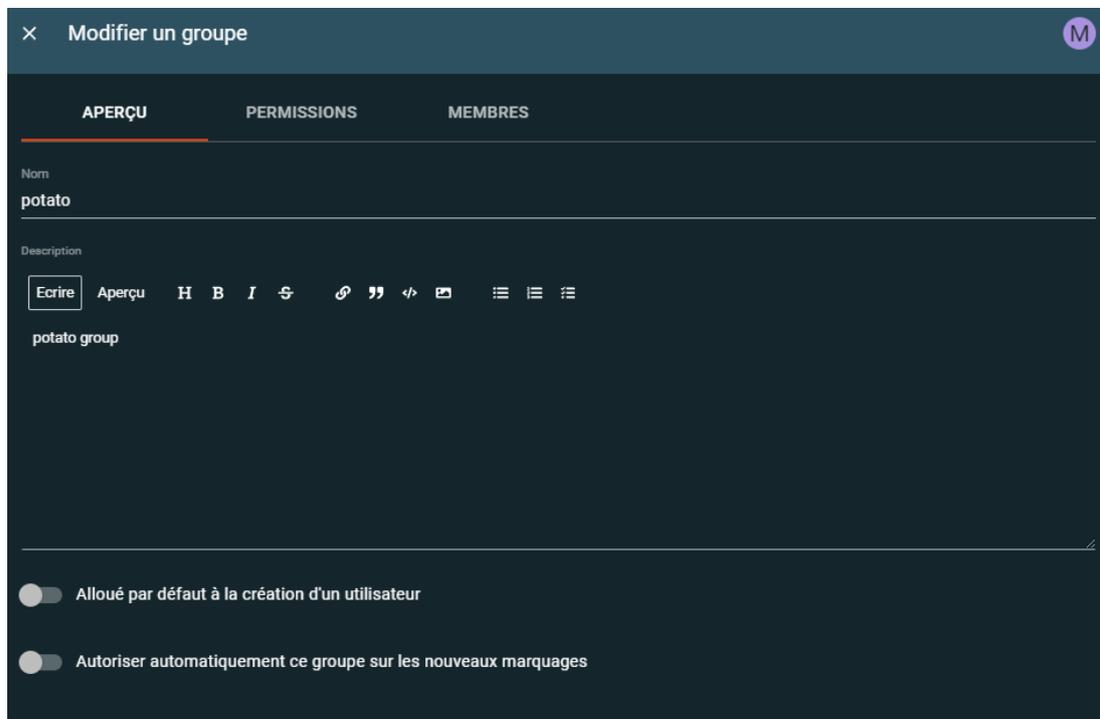
Pour créer un groupe il faut remplir les champs suivants :

- Nom
- Description

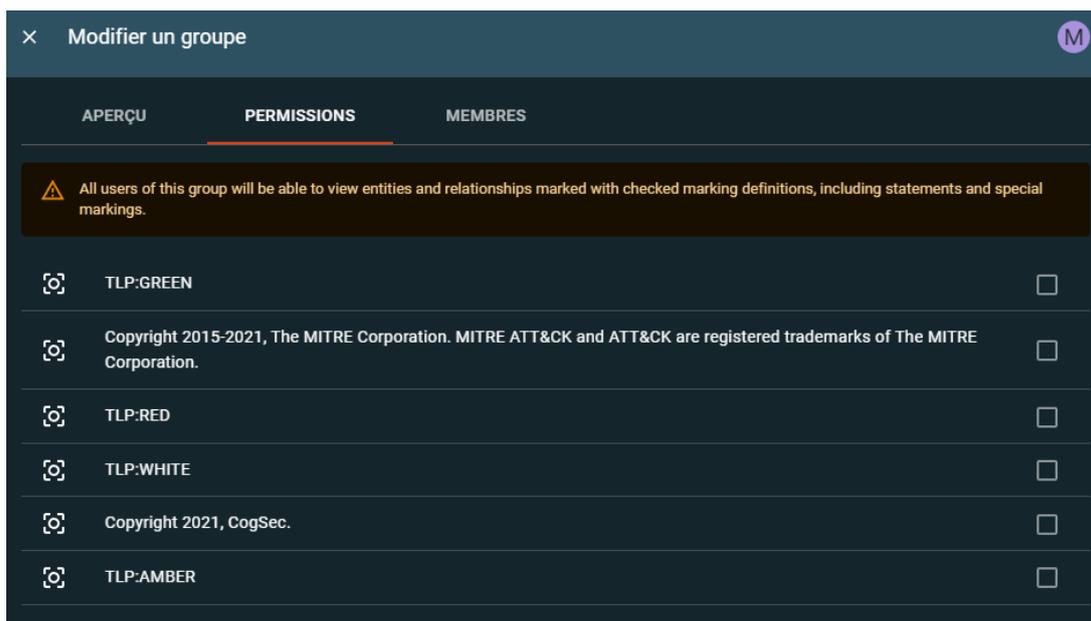
A screenshot of the 'Créer un groupe' (Create a group) form in OpenCTI. The form has a dark theme. At the top, there is a title bar with a close button and the text 'Créer un groupe'. Below the title bar, there are two main input fields: 'Nom' (Name) and 'Description'. The 'Description' field has a rich text editor toolbar with options like 'Ecrire', 'Aperçu', 'H', 'B', 'I', 'G', 'Link', 'Quote', 'Code', 'Image', 'List', 'Table', and 'Table of contents'. At the bottom right of the form, there are two buttons: 'ANNULER' (Cancel) and 'CRÉER' (Create).

Lorsque le groupe est créé il faut modifier les paramètres :

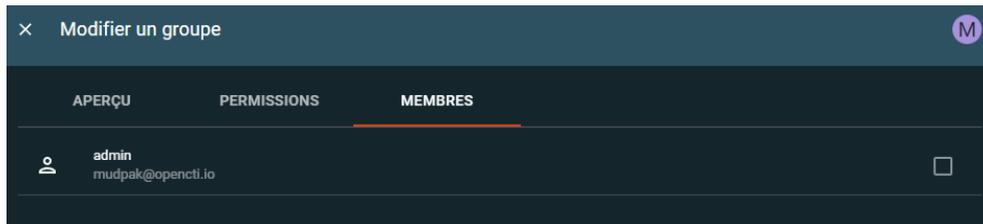
- Alloué par défaut à la création d'un utilisateur : est-ce qu'on souhaite ajouter tous les nouveaux comptes crée à ce groupe ?
- Autoriser automatiquement ce groupe sur les nouveaux marquages : est-ce qu'on ajoute ce groupe sur tous les nouveaux marquages ?



Dans l'onglet permissions nous pouvons ajuster les droits pour que le groupe puisse accéder à un TLP spécifique de rapports :



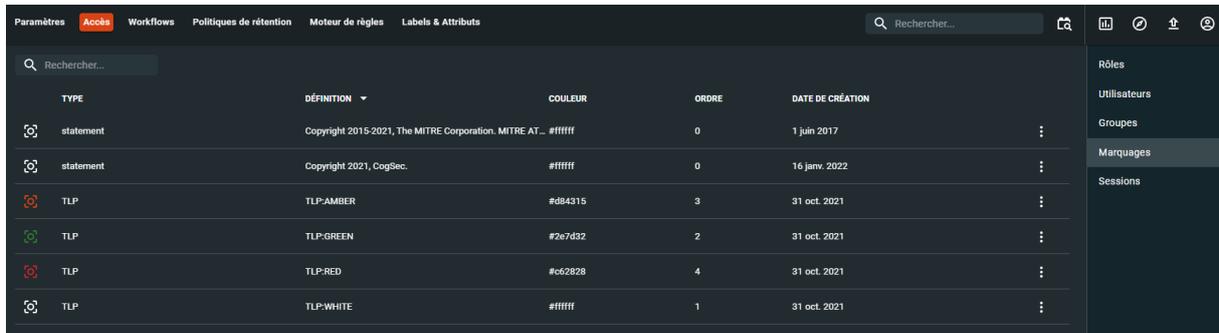
Dans le dernier onglet on peut voir ou ajouter des membres à ce groupe :



#### 10.6.2.4 Marquages

Tout au long du document j'ai évoqué les « TLP », voici donc les différents types de TLP du niveau le plus critique au moins critique :

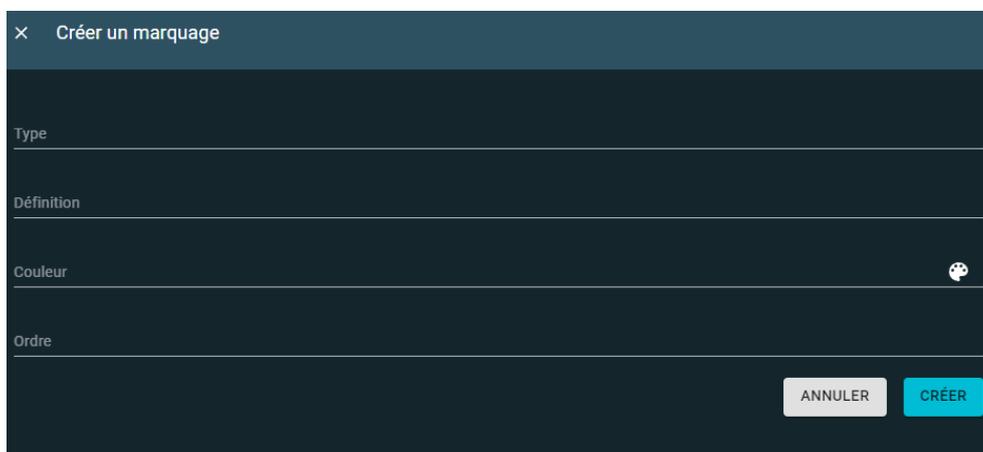
- RED
- AMBER
- GREEN
- WHITE



TYPE	DÉFINITION	COULEUR	ORDRE	DATE DE CRÉATION
statement	Copyright 2015-2021, The MITRE Corporation. MITRE AT... #ffffff		0	1 juin 2017
statement	Copyright 2021, CogSec.	#ffffff	0	16 janv. 2022
TLP	TLP-AMBER	#84315	3	31 oct. 2021
TLP	TLP-GREEN	#2e7d32	2	31 oct. 2021
TLP	TLP-RED	#c62828	4	31 oct. 2021
TLP	TLP-WHITE	#ffffff	1	31 oct. 2021

Vous pouvez créer un type de marquage adapté à vos besoins, pour cela il faut remplir les champs suivants :

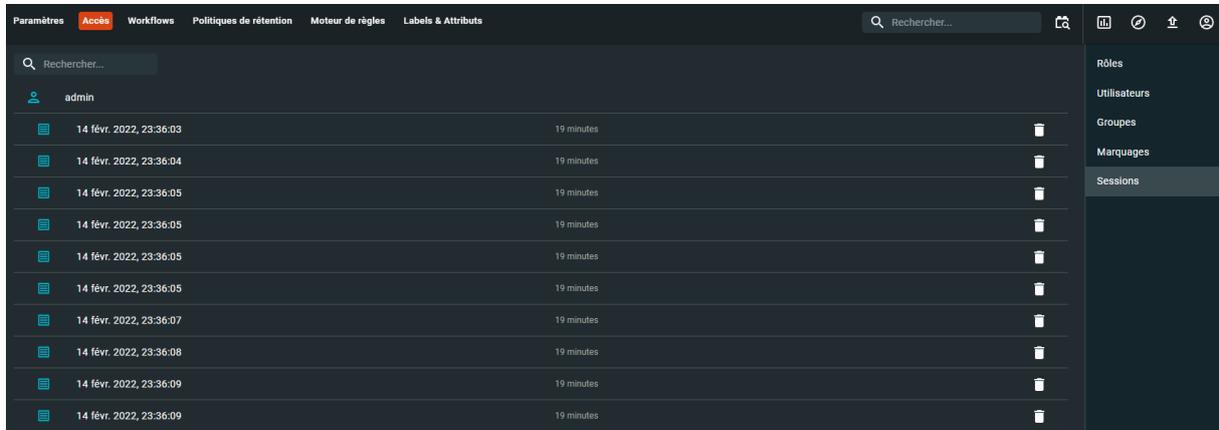
- Type
- Définition
- Couleur
- Ordre



### 10.6.2.5 Sessions

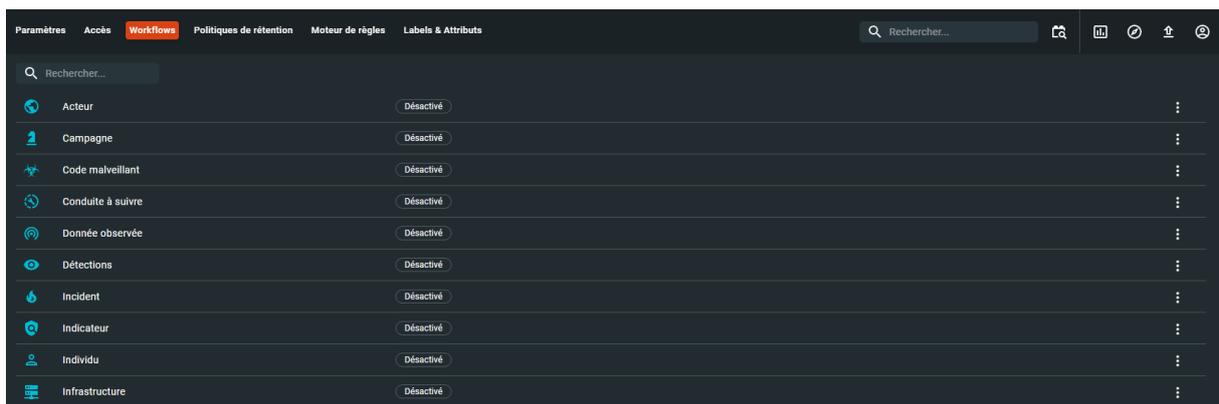
Dans cette partie nous pouvons voir l'historique des connexions des différents utilisateurs.

Il est tout à fait possible de révoquer la connexion à un utilisateur en cliquant sur la corbeille située à droite de la fenêtre :



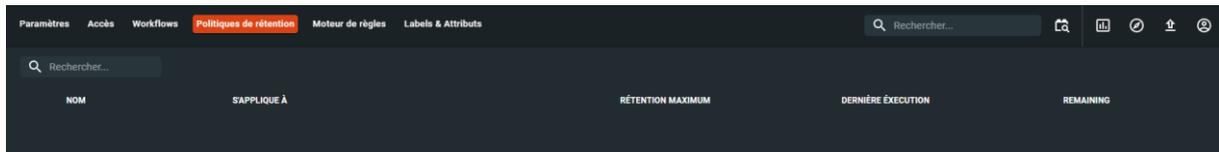
### 10.6.3 Workflows

Permet d'associer un workflow manuel.



### 10.6.4 Politique de rétention

Par défaut il n'y a pas de politique de rétention, donc les données sont enregistrées jusqu'à saturation du disque dur :



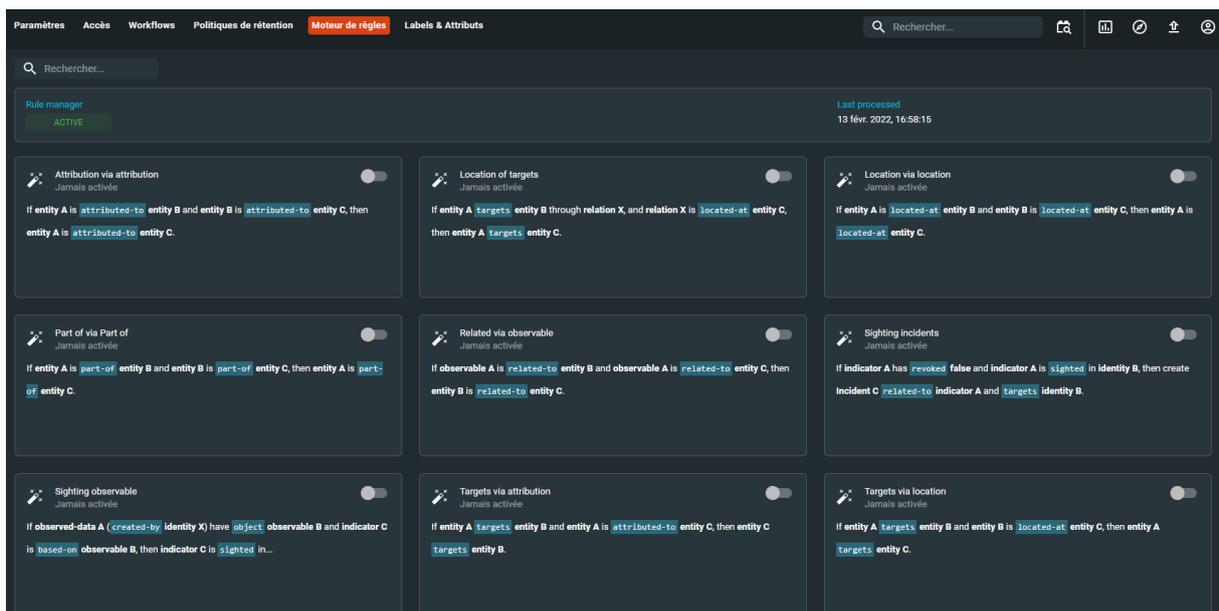
Nous pouvons créer une règle de rétention en remplissant les champs suivants :

- Nom
- Jours de rétention maximum : durée après laquelle les données peuvent être supprimées
- Filtres : ces filtres vous permettront de sélectionner précisément par exemple quels niveaux de TLP sélectionner pour la conservation

### 10.6.5 Moteur de règles

C'est un moteur qui permet de créer des relations différentes entre des éléments.

Par exemple si MALWARE1 target CITY et CITY part-of COUNTRY alors MALWARE1 target COUNTRY.



### 10.6.6 Labels & attributs

Ce menu est composé de différents onglets :

- Labels
- Phases de kill chain
- Types de rapport



#### 10.6.6.1 Labels

Tout au long du document nous avons vu sur chaque rapport l'existence de labels dès qu'il y en fait, au-delà de cet aspect lors de la création d'un élément quasi systématiquement cette option était proposée, en fait on peut la comparer au système de « tags », cela permet de trier / retrouver des éléments plus rapidement.

VALEUR	COULEUR	DATE DE CRÉATION
.net	#af9216	16 janv. 2022
32	#54483b	16 janv. 2022
activex	#3262e0	16 janv. 2022
adwind	#abf23e	21 janv. 2022
agent tesla	#3c8c75	16 janv. 2022
agenttesla	#3225a5	16 janv. 2022
aggag	#c748b7	16 janv. 2022
alphav	#d87aac	21 janv. 2022
andariel	#886570	26 janv. 2022
android	#6f36a8	16 janv. 2022

Pour créer un attribut il faut remplir le champ suivant :

- Valeur : par la valeur que l'attribut va porter

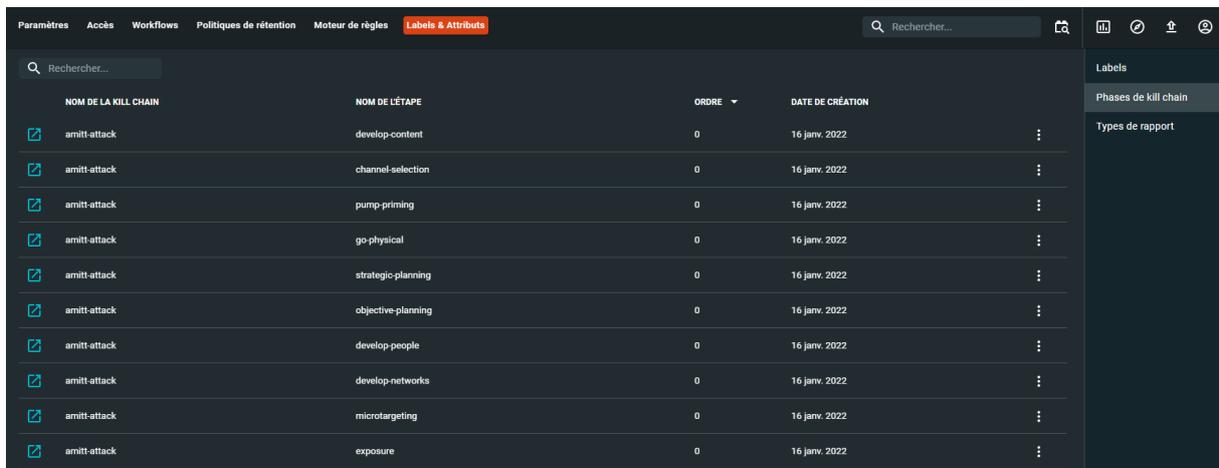
Créer un attribut

Valeur

ANNULER CRÉER

### 10.6.6.2 Phases de kill chain

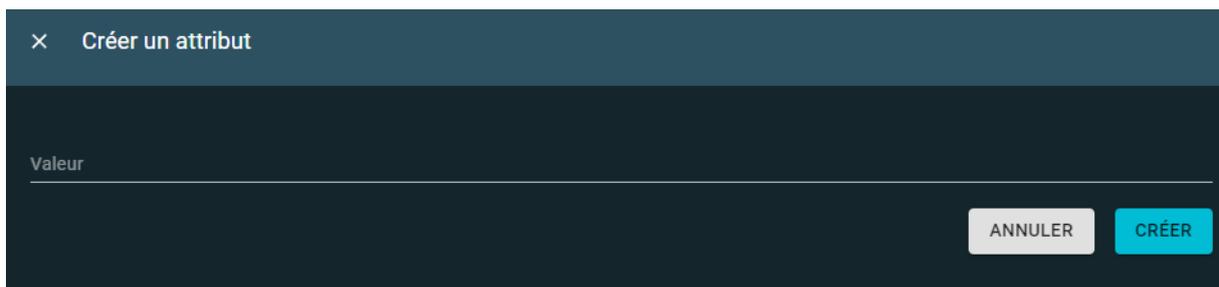
Comme nous l'avons vu précédemment ici nous avons une autre représentation de la matrice MITRE ATT&CK :



NOM DE LA KILL CHAIN	NOM DE L'ÉTAPE	ORDRE	DATE DE CRÉATION
amitt-attack	develop-content	0	16 janv. 2022
amitt-attack	channel-selection	0	16 janv. 2022
amitt-attack	pump-priming	0	16 janv. 2022
amitt-attack	go-physical	0	16 janv. 2022
amitt-attack	strategic-planning	0	16 janv. 2022
amitt-attack	objective-planning	0	16 janv. 2022
amitt-attack	develop-people	0	16 janv. 2022
amitt-attack	develop-networks	0	16 janv. 2022
amitt-attack	microtargeting	0	16 janv. 2022
amitt-attack	exposure	0	16 janv. 2022

Pour créer un nouvel attribut il faut remplir le champ suivant :

- Valeur



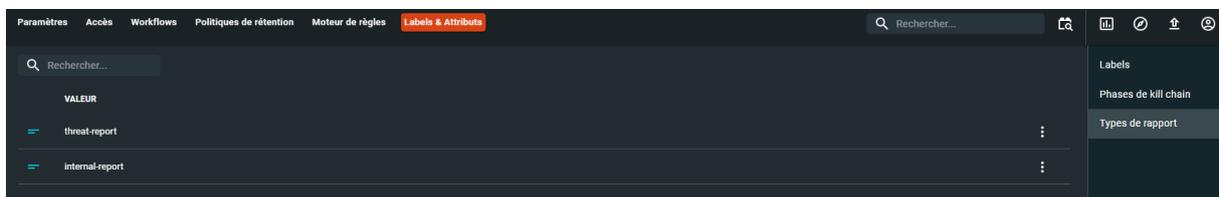
Créer un attribut

Valeur

ANNULER CRÉER

### 10.6.6.3 Types de rapport

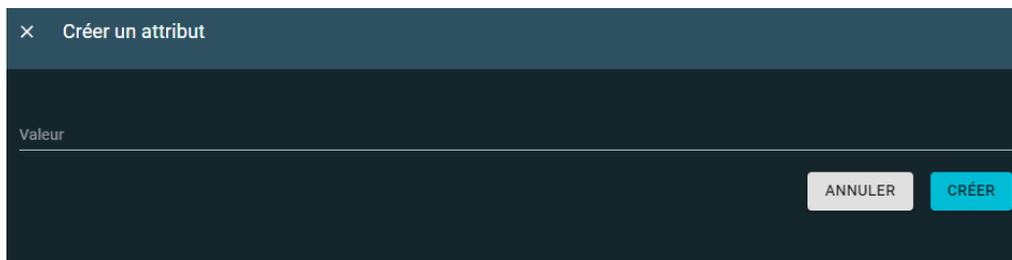
Sur les rapports que nous avons pu visualiser sur la plateforme ils correspondaient à une des deux catégories ci-dessous :



VALEUR
threat-report
internal-report

Il peut être pertinent de créer une catégorie adaptée à votre contexte, pour créer un nouvel attribut il faut remplir le champ suivant :

- Valeur



× Créer un attribut

Valeur

ANNULER CRÉER

## 11. Erreurs courantes

Voici une liste des erreurs les plus courantes que j'ai pu rencontrer et leurs solutions.

### 11.1 Docker

1. Impossible d'exécuter docker en tant que simple utilisateur
  - a. Est-ce que « docker rootless » a été configuré ?
  - b. Est-ce que l'utilisateur a été ajouté au groupe « docker » ?
  - c. Est-ce que l'utilisateur s'est déconnecté et reconnecté à son compte ?

### 11.2 Docker-Compose

1. La nouvelle configuration du fichier « docker-compose.yml » ne fonctionne pas
  - a. Est-ce que la stack a été stoppée ?
  - b. Est-ce que le pull de nouveaux containers a été réalisée ?
  - c. Est-ce que le fichier de configuration « docker-compose.yml » contient les informations du connecteur qui ne fonctionne pas ?

### 11.3 OpenCTI

1. L'accès à l'interface web ne fonctionne pas
  - a. Est-ce que tous les containers ont fini de démarrer ?
  - b. Est-ce que le port de connexion a été modifié ?
2. La carte des pays s'affiche mais selon le nombre de rapports il n'y a pas de coloration sur la carte
  - a. Est-ce que le connecteur « opencti » a été ajouté au fichier « docker-compose.yml » ?

## 12. Conclusion

A travers ce long document nous avons vu les différentes étapes pour la mise en place, alimentation et utilisation de la plateforme OpenCTI.

Il existe des méthodes plus simples et rapides pour la mise en place tel que l'utilisation de la machine virtuelle ou simplement de l'utilisation de la démo avant d'implémenter la solution en entreprise ou chez soi.

Quoi qu'il en soit en tant que français nous pouvons être fiers d'avoir un tel outil Made In France car il a bien des concurrents en place déjà depuis des années mais aucun d'entre eux n'intègre la CTI pour tous types de personnes au même endroit et c'est une des forces de OpenCTI !

Je ne peux que vous inviter à utiliser la solution que ce soit pour un usage professionnel, ou personnel par exemple pour faire de la veille cyber !

Pour aller plus loin il est possible de contribuer au projet de différentes manières :

- En faisant partager la solution à un maximum de monde !
- En améliorant la documentation
- En ajoutant des fonctionnalités via GitHub
- En rejoignant la communauté Slack
- En aidant financièrement
  - En effectuant un don
  - En devenant un « membre actif » ou « Sponsor »

## 13. Sources

Voici les différentes sources qui m'ont été utiles pour la réalisation de ce document :

- <https://demo.opencti.io/>
- <https://www.opencti.io/fr/>
- <https://github.com/orgs/OpenCTI-Platform/repositories>
- <https://github.com/OpenCTI-Platform/connectors/tree/master/external-import>
- <https://www.notion.so/OpenCTI-Public-Knowledge-Base-d411e5e477734c59887dad3649f20518>