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

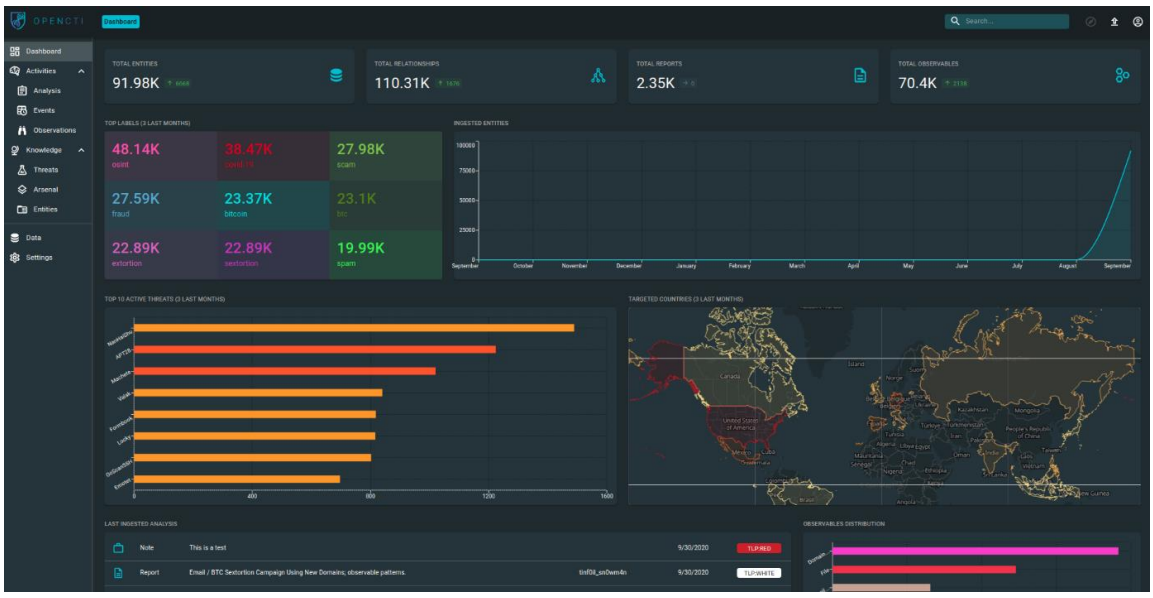


Table des matières

0. Avant-propos

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 à la documentation officielle de l'outil, qui est tenue à jour très régulièrement !

Tout au long 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 peut 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 crées 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

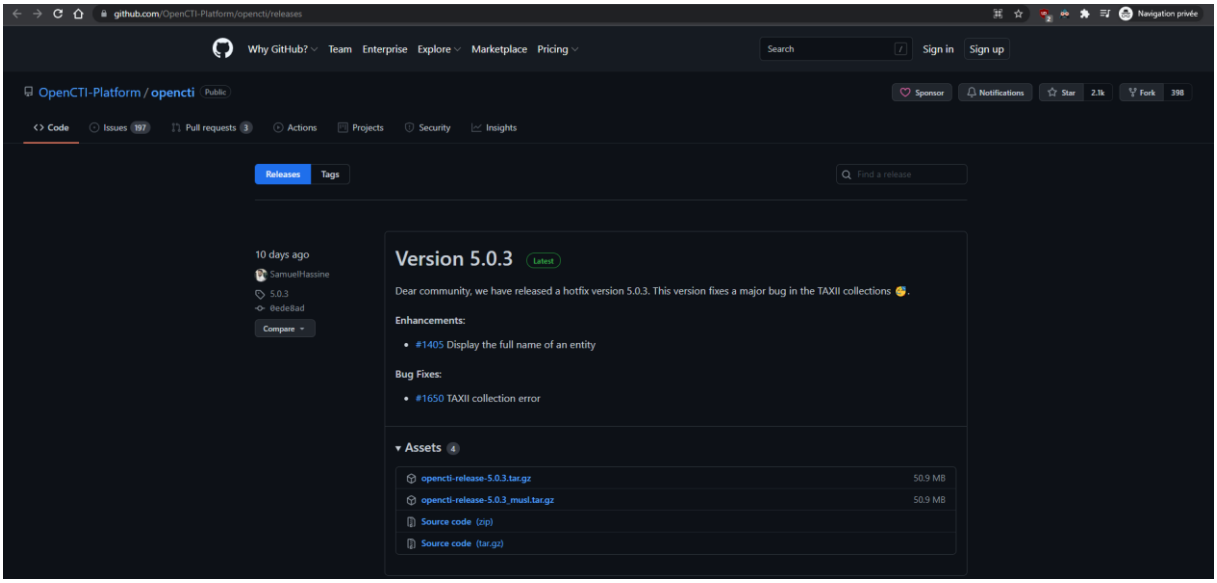
Nous allons voir le site de OpenCTI rapidement, les ressources présentes dessus vont nous être utiles par la suite.

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

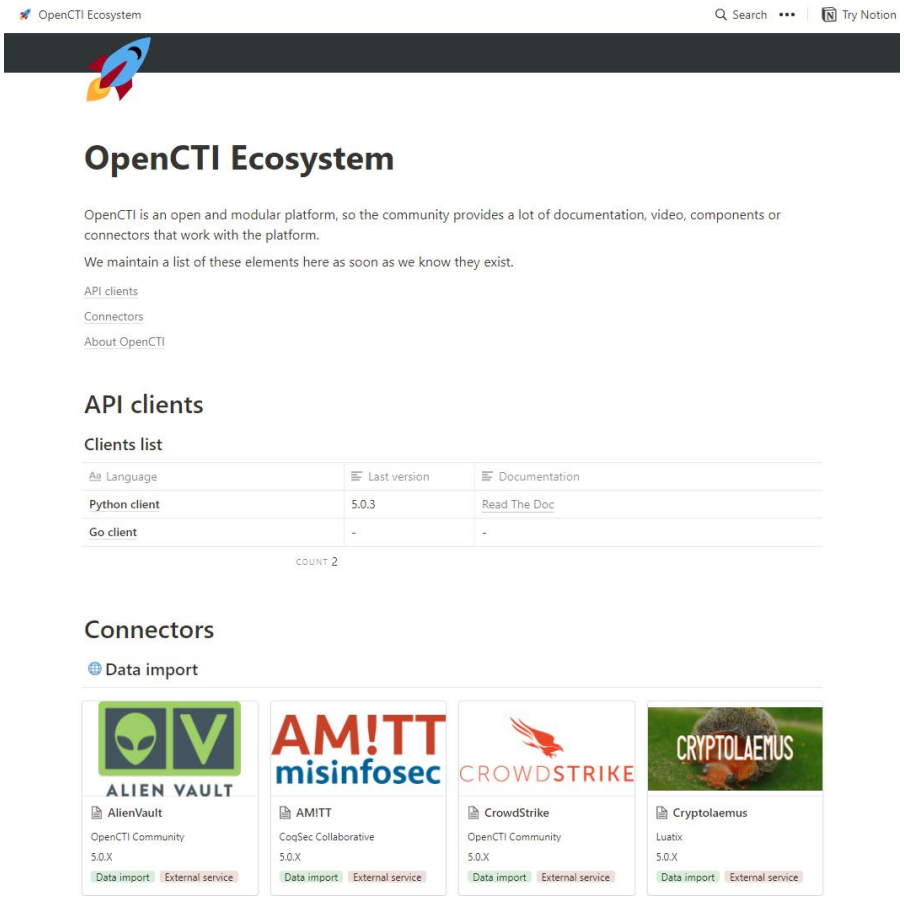
Ou créer un compte via une adresse email :

2.2.3 Feuille de route / Roadmap

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

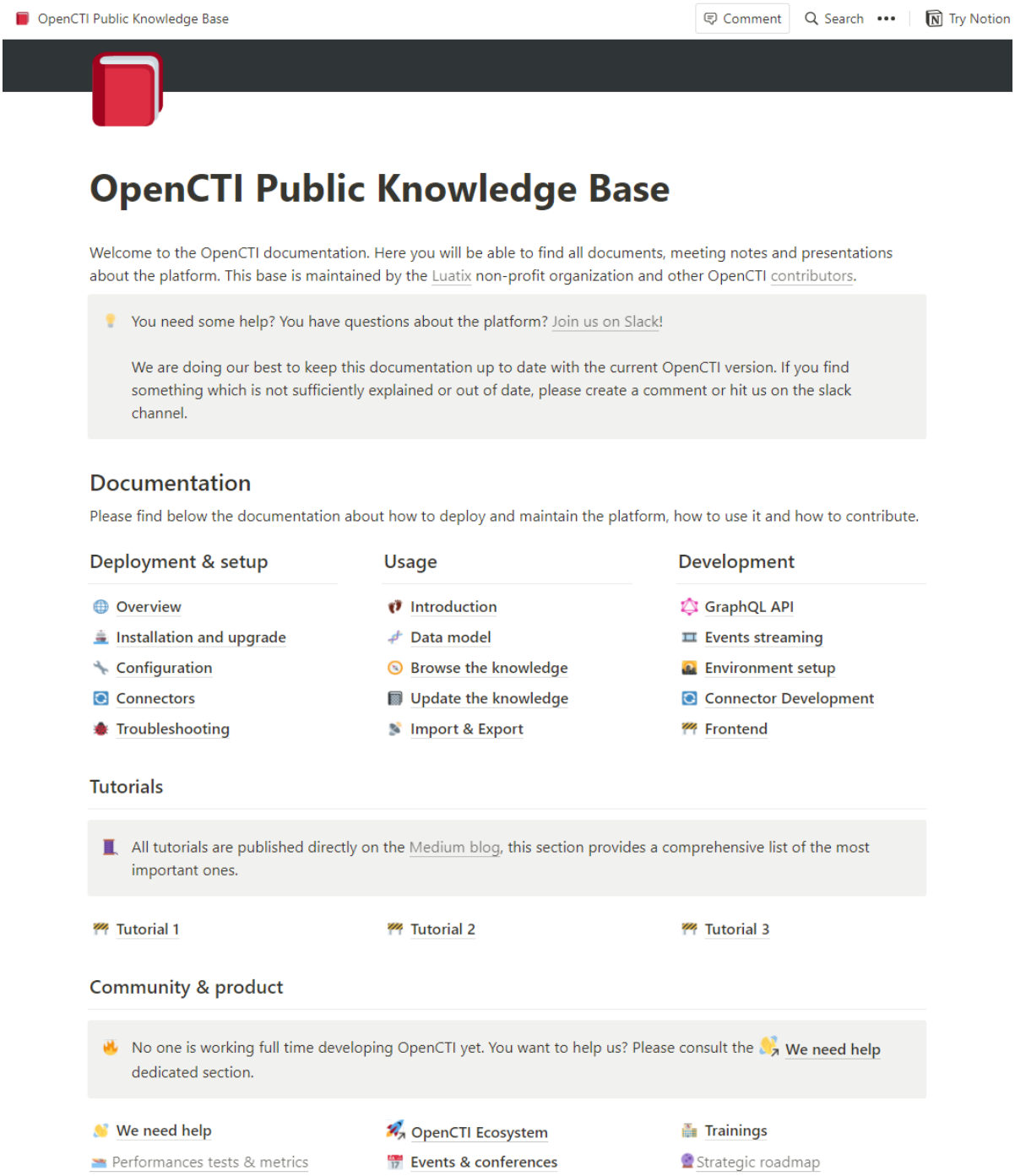
2.2.4 Ecosystème

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.



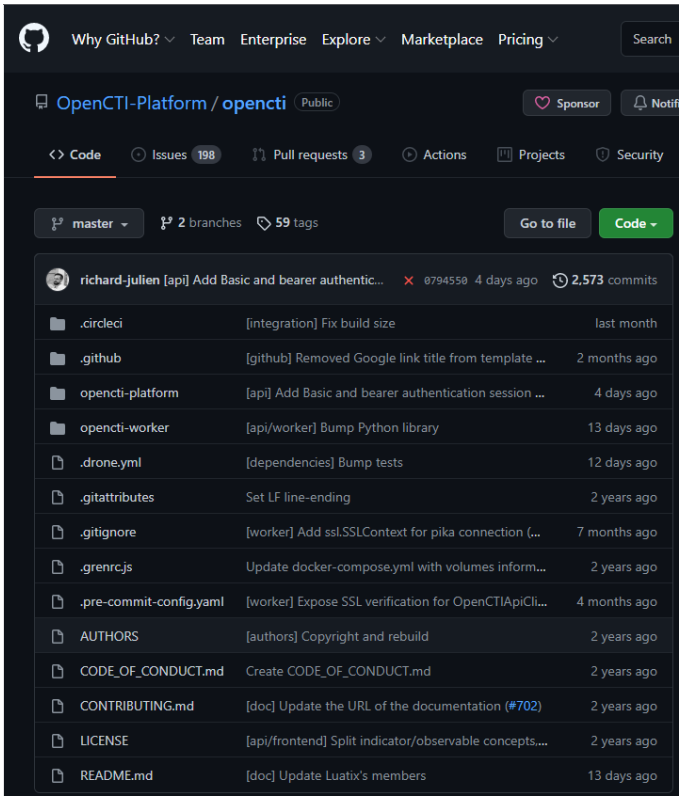
2.2.5 Documentation

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

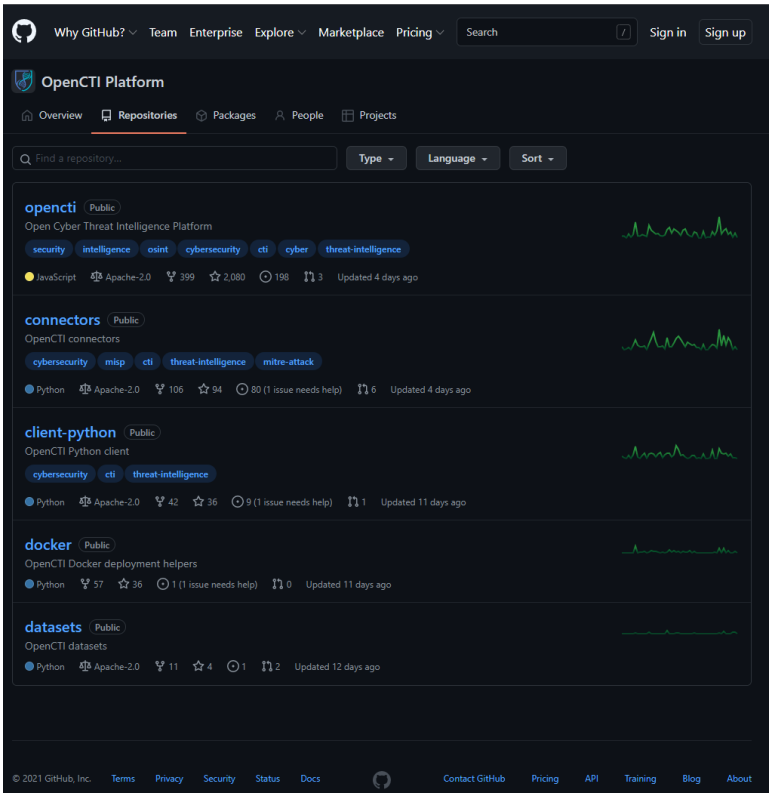


2.2.6 GitHub

La page GitHub du projet est la suivante :

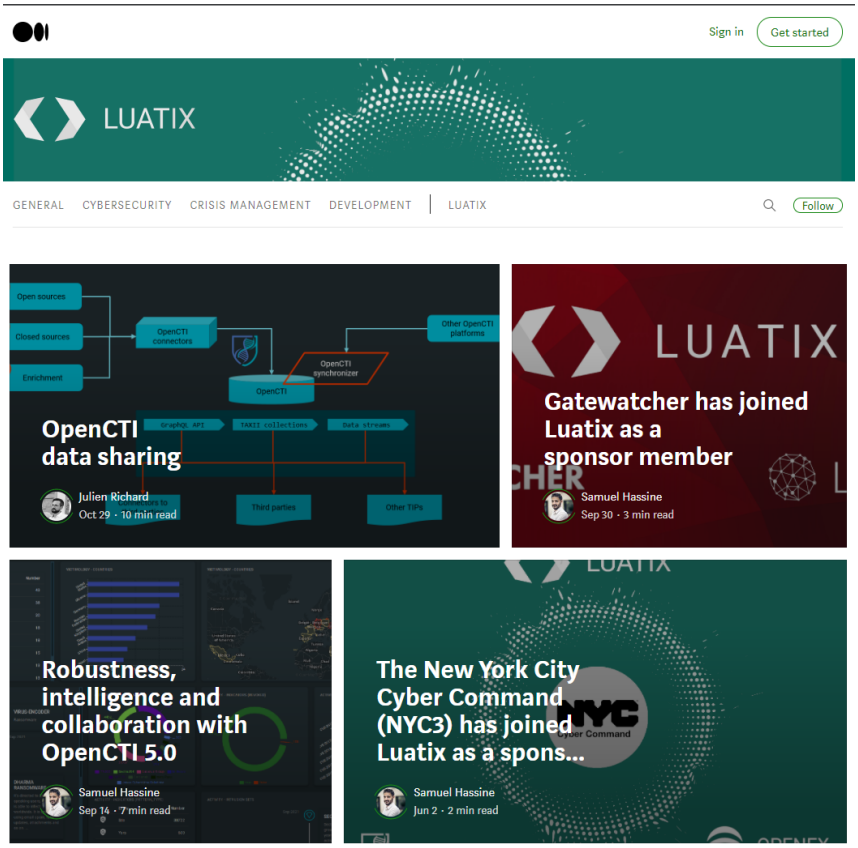


D'autres répertoires du même projet nous serons utiles par la suite :



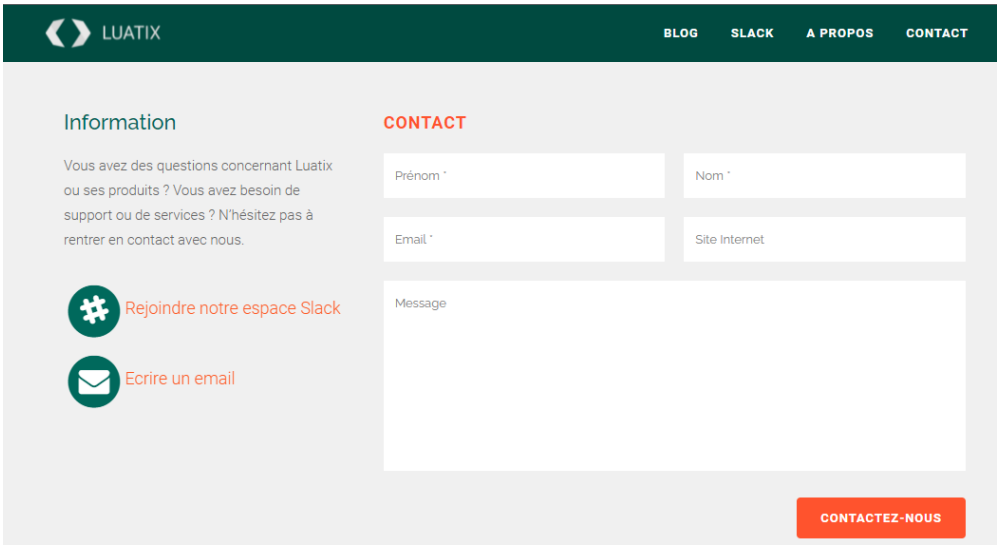
2.2.7 Blog

Des articles intéressants sont disponibles sur le blog :



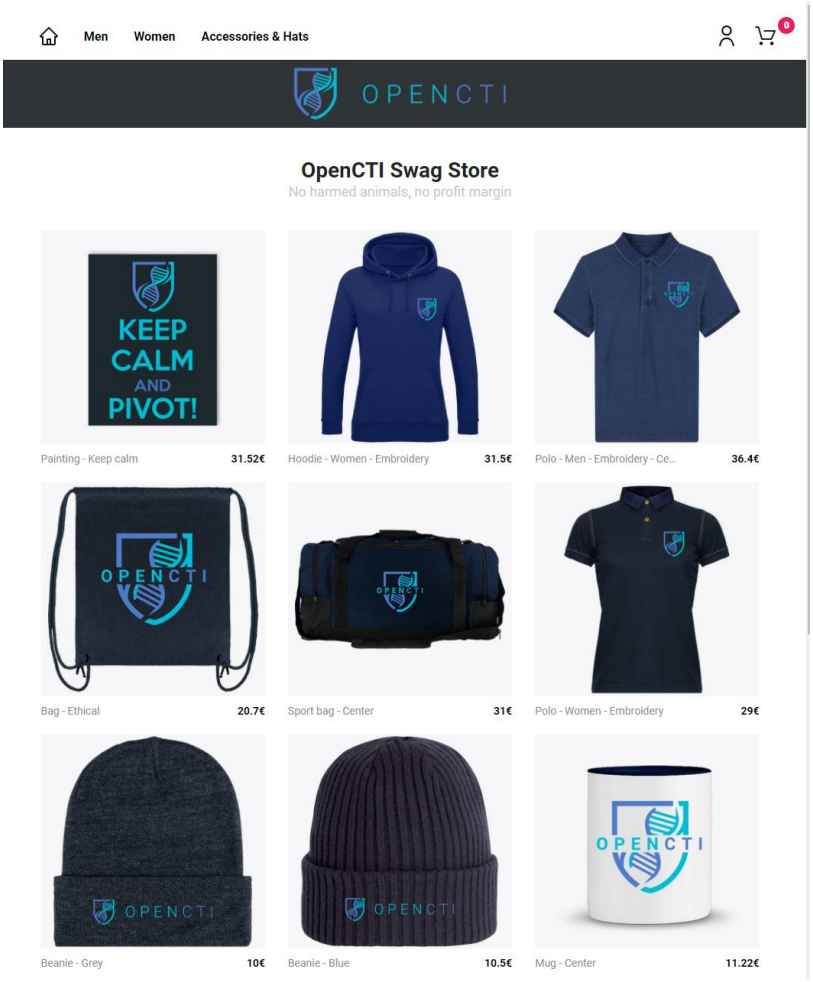
2.2.8 Contact

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



2.2.9 Swag

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



3. Ubuntu Server

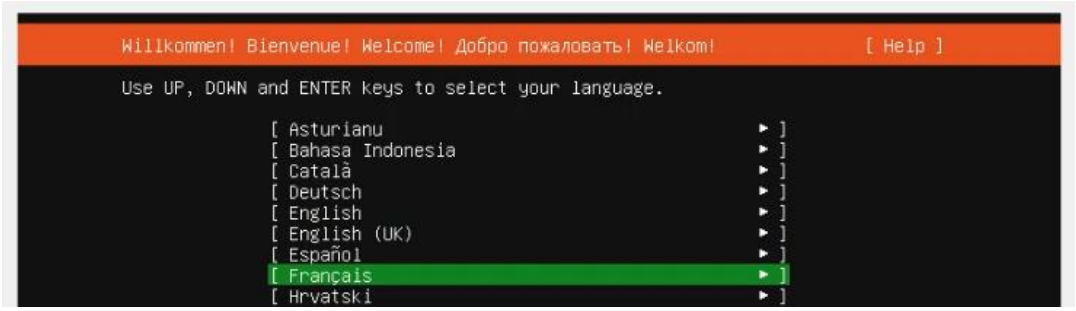
3.1 Installation

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

3.1.1 Willkomen ! Bienvenue ! Welcome !

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

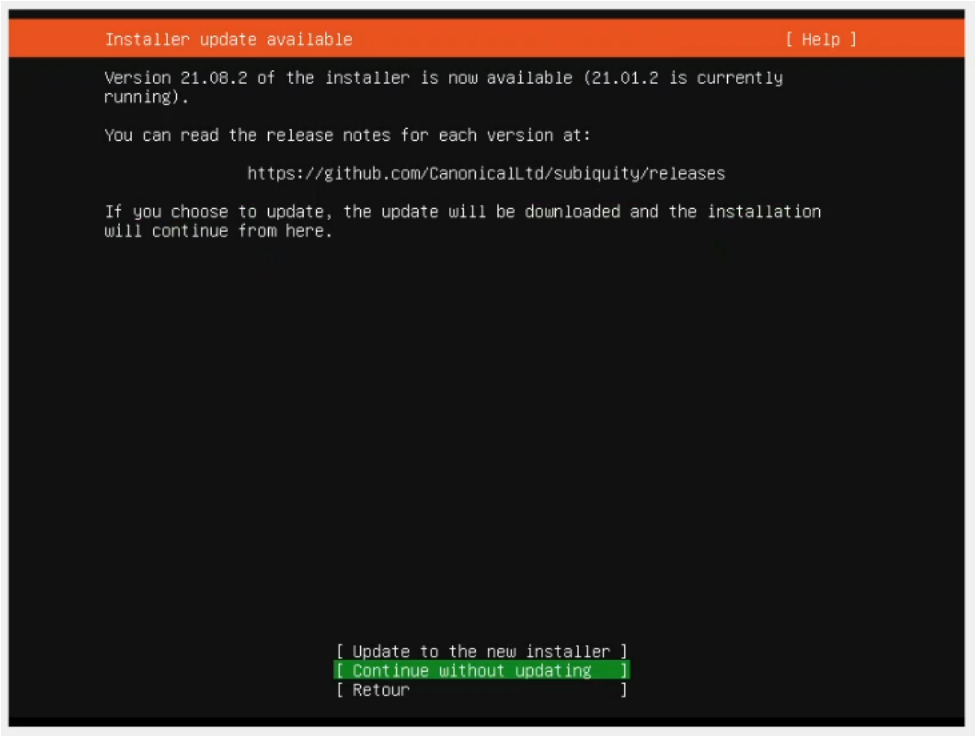
- Français



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



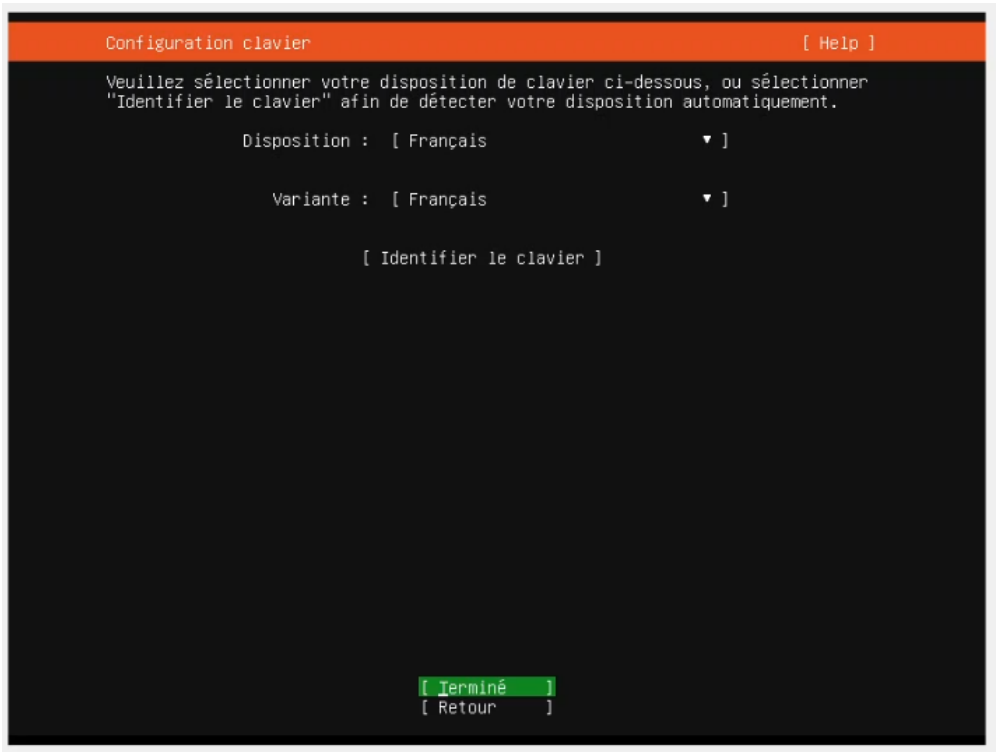
3.1.3 Configuration clavier

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

- Dispositon
- Variante

Lorsque vous avez terminé sélectionner :

- Terminé

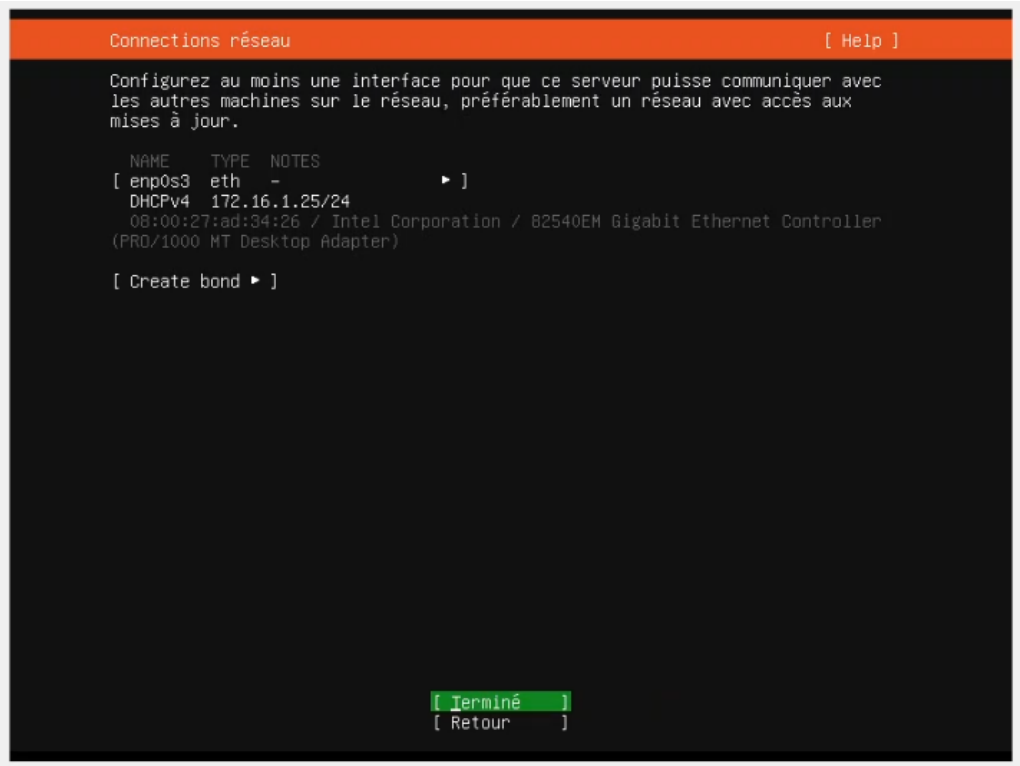


3.1.4 Connexions réseau

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 :

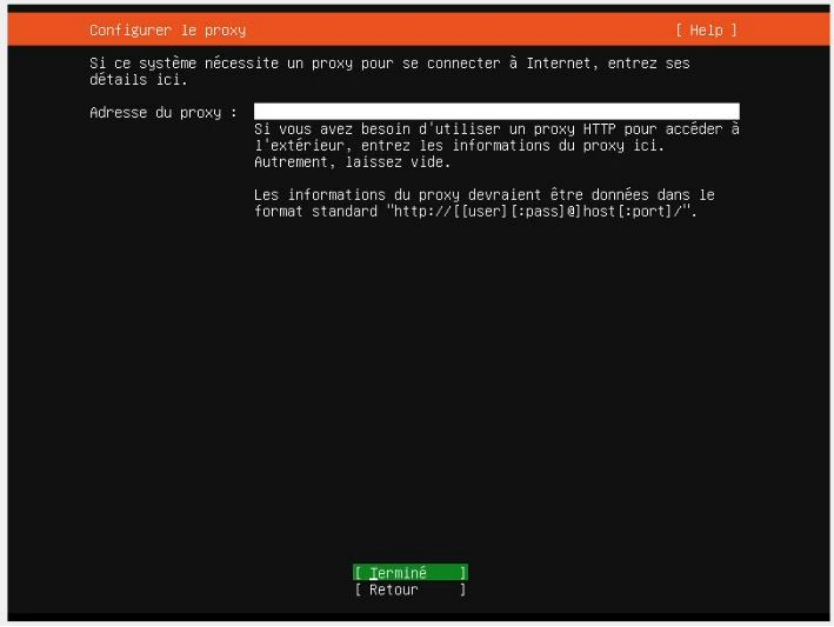
- Terminé



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 :

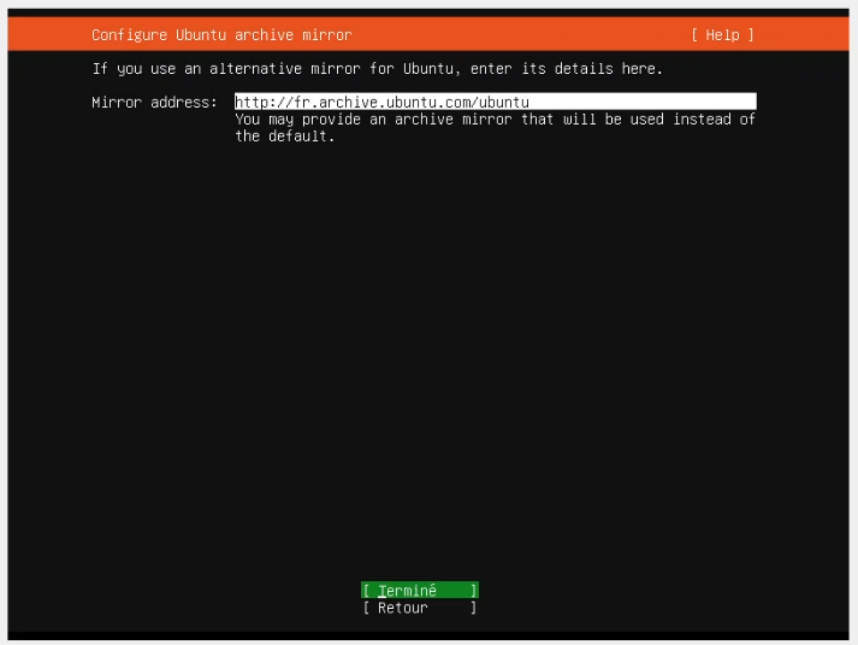
- Terminé



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

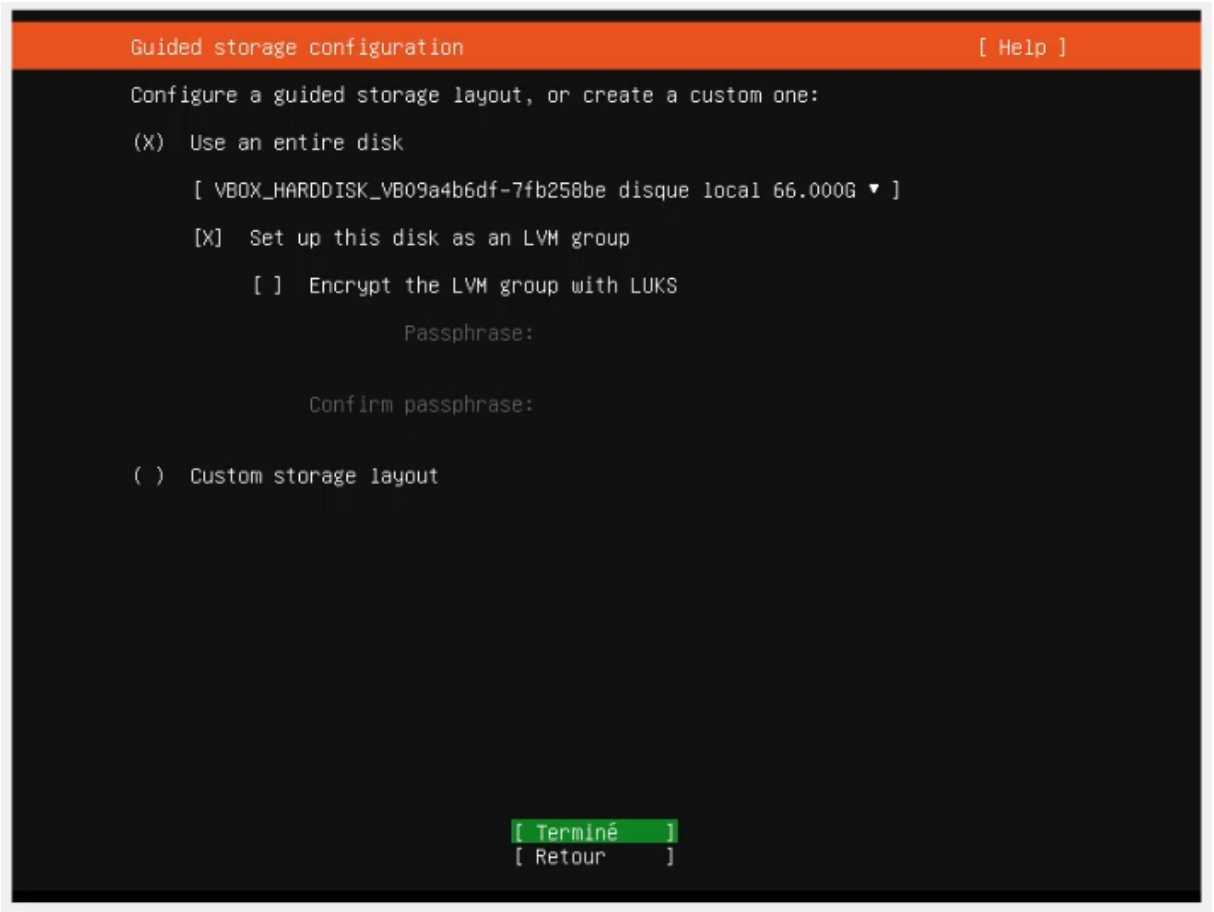
Vous pouvez configurer le partitionnement selon vos préférences, dans notre cas pour des besoins de démonstrations nous n'avons pas chiffrer le disque mais puisque les données contenues peuvent être de nature confidentielle je vous recommande de le chiffrer.

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 :

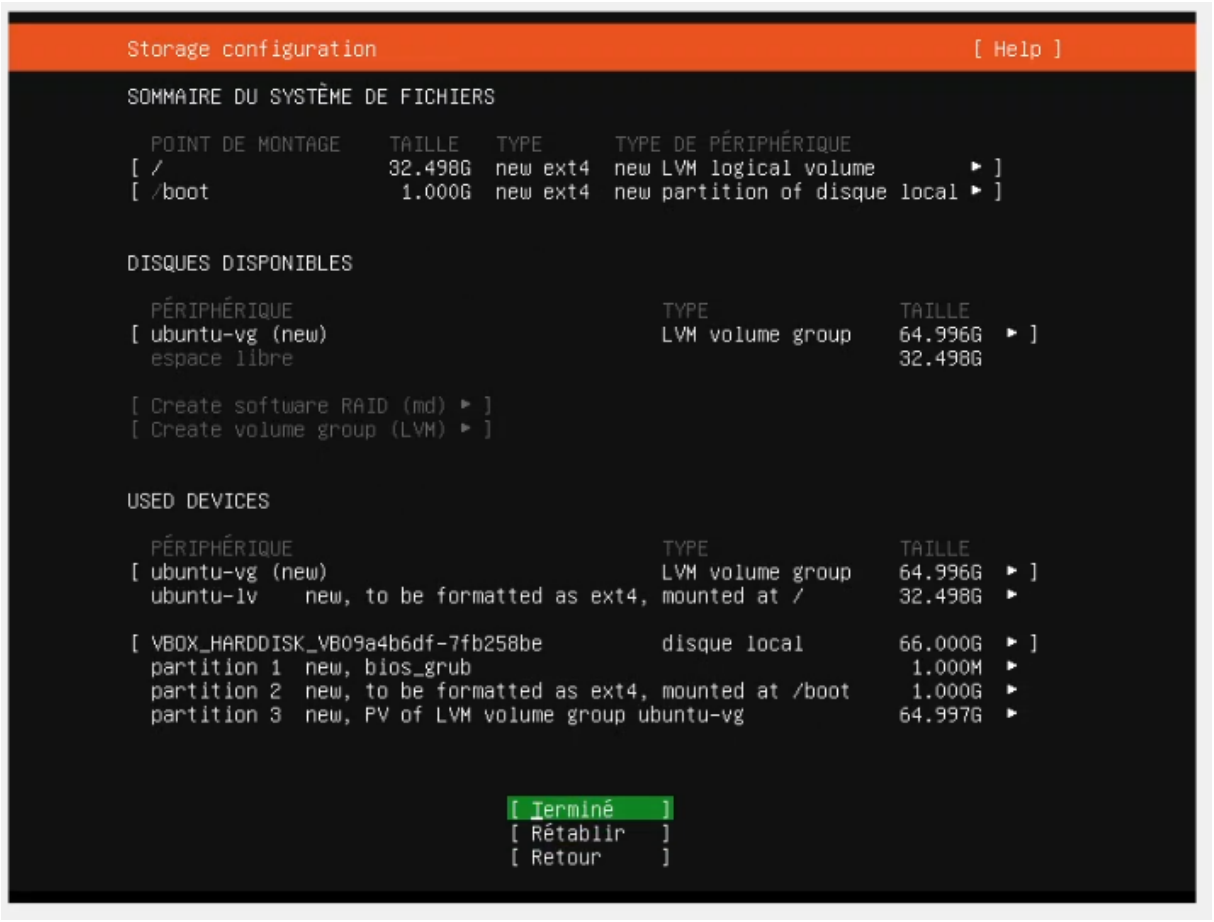
- Terminé



3.1.8 Configuration du stockage

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

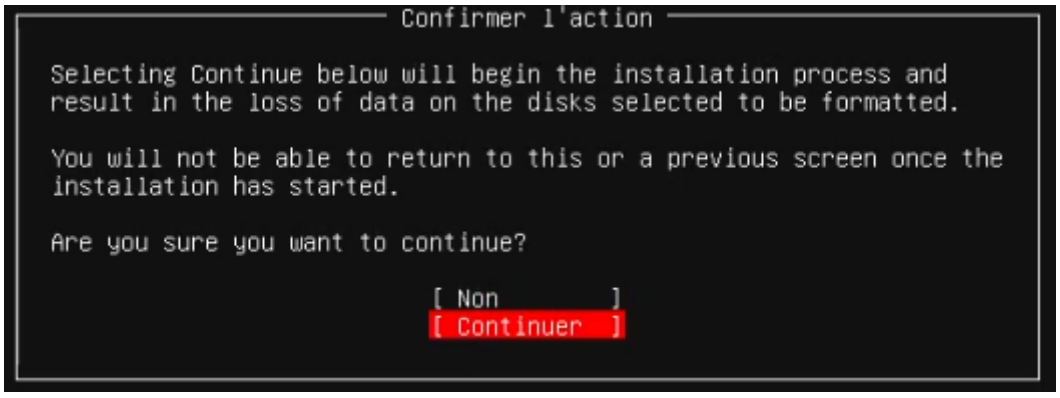
- Terminé



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



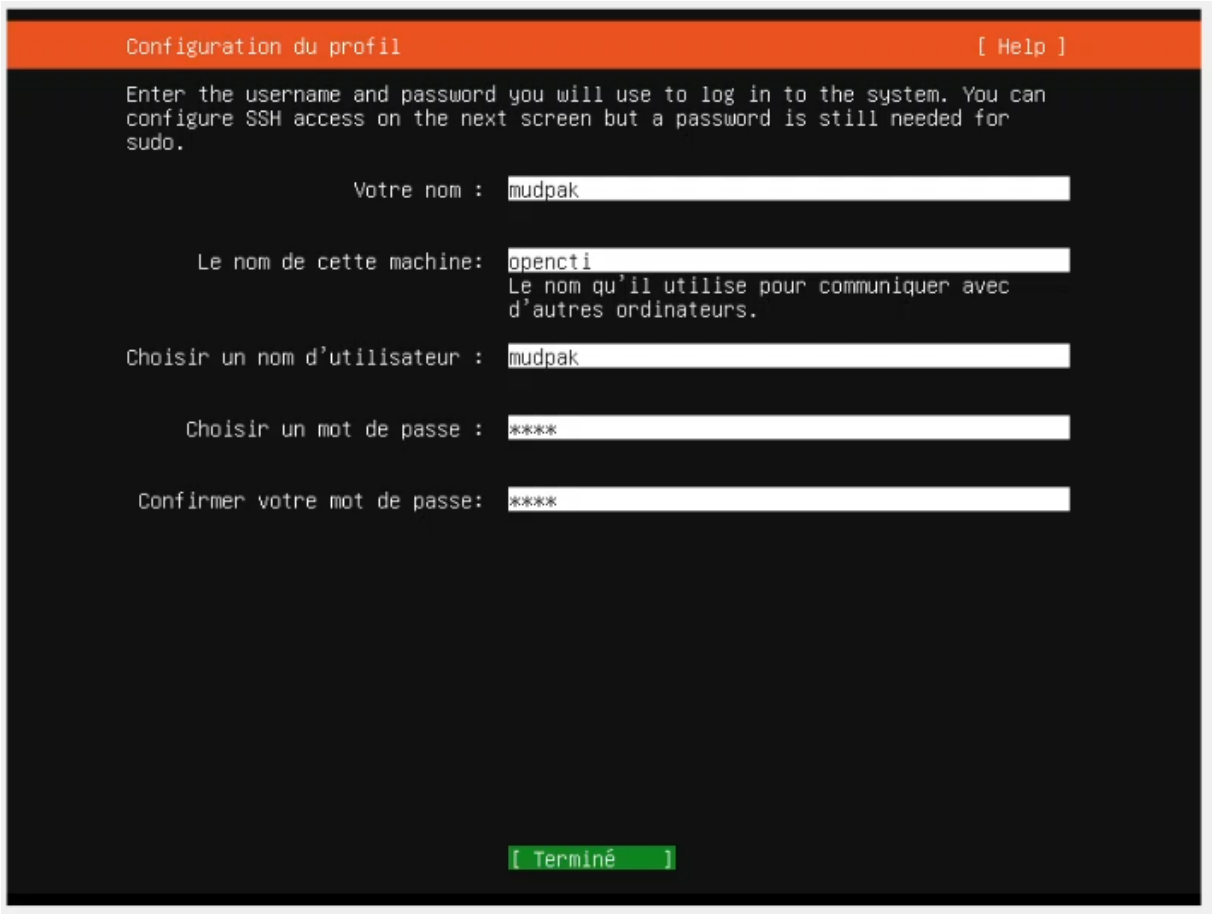
3.1.10 Configuration du profil

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



3.1.11 SSH Setup

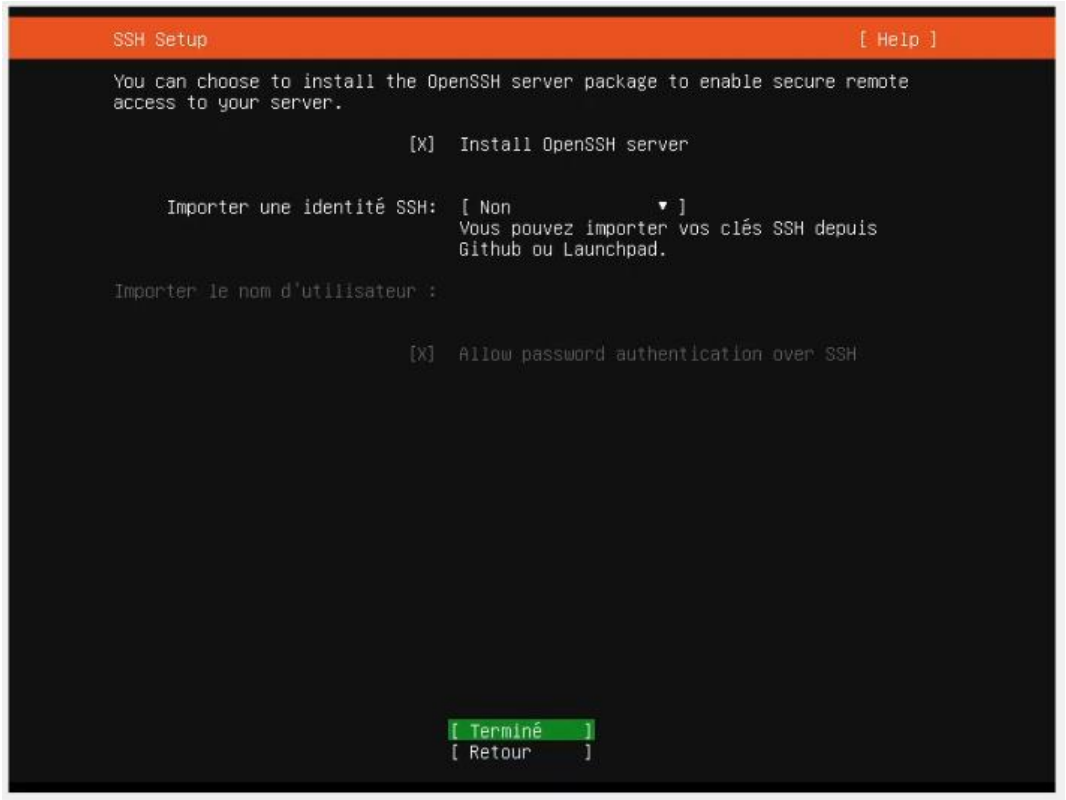
Pour des raisons de simplicité et d'administration je vous recommande fortement l'installation du serveur SSH qui vous permettra par la suite d'administrer le serveur à distance.

Sélectionner :

- Install OpenSSH server

Sélectionner :

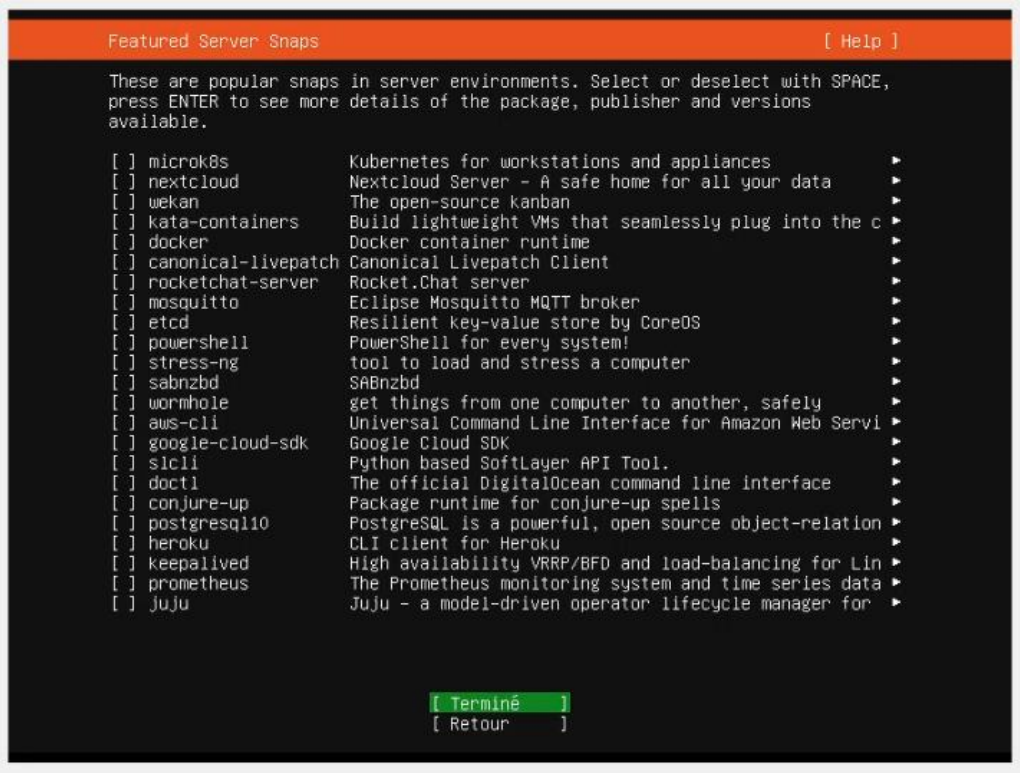
- Terminé



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

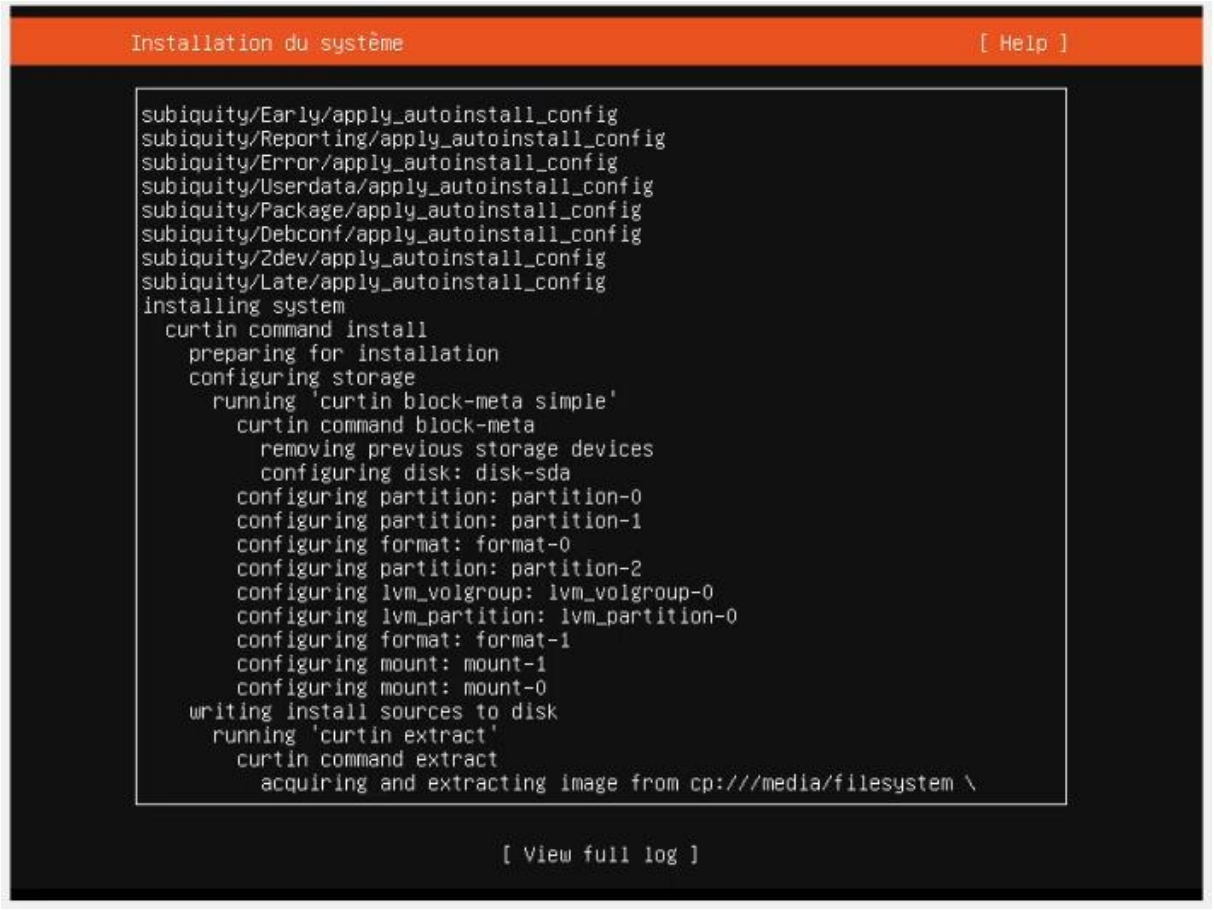


3.1.13 Installation du système

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

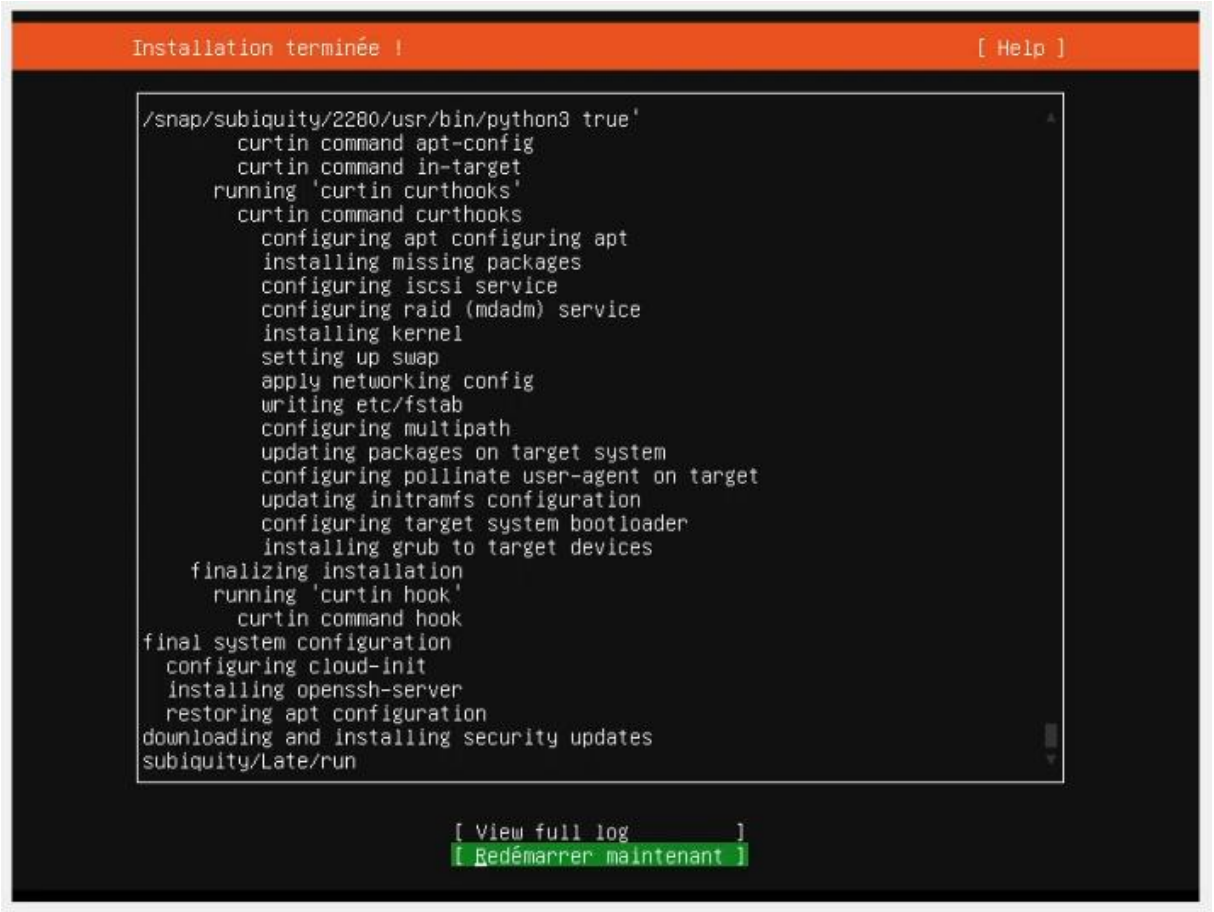


3.1.14 Installation terminée !

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

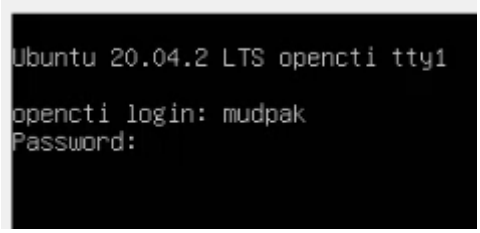
- Redémarrer maintenant

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



3.1.15 Première connexion

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



3.1.16 Configuration IP

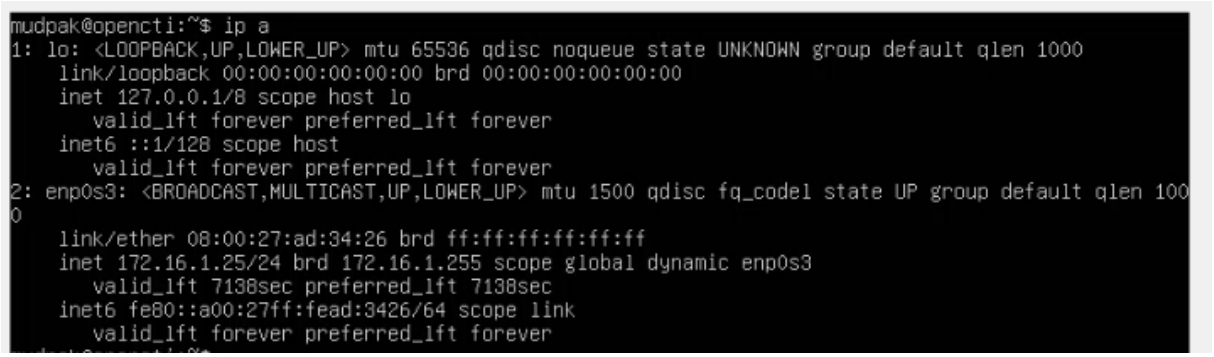
Puisque nous avons choisi l'installation du serveur SSH pour administrer la machine à distance, il nous faut son adresse IP, pour l'obtenir saisir la commande :

- 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.



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                                    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.
```

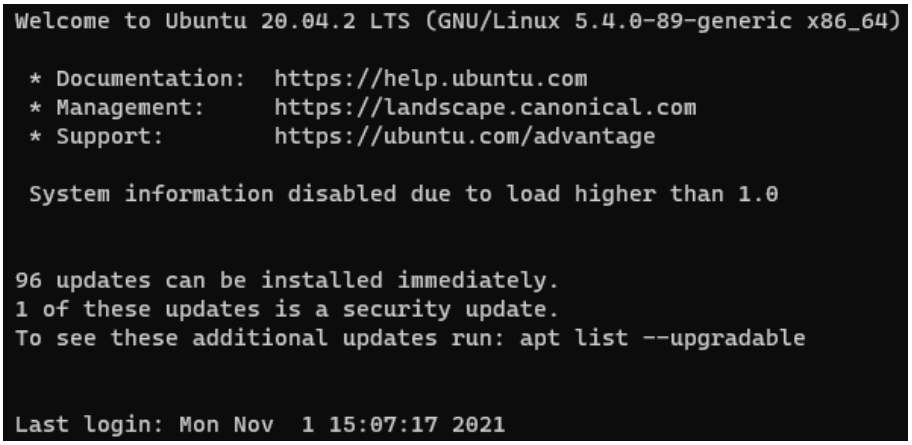
Vous êtes invité à saisir le mot de passe du compte utilisateur, saisir le mot de passe et appuyer sur la touche

- « Entrée »

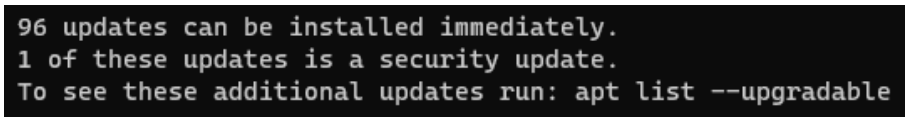
Remarque : si vous ne voyez pas le mot de passe que vous avez saisi c'est tout à fait normal, il s'agit d'une mesure de sécurité sous Linux.

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

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



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



3.3 Mise à jour de la liste des paquets

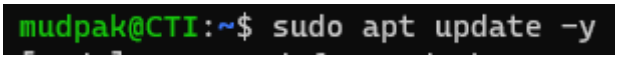
Maintenant que le système d'exploitation est installé et que nous sommes connectés à la machine, il faut en premier lieu procéder à la mise à jour.

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



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-crypto2 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 dirmngr friendly-recovery fwupd fwupd-signed gnupg gnupg-l10n gnupg-utils gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf gpgsm gpgv initramfs-tools
  initramfs-tools-bin initramfs-tools-core landscape-common libapt-pkg6.0 libasound2 libasound2-data libdrm-common libdrm2 libfwupd2 libfwupdplugin1 libglib2.0-0 libglib2.0-bin libglib2.0-data libldap-2.4-2
  libldap-common libnetplan0 libnss-systemd libpam-modules libpam-modules-bin libpam-runtime libpam-systemd libpam0g libpci3 libprocps8 libseccomp2 libsystemd0 libudev1 libxmlb1 linux-base login
  motd-news-config netplan.io networkd-dispatcher open-iscsi open-vm-tools passwd pciutils pollinate procps python-apt-common python3-apt python3-distupgrade python3-software-properties python3-twisted
  python3-twisted-bin python3-update-manager snapd software-properties-common sosreport systemd 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 dirmngr 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.tmpl ...
Installing new version of config file /etc/cloud/templates/resolv.conf.tmpl ...
```

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 1er 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-scan-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-docopt 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-docopt 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-docopt 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-docopt.
```

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
```

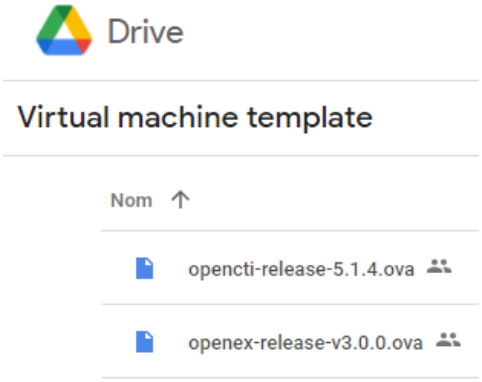
6. OpenCTI – Installation

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 fourni 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-88KbAit9GRZlL5Bj



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

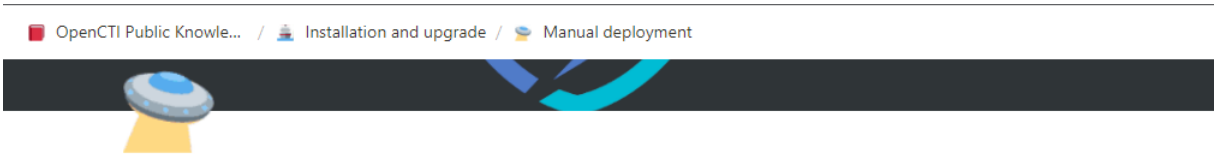
6.2 Via Terraform

Vous pouvez installer la solution via Terraform, pour cela je vous invite à vous référrer 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 !



Manual deployment

Prerequisites

Dependencies

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

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 crée

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

Pour nous déplacer dans le répertoire crée 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 ».

```
opencti:
  image: opencti/platform:5.1.3
  environment:
    - NODE_OPTIONS=--max-old-space-size=8096
    - APP__PORT=8080
    - APP__ADMIN__EMAIL=${OPENCTI_ADMIN_EMAIL}
    - APP__ADMIN__PASSWORD=${OPENCTI_ADMIN_PASSWORD}
    - APP__ADMIN__TOKEN=${OPENCTI_ADMIN_TOKEN}
    - APP__APP_LOGS__LOGS_LEVEL=error
    - REDIS__HOSTNAME=redis
    - REDIS__PORT=6379
    - ELASTICSEARCH__URL=http://elasticsearch:9200
    - MINIO__ENDPOINT=minio
    - MINIO__PORT=9000
    - MINIO__USE_SSL=false
    - MINIO__ACCESS_KEY=${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
```

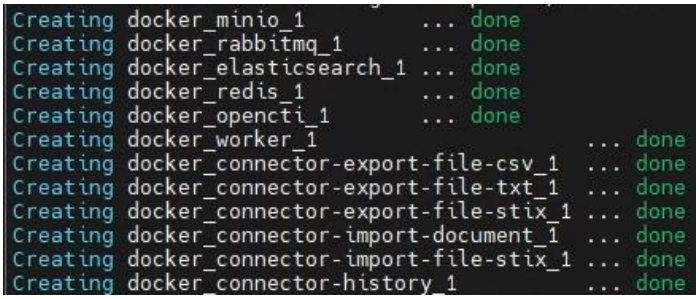
Docker applique la configuration du fichier « docker-compose.yml », dans le cas présent la création d'un réseau, des volumes, téléchargement des containers sont réalisées.

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

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.



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.

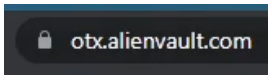
7.1 AlienVault OTX

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 :

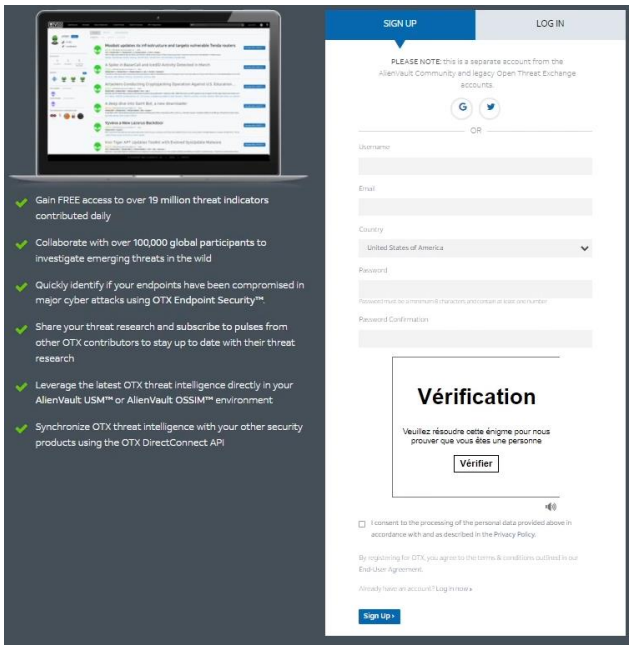
- Username : par un pseudonyme contenant entre 8 à 30 caractères
- Email : une adresse email valide pour confirmer la création de votre compte
- Country : par votre pays
- Password : un mot de passe robuste
- Password Confirmation : saisir à nouveau le mot de passe pour être certain
- Vérifier : cliquer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

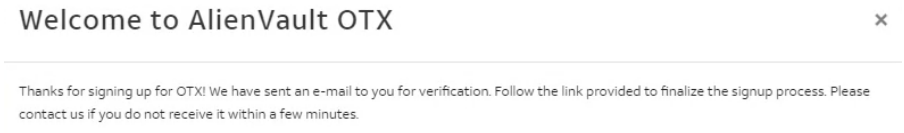
Cliquer sur

- Sign Up

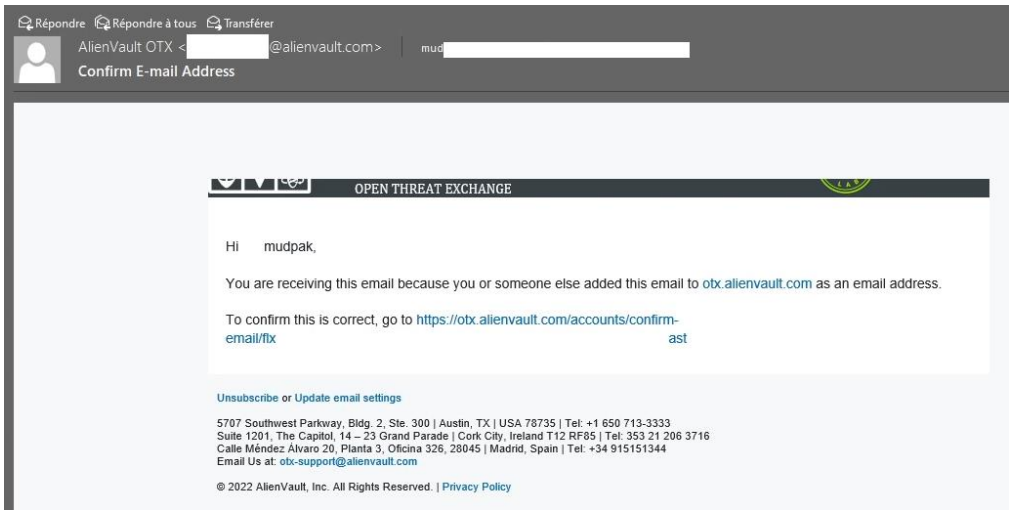


7.1.2 Welcome to AlientVault OTX

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 :

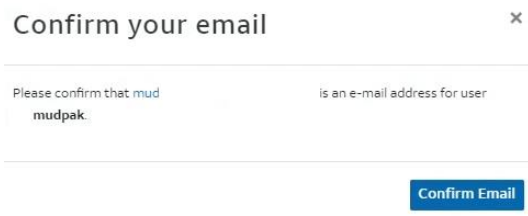


Voici un exemple de mail que vous recevez et il faut cliquer sur le lien fourni pour procéder à la vérification du compte :



Cliquer sur

- Confirm Email



Le compte est désormais confirmé et nous pouvons nous connecter :

7.1.3 LOG IN

Cliquer sur

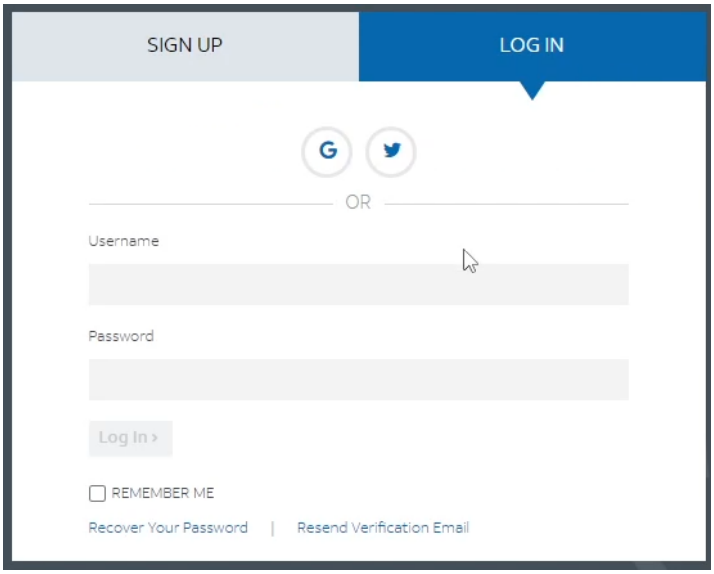
- Log In

Remplir les champs

- Username
- Password

Cliquer sur

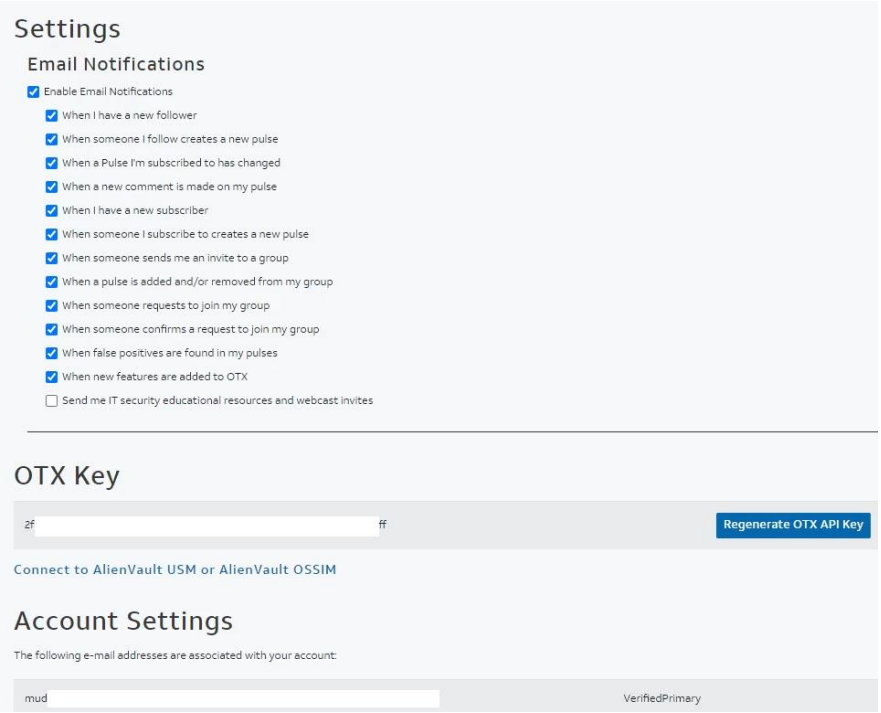
- Log In



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 sur car par la suite nous allons en avoir besoin.



7.1.4 Ajout du connecteur

Voici la configuration par défaut du connecteur AlienVault OTX :

```yaml
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=[redacted]
ALIENVAULT_OTX_API_KEY=2f[redacted]ff
```

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

```yaml
version: '3'
services:
  connector-cve:
    image: opencti/connector-cve:5.1.4
    environment:
      - OPENCTI_URL=http://localhost:8080
      - OPENCTI_TOKEN=ChangeMe
      - CONNECTOR_ID=ChangeMe
      - 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
```

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 :

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-urlhaus_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_opencti_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 :

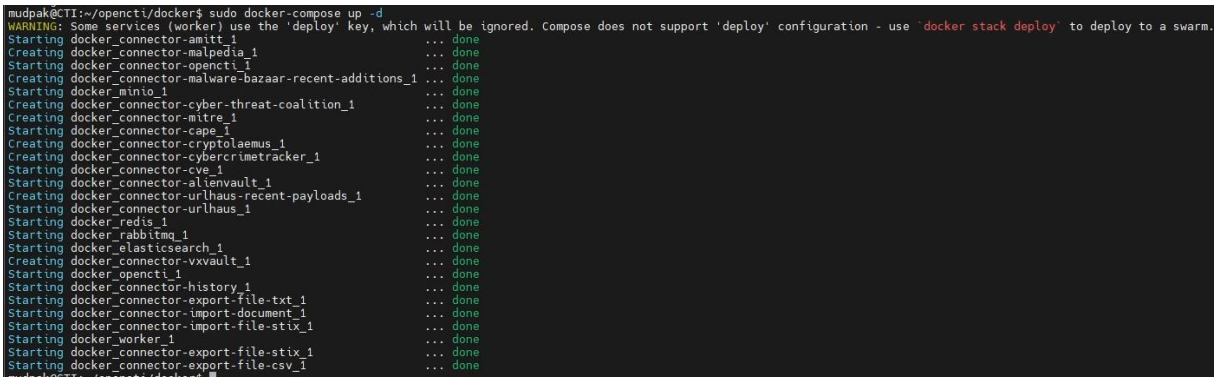
- sudo docker-compose pull

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...nnector-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-urlhaus                     ... 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-urlhaus-recent-payloads     ... pull complete
Pulling connector-vxvault                     ... done
```

Pour démarrer la stack saisir la commande suivante :

- sudo docker-compose up -d



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

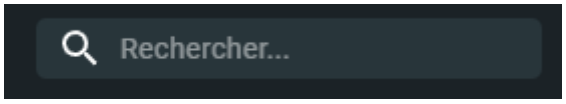
- S’IDENTIFIER

10.2 Tableau de bord

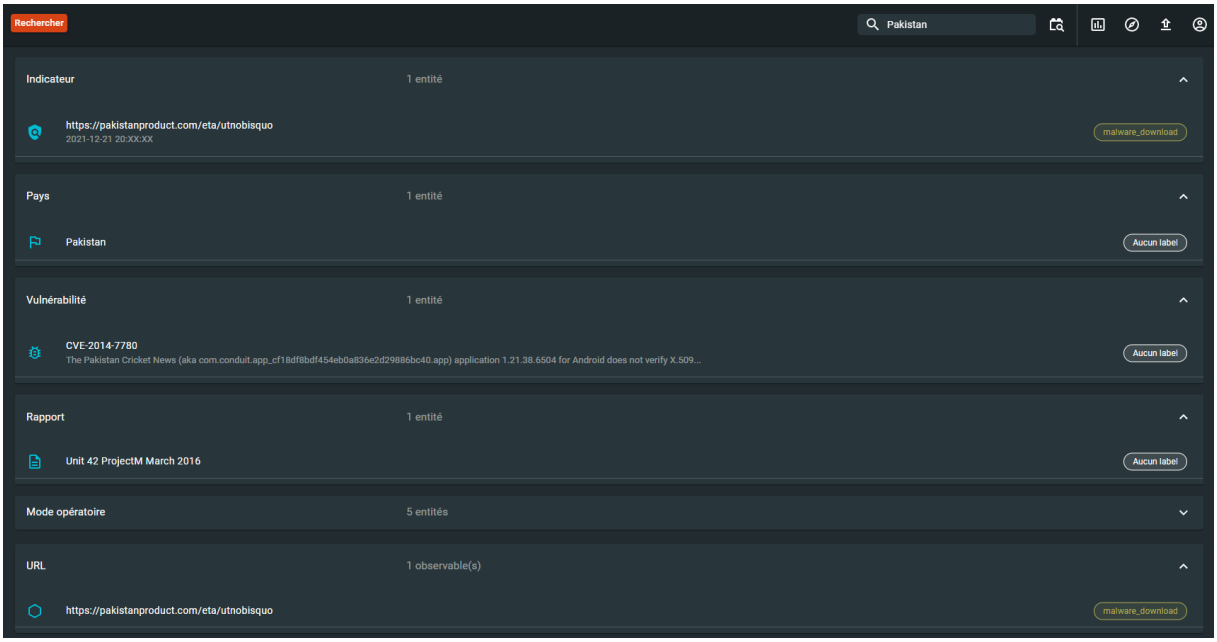
Commençons par le tableau de bord :

10.2.1 Recherche

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

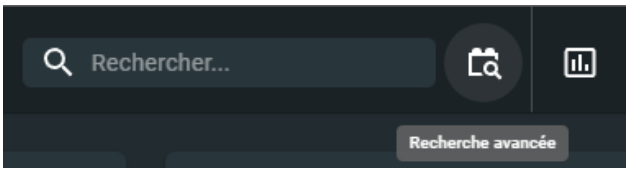


L'avantage de ce menu c'est qu'on peut chercher tous types d'éléments sans avoir à préciser de paramètres spécifiques :



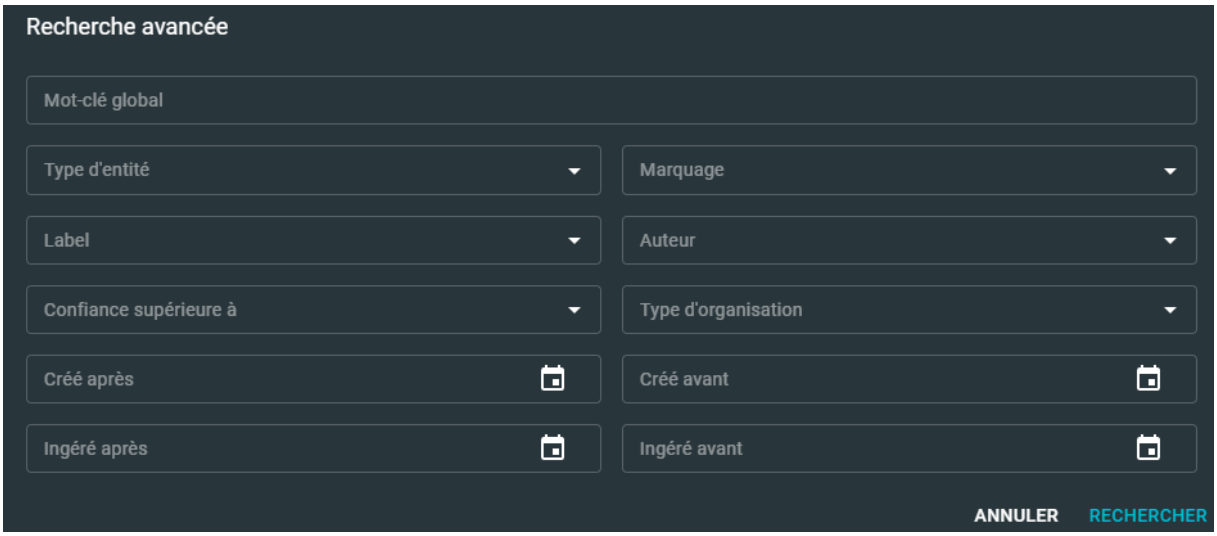
10.2.2 Recherche avancée

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



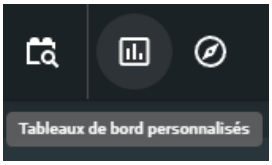
Nous pouvons chercher les éléments via les critères suivants :

- 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
- Crée 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 :
- Crée avant : rapport crée avant une certaine date
- Ingéré avant : ingestion dans la plateforme avant une certaine date



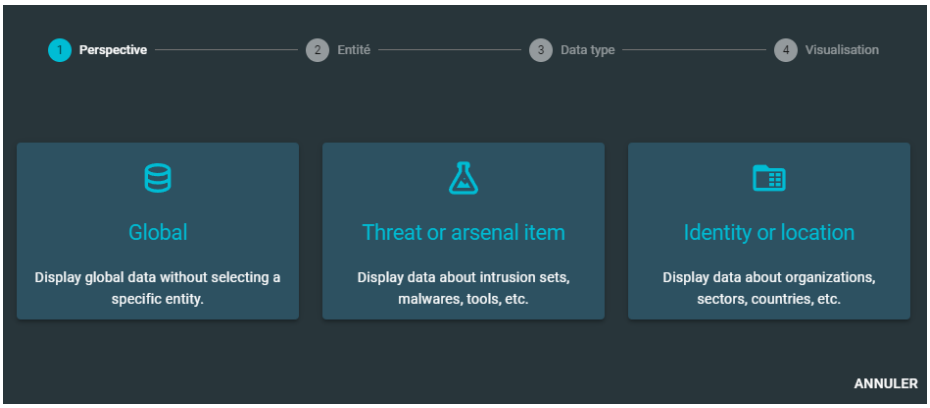
10.2.3 Tableaux de bords personnalisés

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

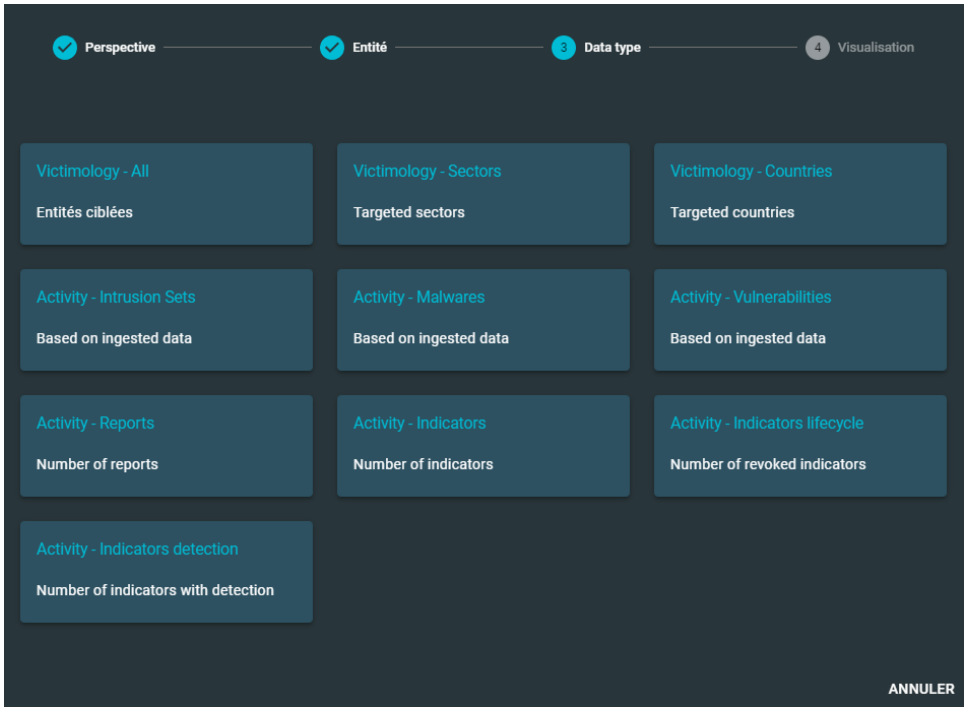


Il est possible de créer des tableaux de bords via différents critères tels que :

- 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

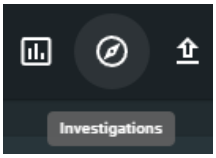


Selon le choix précédent, les données pourront être représentées sous différentes formes :



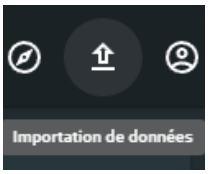
10.2.4 Investigations

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



10.2.5 Importation de données

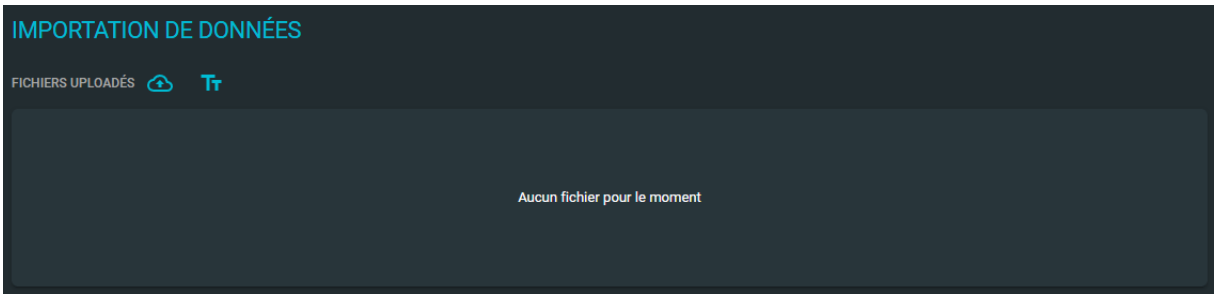
Nous pouvons importer des données manuellement :



10.2.5.1 Fichiers uploadés

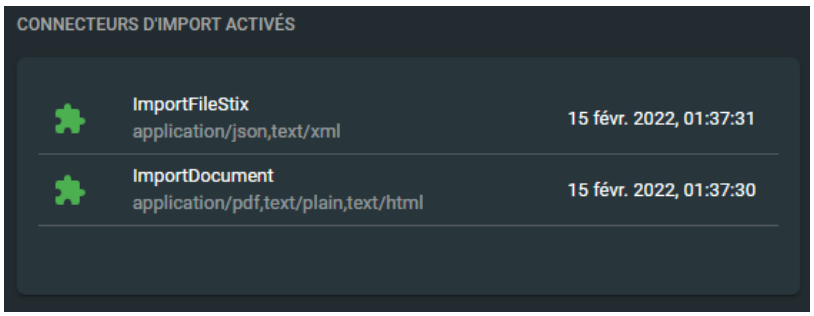
Nous pouvons uploader des fichiers :

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



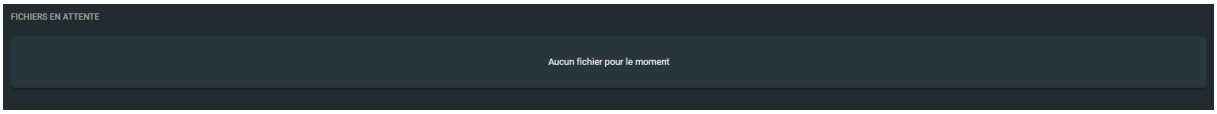
10.2.5.2 Connecteurs d'import activés

Nous pouvons voir que les connecteurs sont bien actifs :



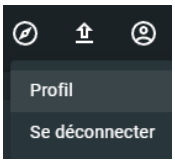
10.2.5.3 Fichiers en attente

Si des fichiers sont en attente ils seront listés ici :



10.2.6 Profil

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

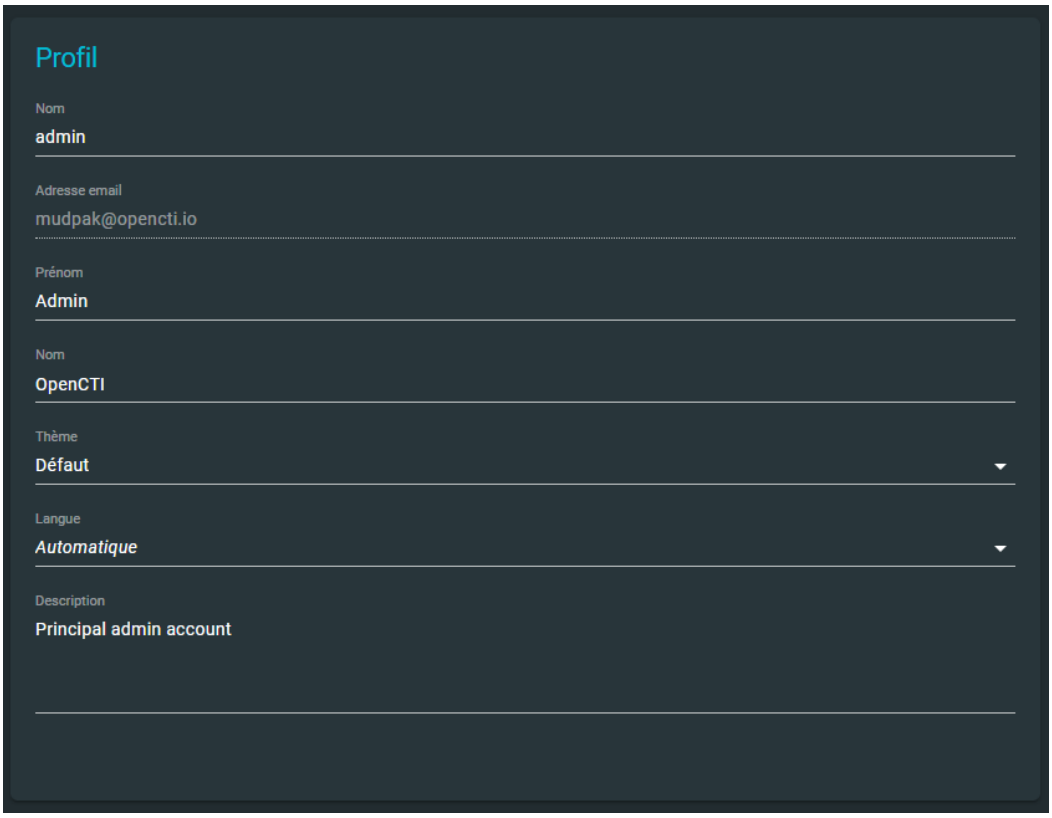


10.2.6.1 Profil

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

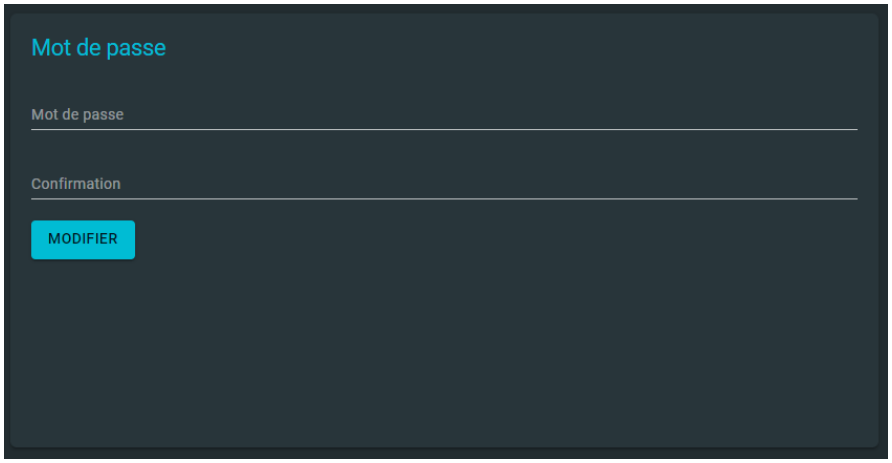
Dans le cas présent nous pouvons constater que le compte actuel :

- 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



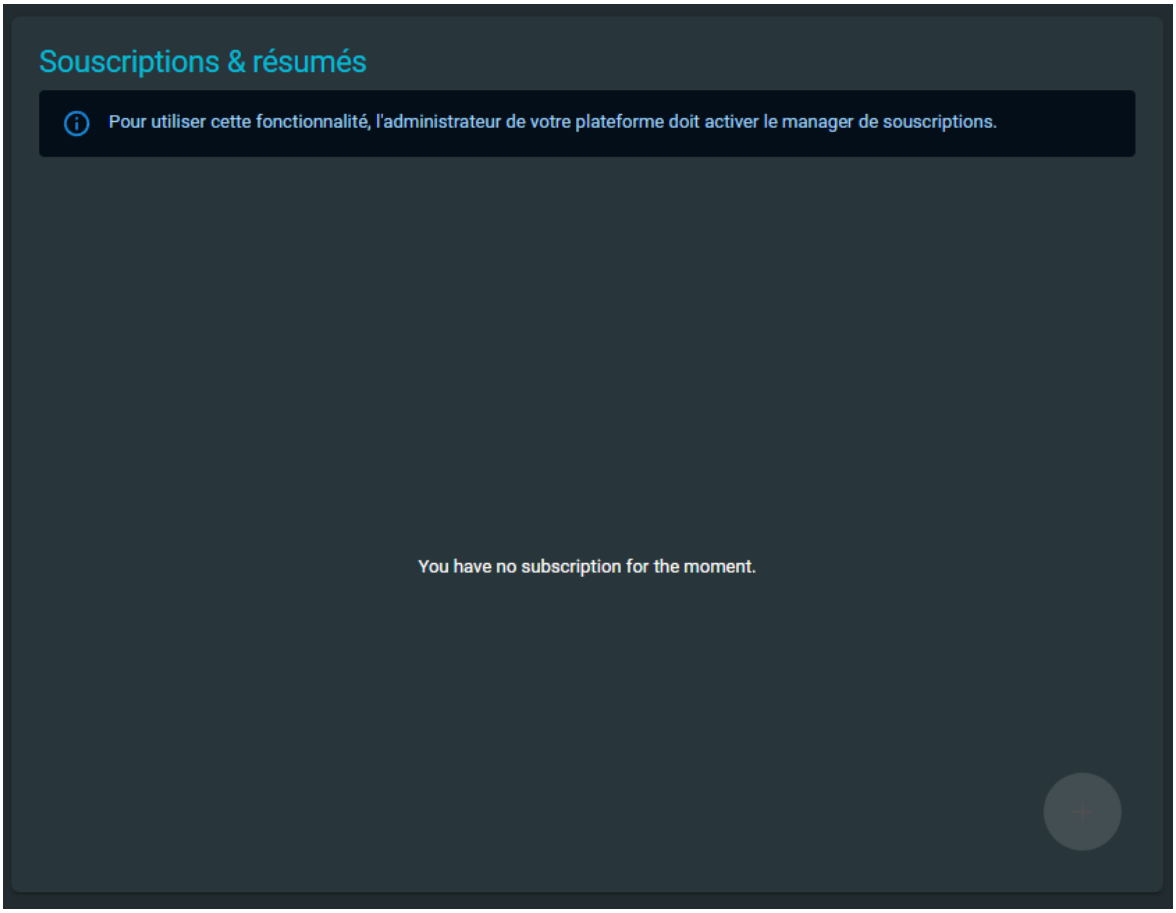
10.2.6.2 Mot de passe

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



10.2.6.3 Souscriptions & résumés

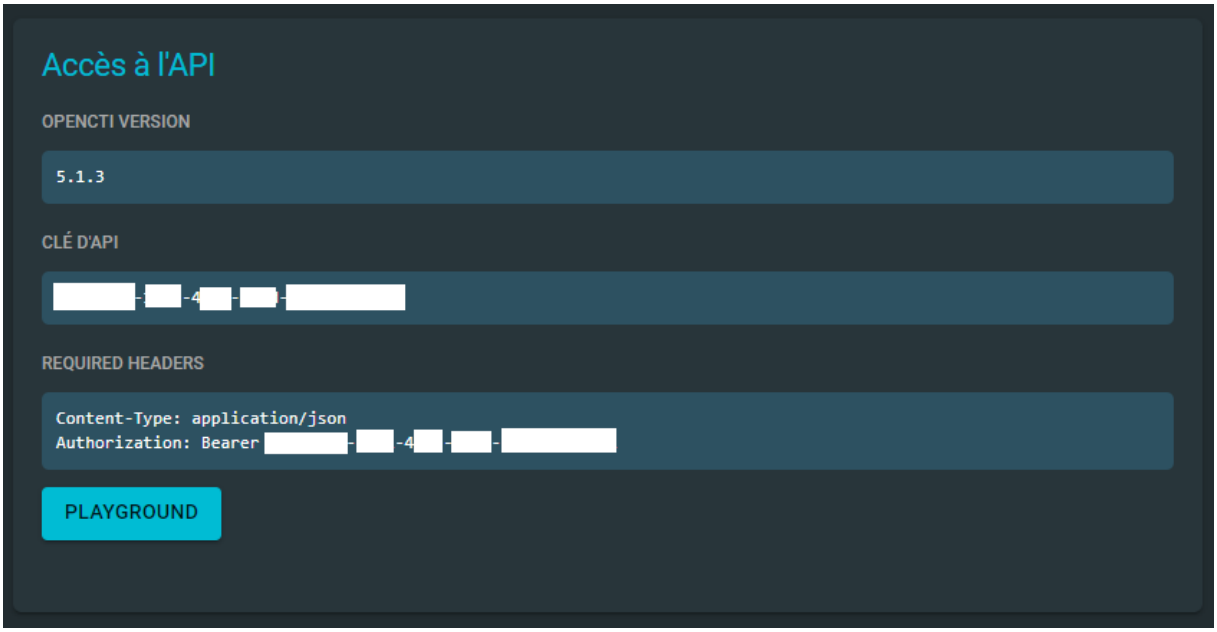
Feature qui permet de souscrire a des envois de mails concernant certaines informations.



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 « GraphSQL ».

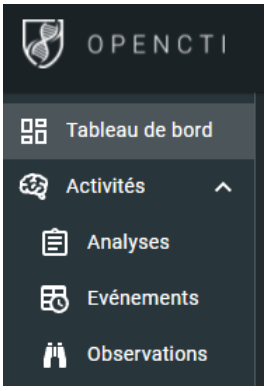


10.2.7 Se déconnecter

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 » :

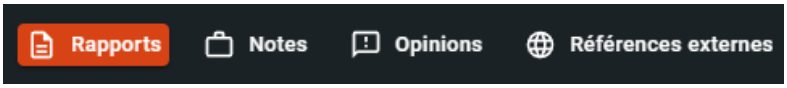


10.3.1 Analyses

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.

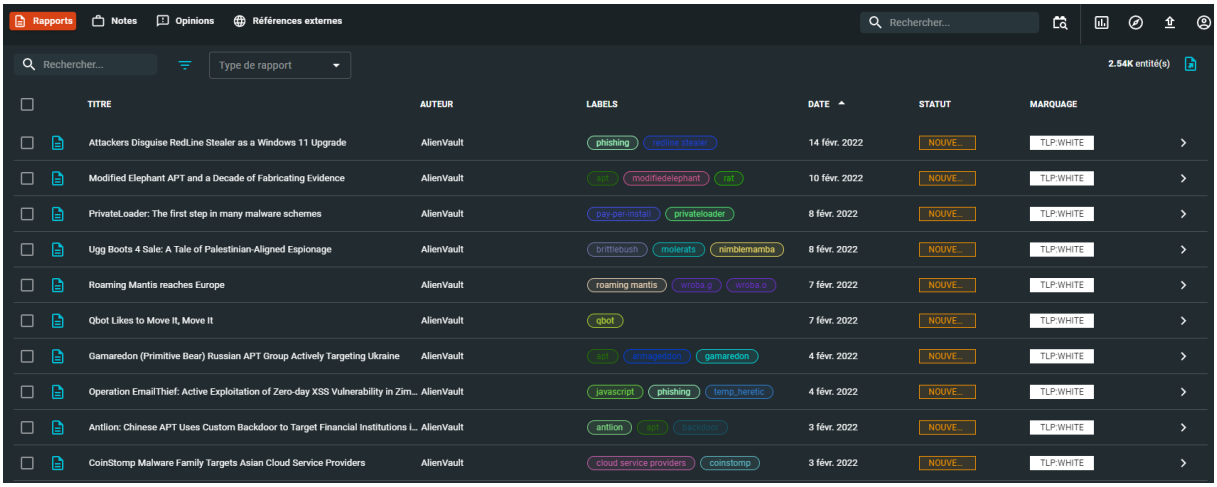
Ce menu est composé de sous-menus :

- Rapports
- Notes
- Opinions
- Références externes



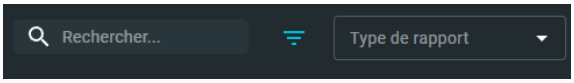
10.3.1.1 Rapports

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).

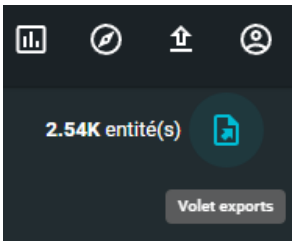


Deux types de filtres sont présents :

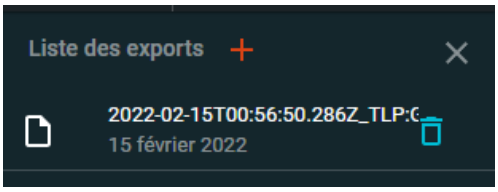
- Recherche
- Type de rapport



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 :

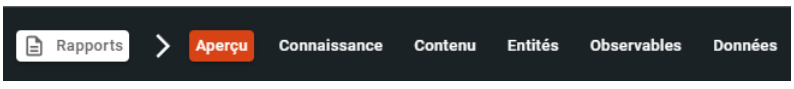


Voici un exemple d'export qui est prêt à être consulté :



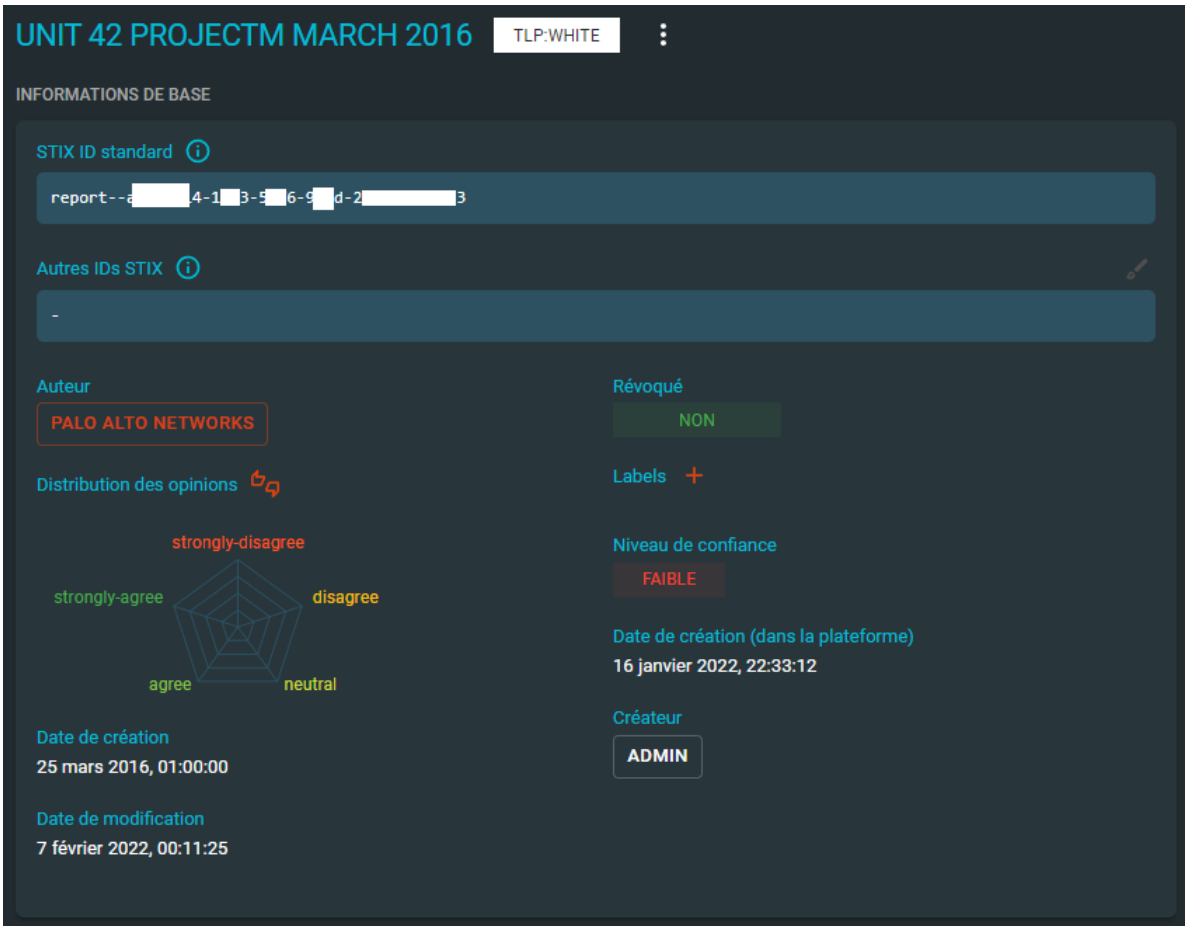
Pour visualiser la puissance de OpenCTI et ses fonctionnalités nous allons prendre le rapport « UNIT 42 PROJECTM MARCH 2016 » comme exemple.

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



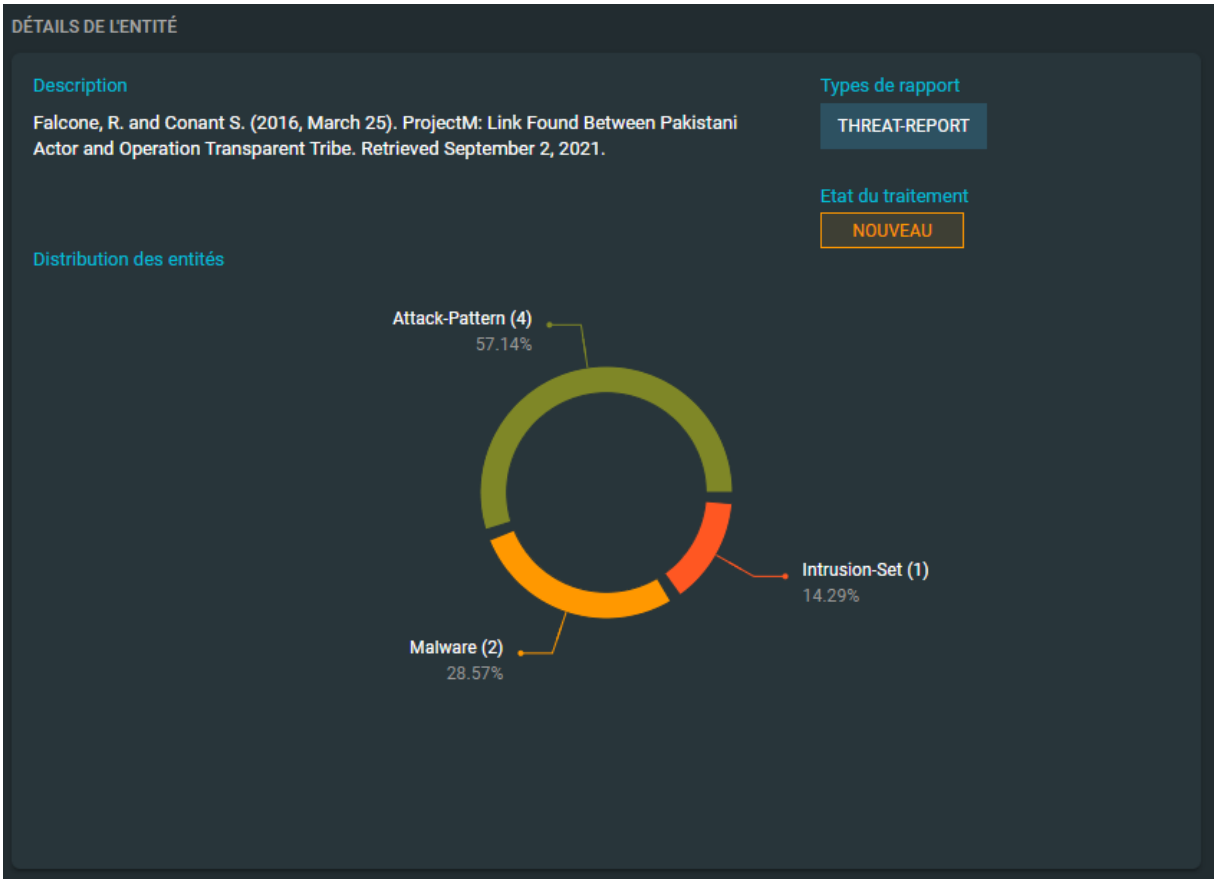
Dans la partie « Informations de base » nous pouvons voir les informations suivantes :

- 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

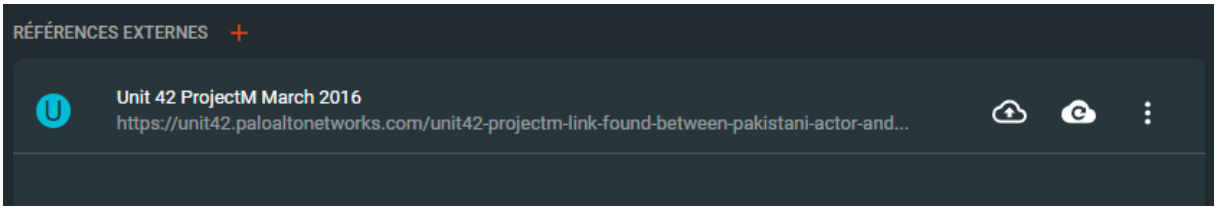


Dans la partie « Détails de l'identité » nous pouvons voir différentes informations :

- 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?

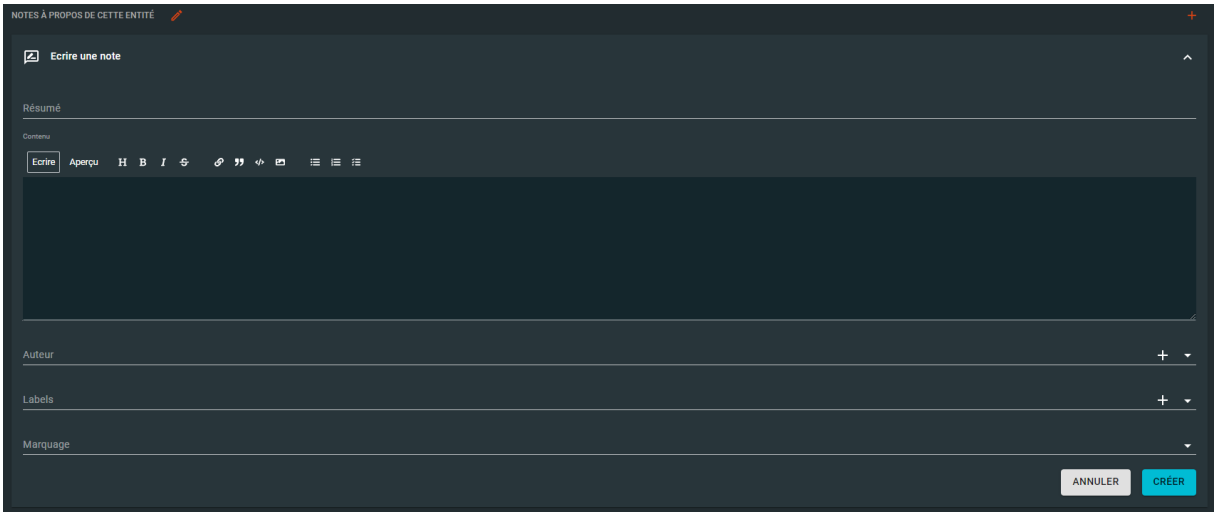


Dans la partie « Références externes » nous pouvons consulter des éléments pour compléter notre étude du rapport :

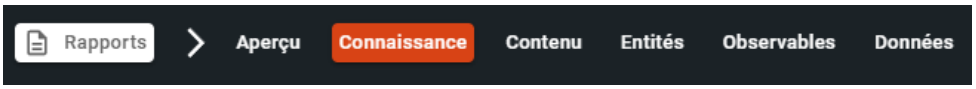


Dans la partie « Historique récent » nous pouvons voir les opérations qui ont été effectuées sur le rapport :

La dernière partie sur cette page « Notes à propos de cette entité » permet d'ajouter des éléments si on souhaite sous forme de note :

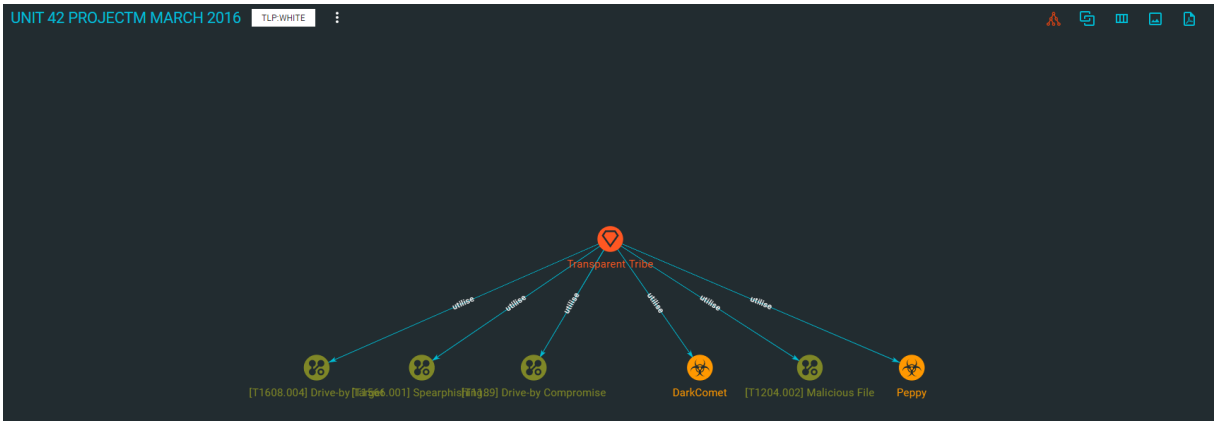


Explorons désormais la partie « Connaissances » du rapport :

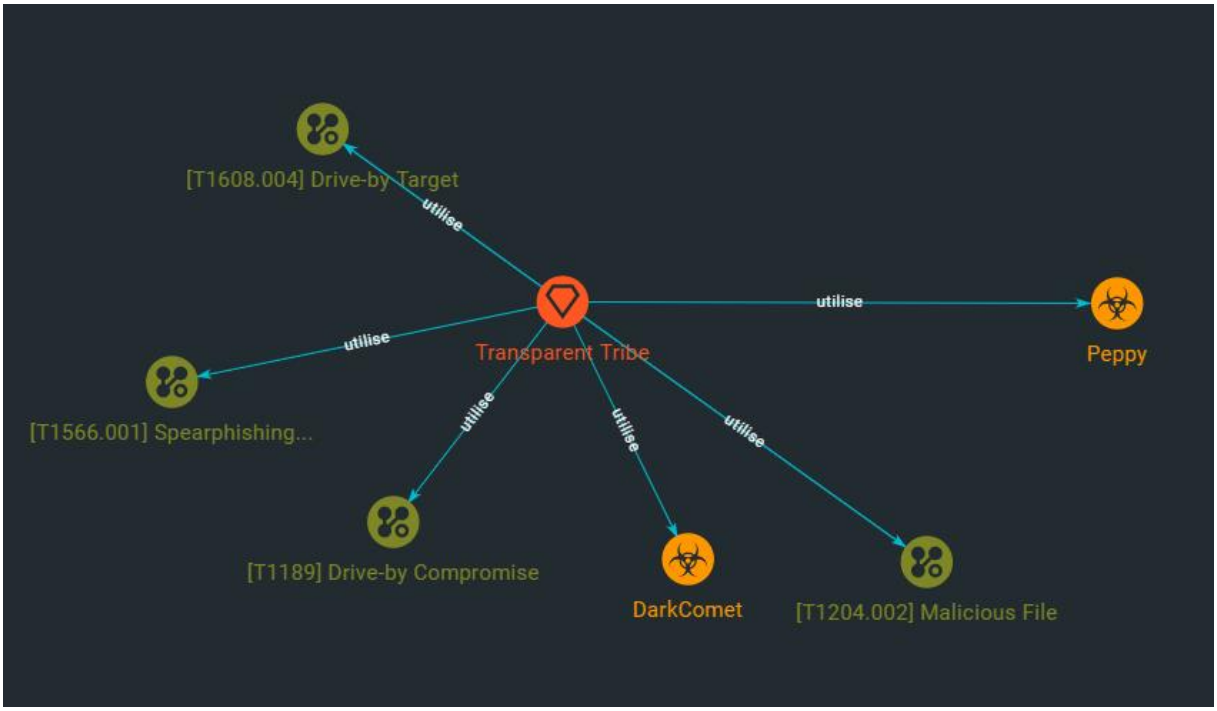


Nous pouvons voir un affichage sous forme de graphe et relations entre les éléments, c'est une manière de représenter les éléments du rapport notamment les IOCs (=Indicator Of Compromission = Indicateurs de compromissions).

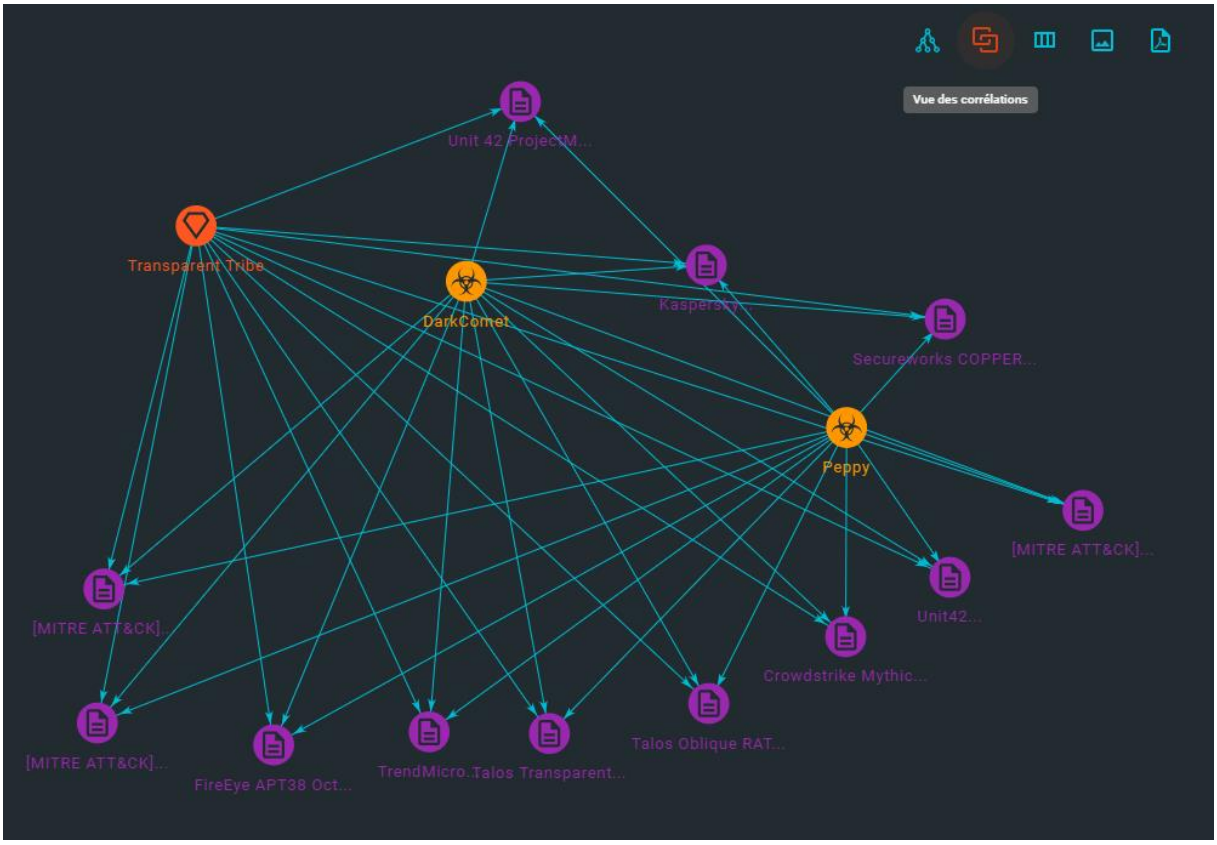
Parmi les éléments présents dans le graphe se trouve « DarkComet », c'est le moment idéal de saluer le bro Jean-Pierre LESUEUR (@darkcodersc) ! You The Best !! ;)



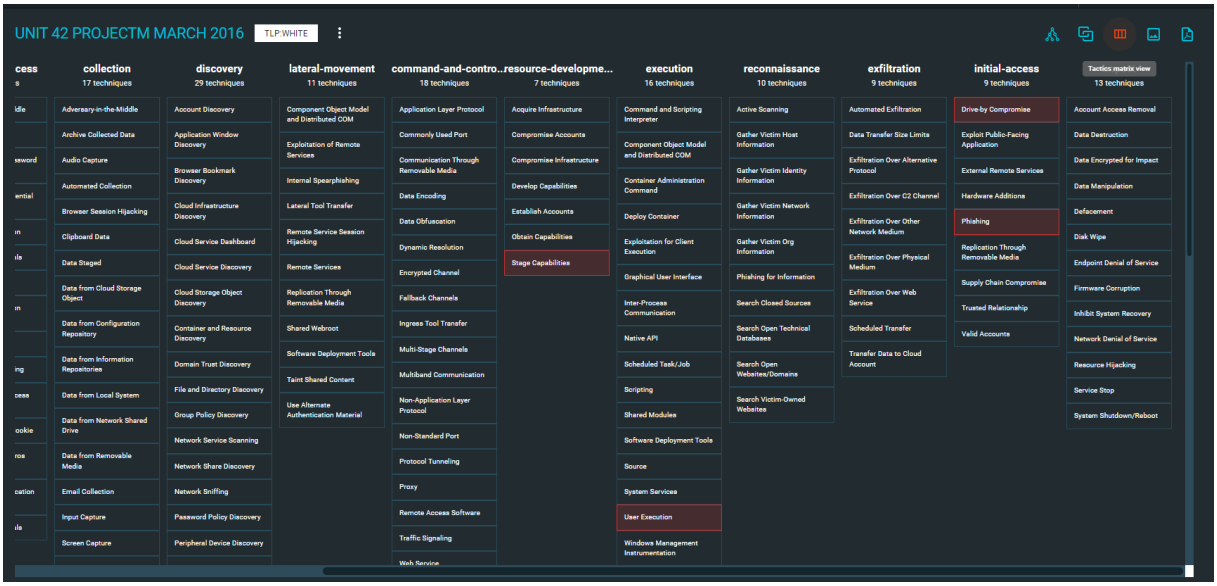
Le graphe étant tout à fait personnalisable, si nous avons du mal à visualiser certains éléments on peut les déplacer à souhait :



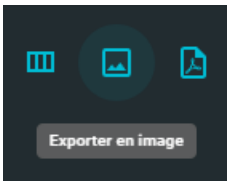
D’autres types de vues permettent d’avoir un visuel des relations de d’autres manières, comme c’est le cas de la « vue des corrélations » ci-dessous :



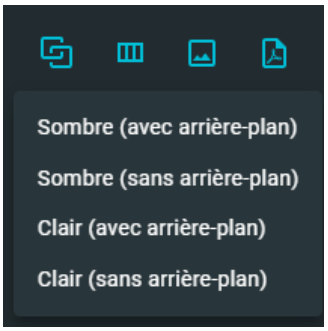
D’un point de vue Blue Team si nous souhaitons avoir comme base la MITRE & ATT&CK nous pouvons avoir le visuel « Tactics matrix view » ainsi les méthodes utilisées sont mises en avant via une couleur différente :



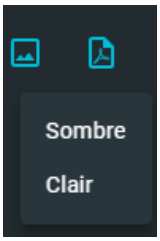
Quel que soit le visuel choisi nous pouvons exporter l'affichage en image :



Nous pouvons choisir parmi les différents types d'exports :

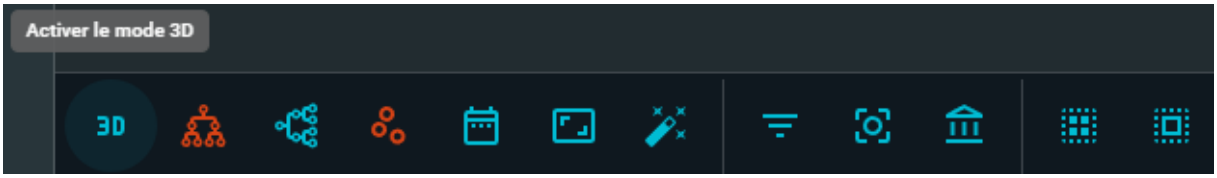


Il est également possible d'exporter le rapport au format PDF :

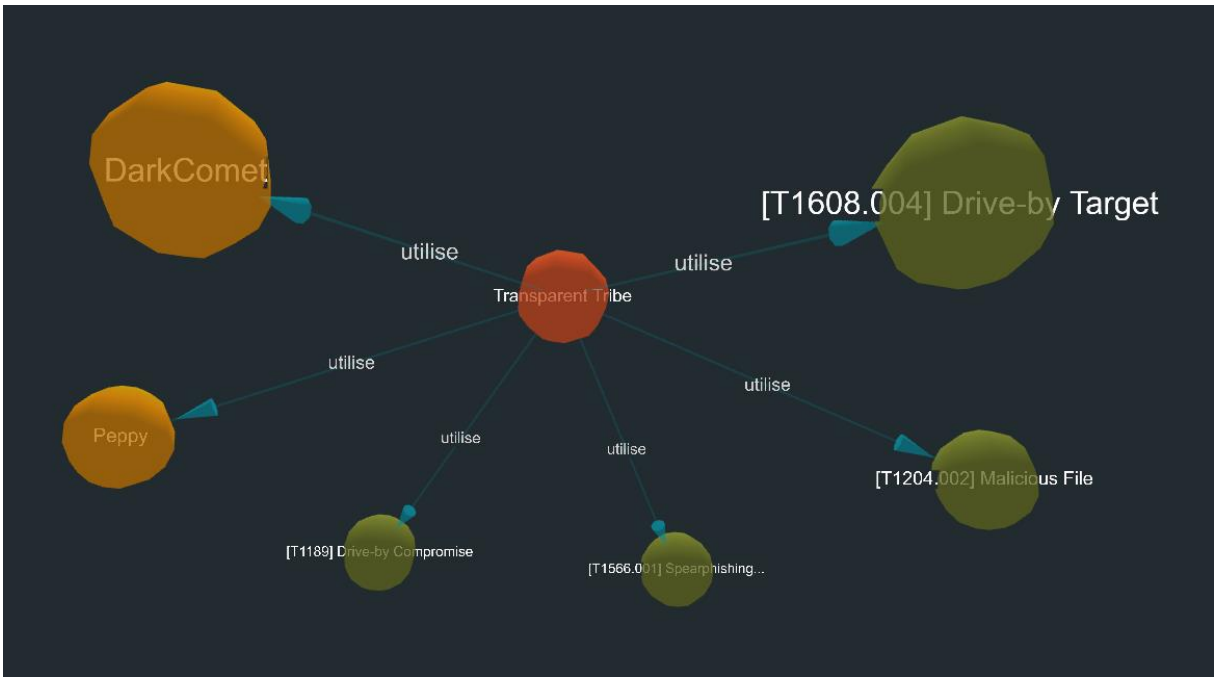


En plus du menu dans la zone supérieure, nous avons le menu de la zone inférieur qui permet d'effectuer d'autres opérations.

Nous pouvons afficher les relations sous forme 3D :



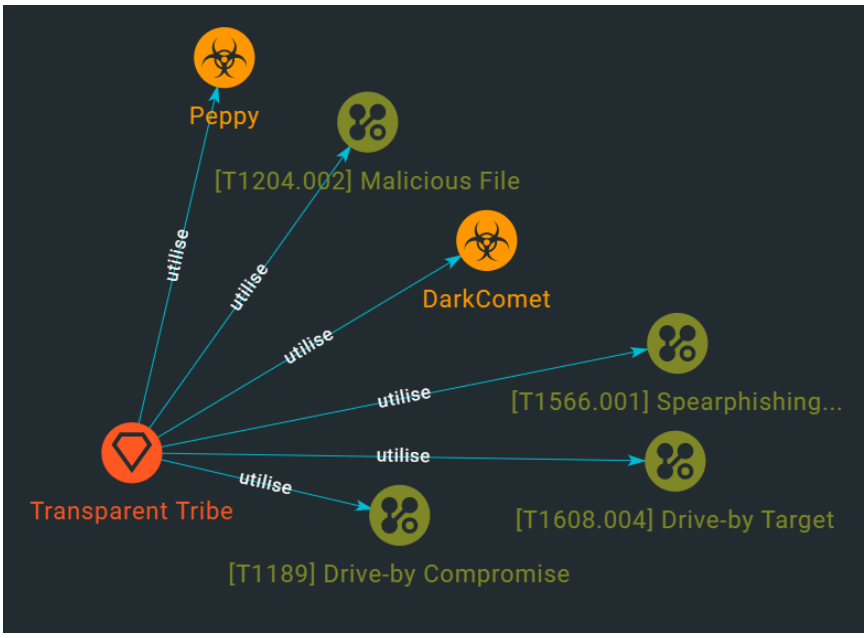
Voici un exemple de résultat qu'on peut obtenir :



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 :

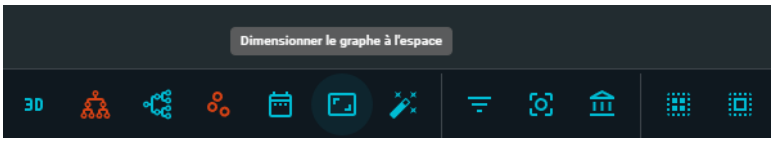


Il est possible de « désactiver les forces » chose que je vous déconseille car si vous déplacez les relations vous risquez de la superposer et puisque cette fonctionnalité n'est pas activée vous risquez de masquer des éléments :

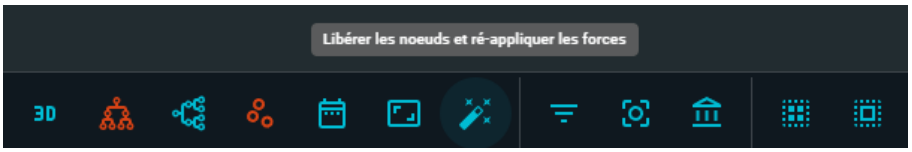
Vous pouvez « Afficher le sélecteur d'intervalle de temps » qui permet de connaitre la date exacte d'ajout de chaque élément au rapport !

En réalité il est possible de connaitre 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 :

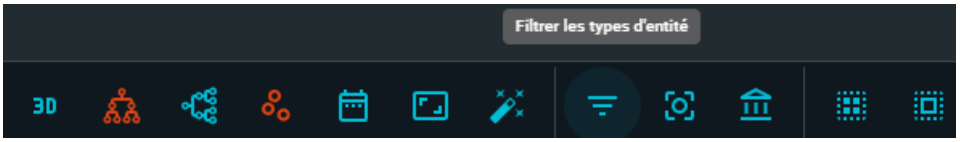


Si vous faites des opérations sur les relations, il se peut que l'affichage de celles-ci ne soit plus à celui d'origine, pour remettre à l'état d'origine les relations nous pouvons choisir d'utiliser la fonctionnalité « Libérer les nœuds et réappliquer les forces » :



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

- Code malveillant
- Mode opératoire
- Motif d'attaque



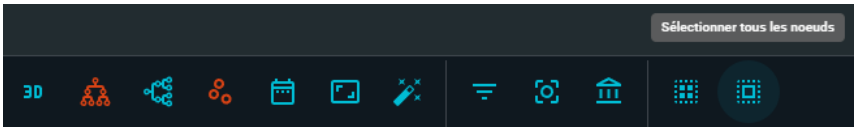
Si vous souhaitez « Filtrer les marquages » vous pouvez le faire via ce filtre, selon les types de marquages du rapport il vous sera possible de ne pas les afficher :

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

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

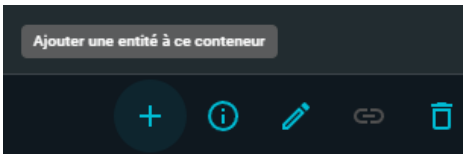
- Code malveillant
- Mode opératoire
- Motif d'attaque

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

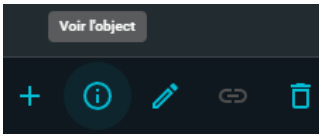


Sur cette page nous avons vu quasiment tous les éléments, il reste les options disponibles dans la zone inférieur droite de la fenêtre lorsque nous sélectionnant un élément du rapport :

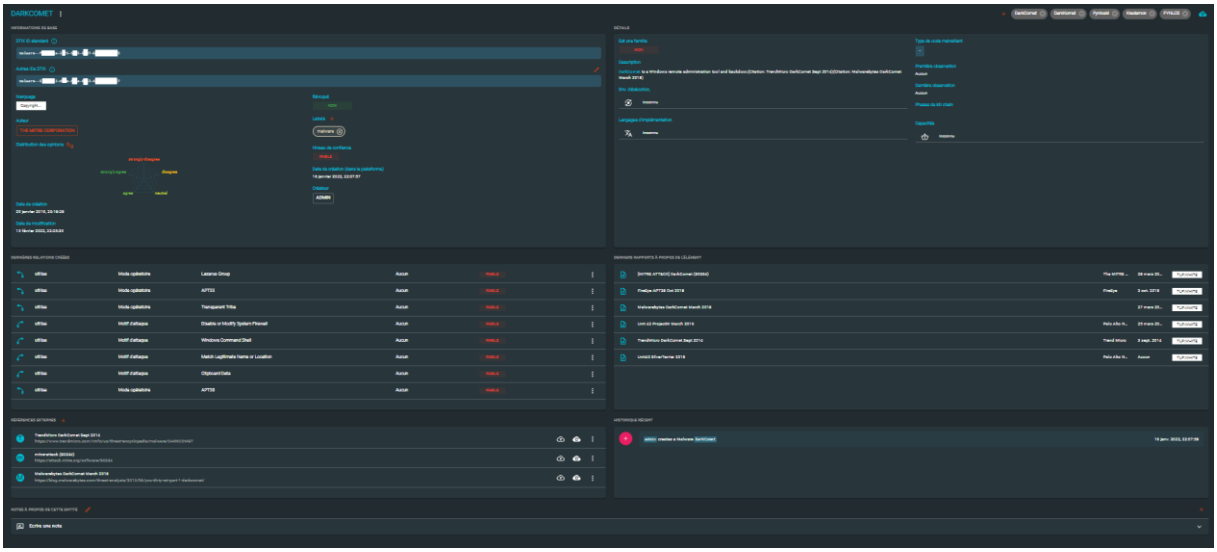
La première option permet d' « Ajouter une entité à ce conteneur » :



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

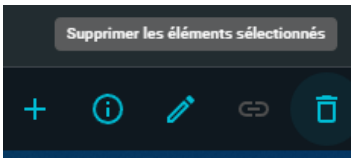


De la même manière qu'un « rapport » nous avons toutes les informations que l'élément :



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 :

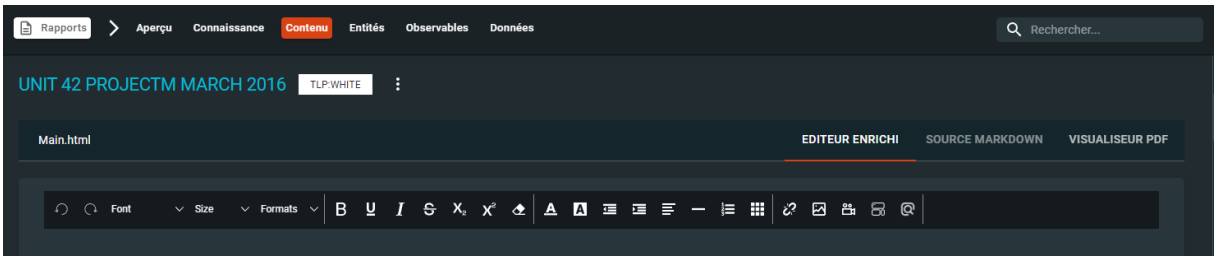


Jusqu'à ce stade nous n'avons parcouru « que » deux sous menus de la partie « Analyses », avec ces éléments nous avons déjà beaucoup d'éléments qui nous permettent de faire notre CTI.

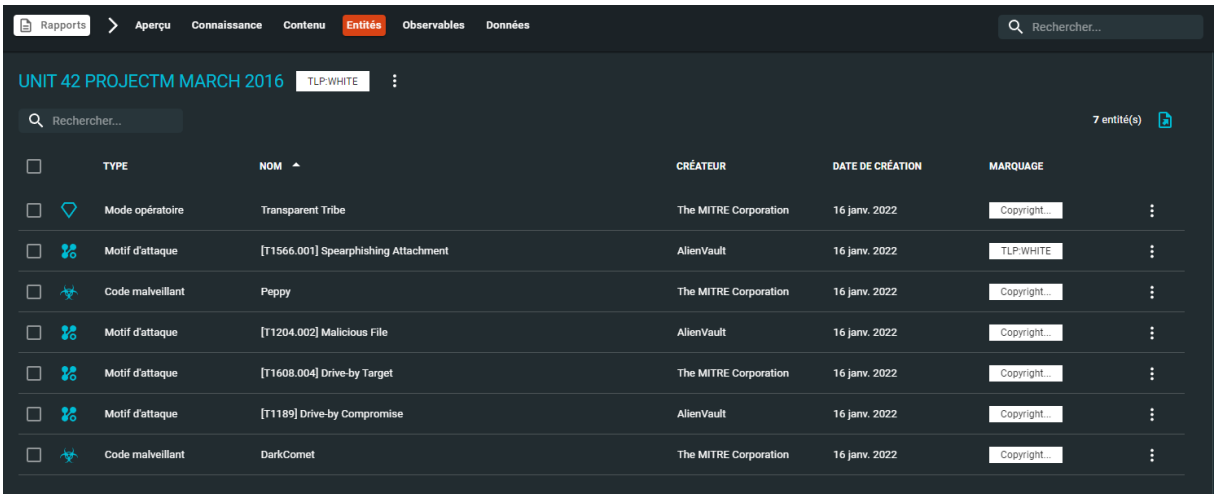
Mais pour compléter notre travail d'autres sous-menus vont nous aider.

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

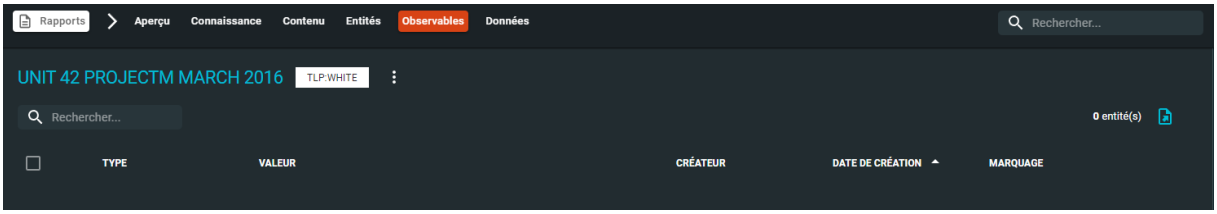
- EDITEUR ENRICHI : un éditeur de texte pour ajouter des éléments
- SOURCE MARKDOWN : non actif à cet instant
- VISUALISEUR PDF : non fonctionnel à cet instant



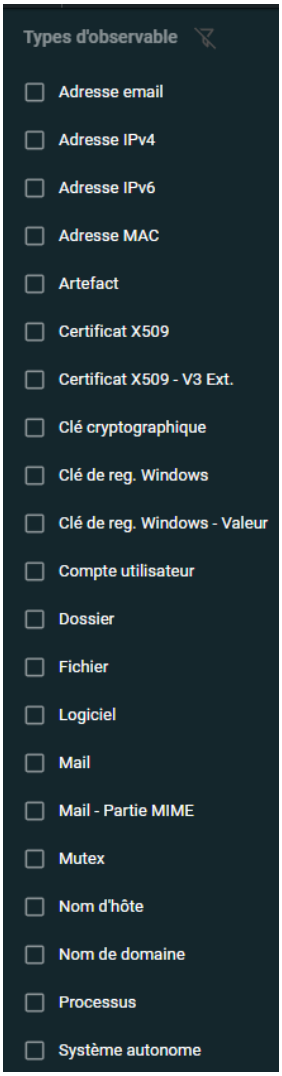
Dans le menu « Entités » nous retrouvons les mêmes informations que précédemment depuis la matrice MITRE ATT&CK ou d'autres visuels des relations car les données sont les mêmes mais représentées différemment :



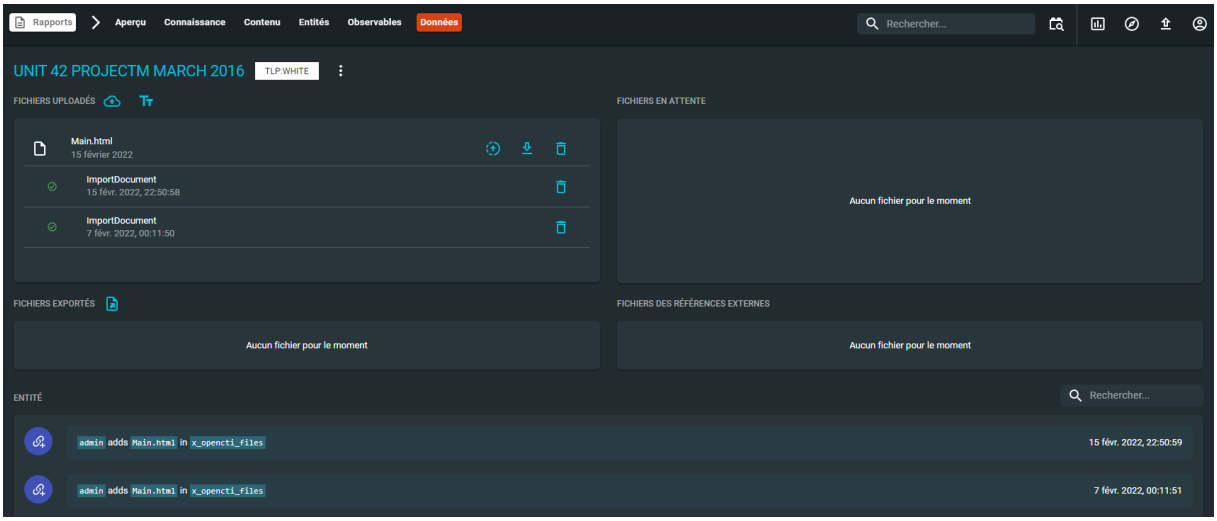
Dans la partie « Observables » doivent apparaitre les éléments en relation avec le rapport :



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 :

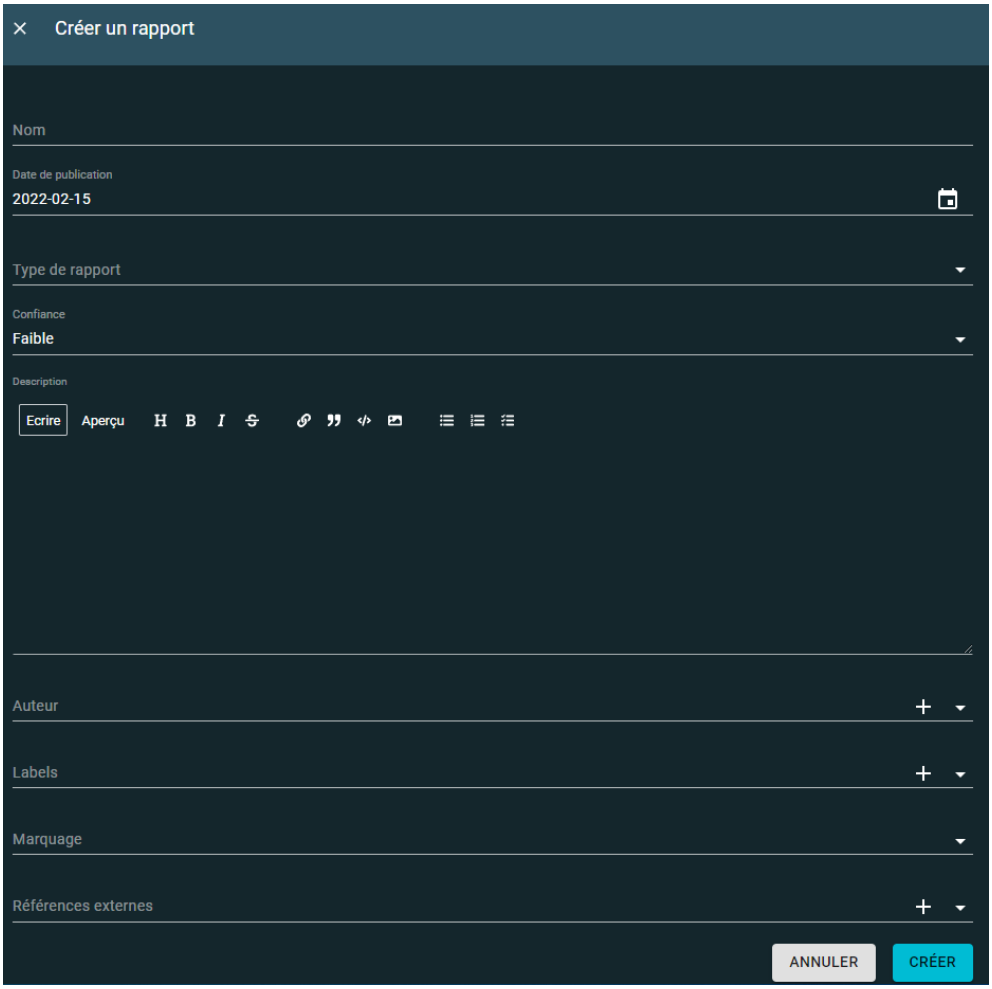


Au vu des éléments que nous fournissent les rapports de différents types de ressources, si le résultat ne vous satisfait pas il est également possible de créer des rapports manuellement.

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

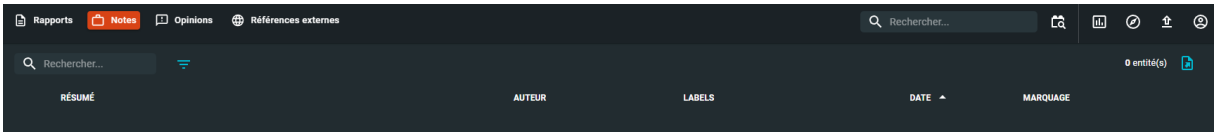
Pour cela il faut renseigner les champs suivants :

- 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



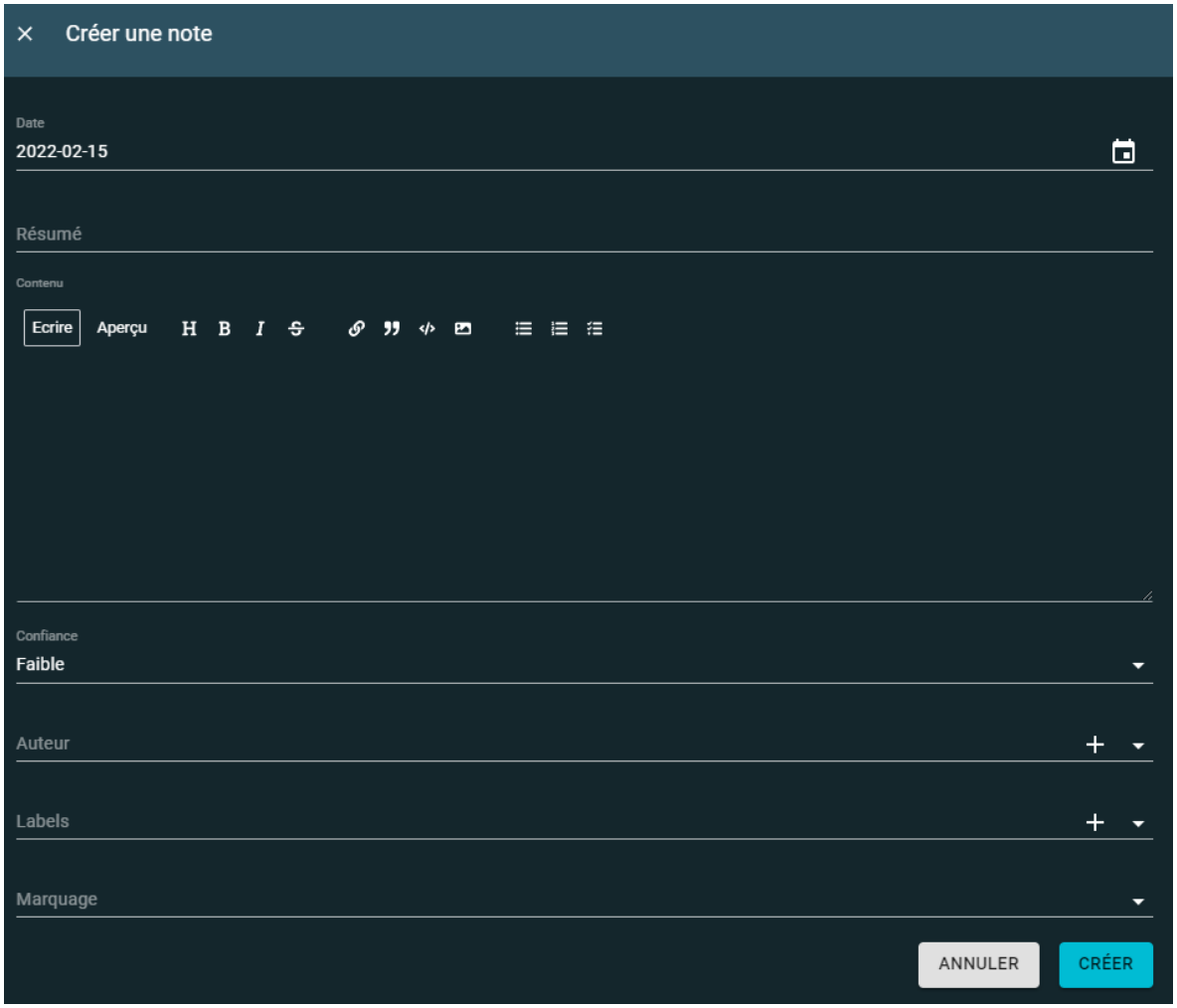
10.3.1.2 Notes

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



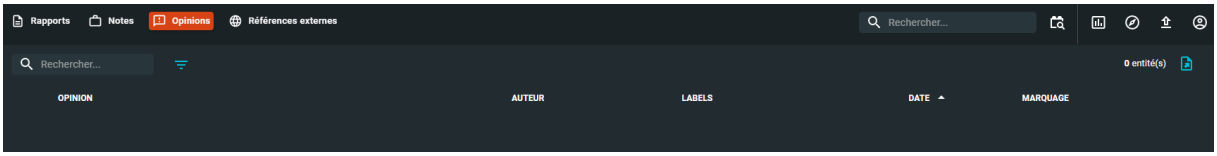
Nous pouvons créer des notes en renseignant les champs suivants :

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



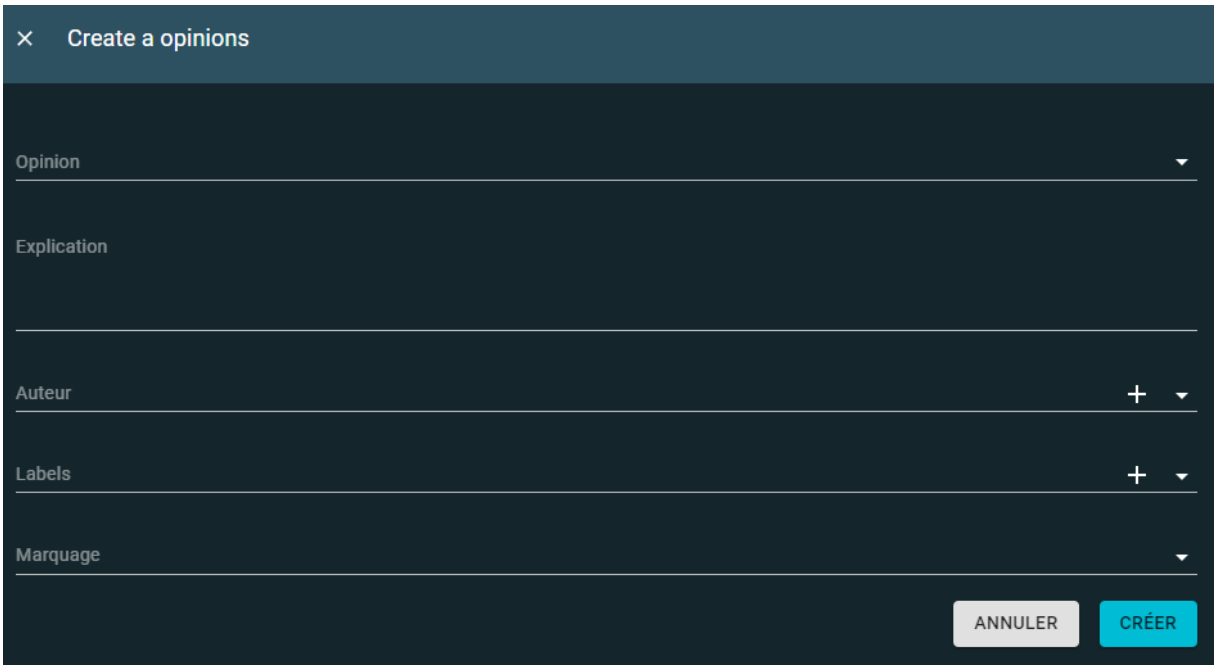
10.3.1.3 Opinions

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 :

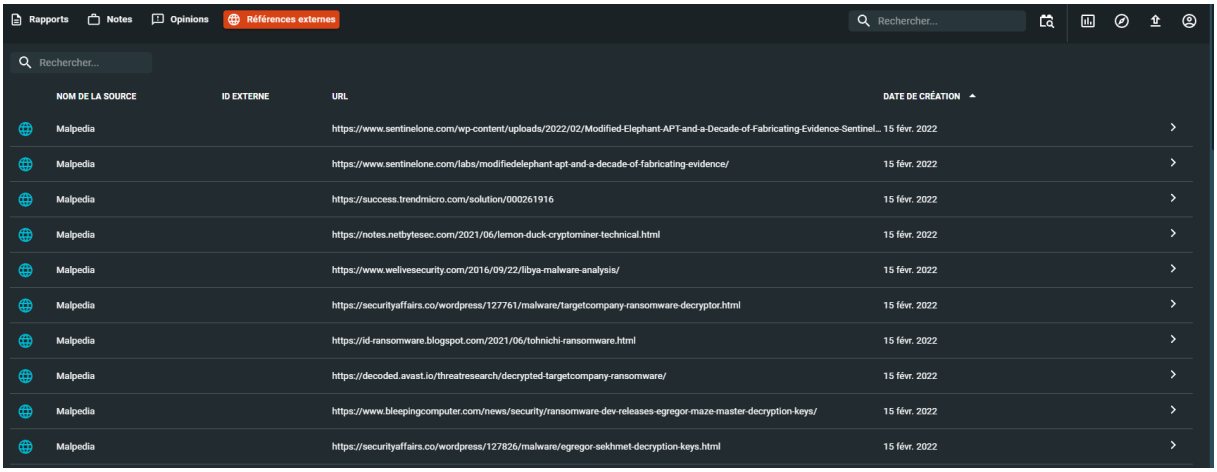
- Opinion : type d'opinion (strongly-disagree, disagree, neutral, agree, strongly-agree)
- Explication : raisons de l'opinion
- Auteur
- Labels
- Marquage



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 :



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

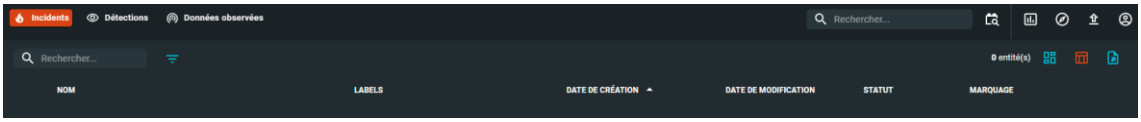
- Nom de la source : le nom que vous souhaitez donner à cette référence
- ID externe : si vous souhaitez attribuer un identifiant à cette référence
- URL : lien qui mène vers la référence
- Description : détails sur la référence
- Choisir un fichier … : vous pouvez joindre un fichier

10.3.2 Evènements

Les évènements peuvent être de différents types :

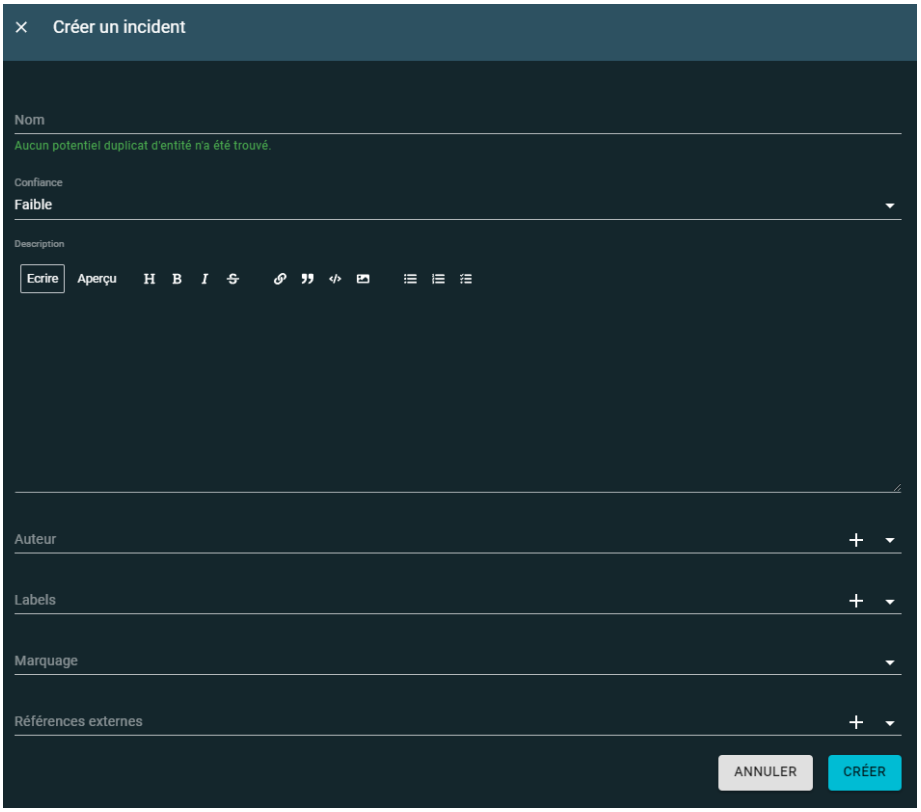
- Incidents
- Détections
- Données observées

10.3.2.1 Incidents

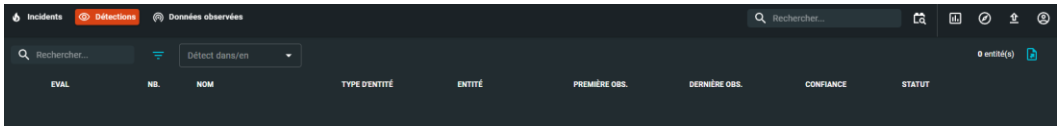


Pour créer un incident il faut remplir les champs suivants :

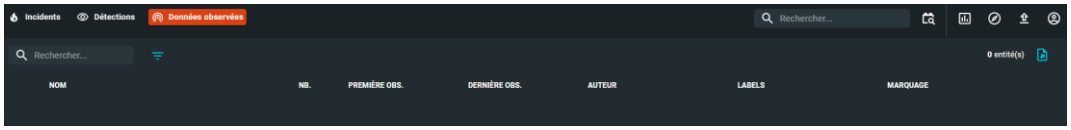
- Nom
- Confiance
- Description
- Auteur
- Labels
- Marquage
- Références externes



10.3.2.2 Détections

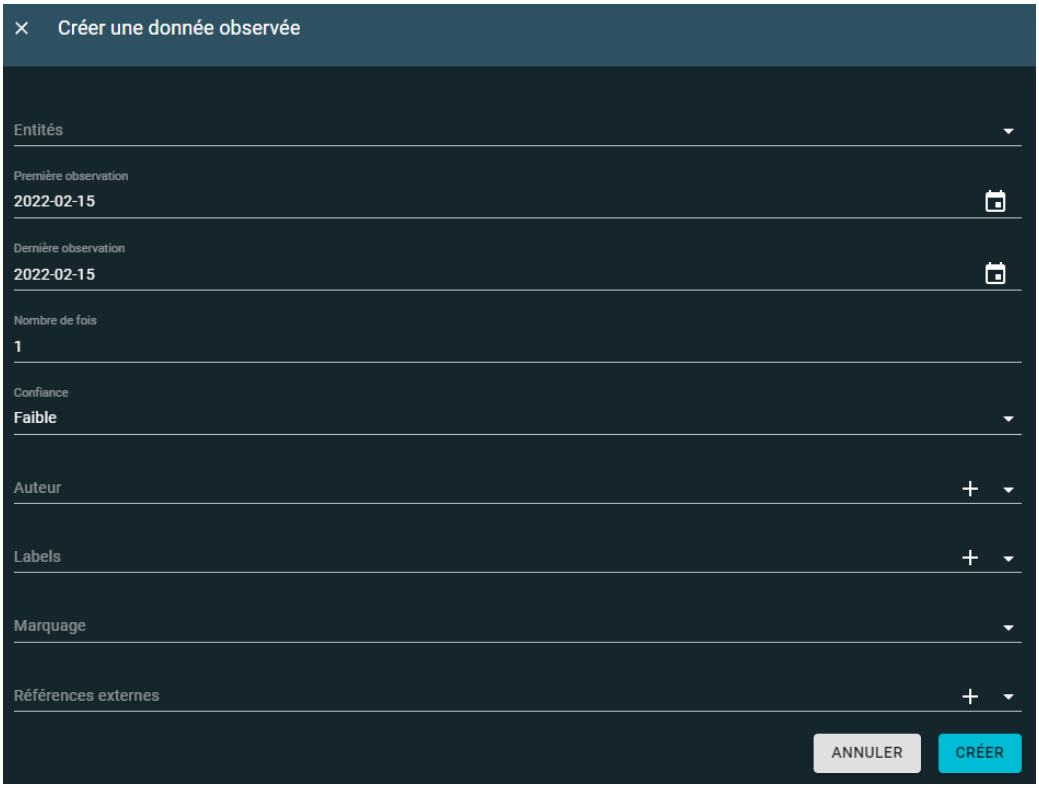


10.3.2.3 Données observées



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

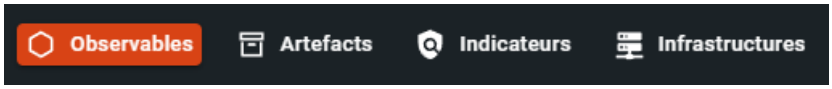
- Entités
- Première observation
- Dernière observation
- Nombre de fois
- Confiance
- Auteur
- Labels
- Marquage
- Références externes



10.3.3 Observations

Il y a différents types d'observables

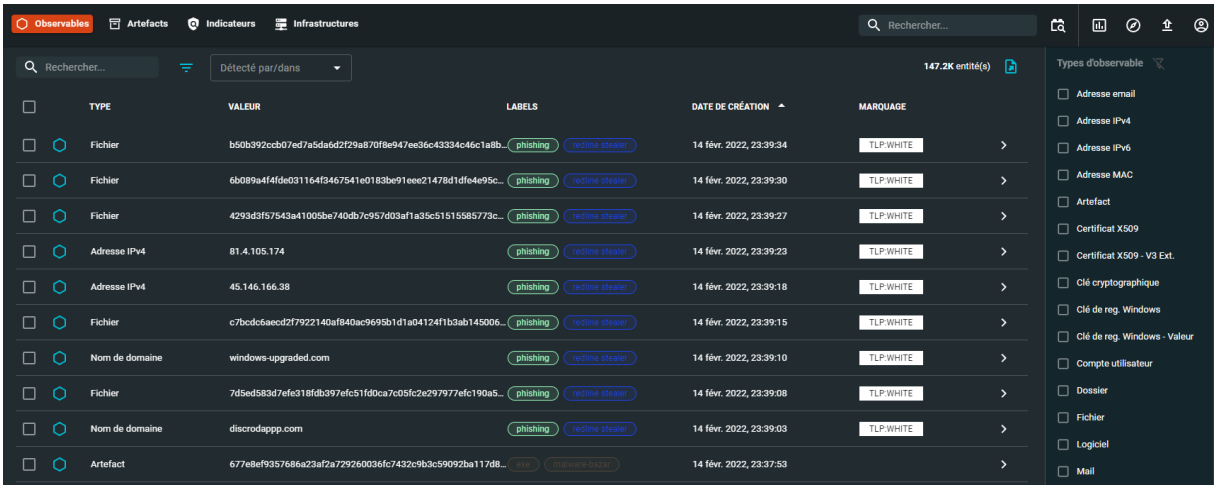
- Observables
- Artefacts
- Indicateurs
- Infrastructures



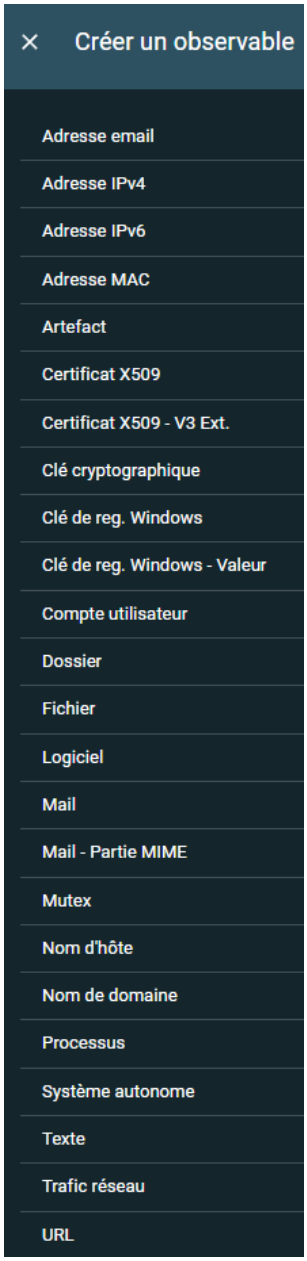
10.3.3.1 Observables

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

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

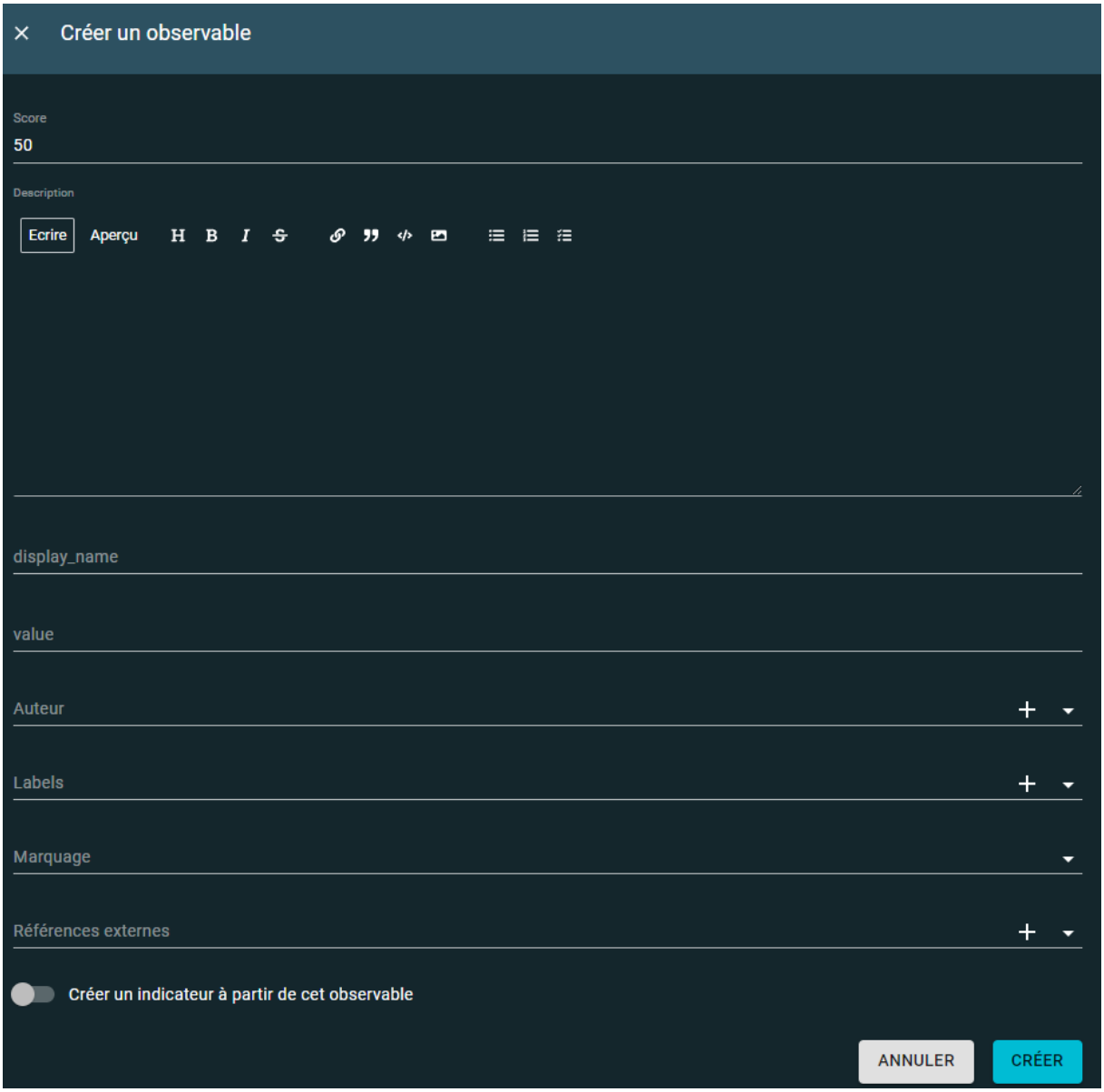


Voici un extrait de types d'observables :



Pour créer un observable il faut remplir les champs suivants :

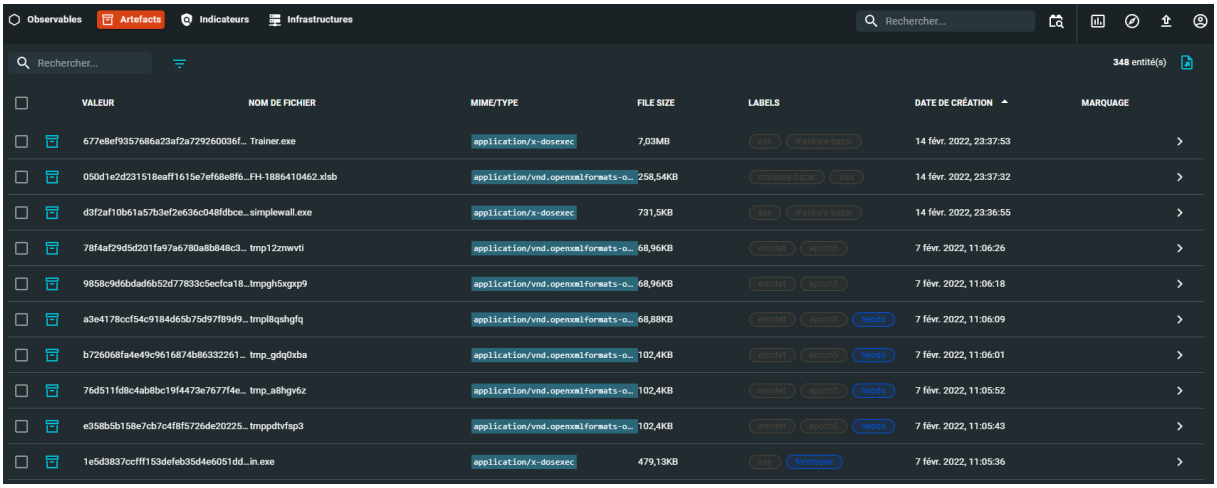
- Score
- Description
- Display_name : nom d'affichage
- Value : la valeur à attribuer
- Auteur
- Labels
- Marquage
- Références externes



10.3.3.2 Artefacts

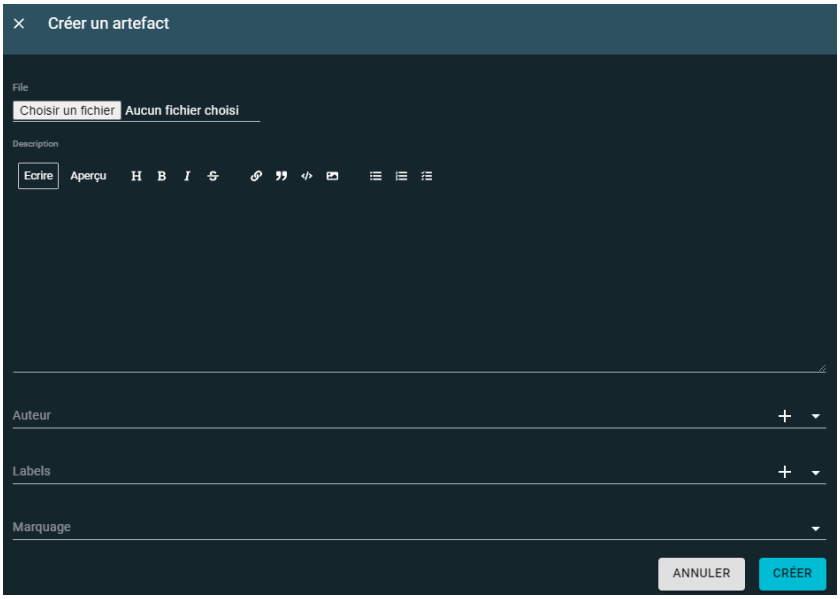
Les artefacts peuvent être triés via les colonnes suivantes :

- Valeur
- Nom de fichier
- MIME/TYPE
- File size
- Labels
- Date de création
- Marquage



Pour créer un artefact il faut remplir les champs suivants :

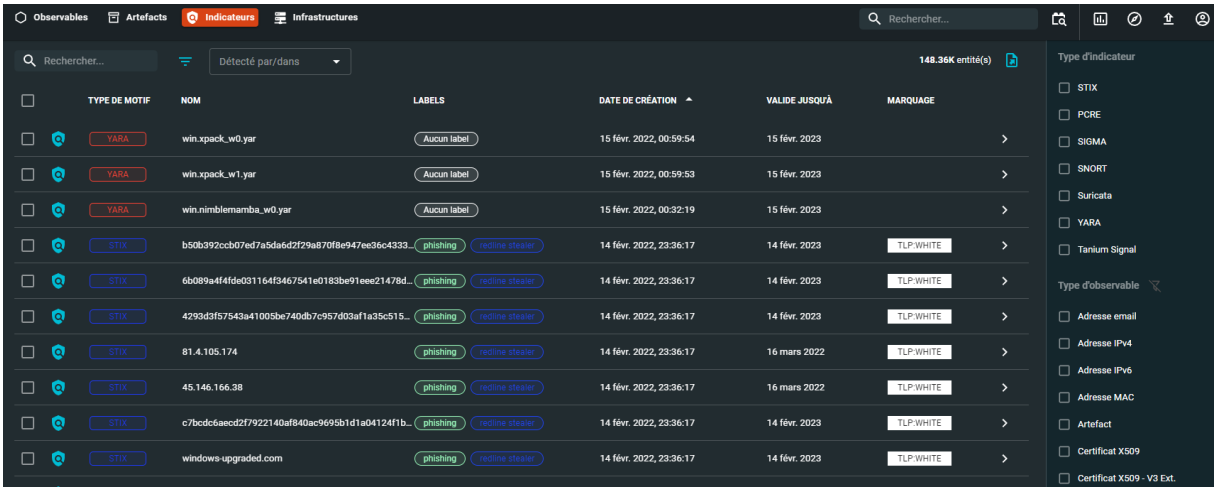
- Choisir un fichier : qui sera l'artefact
- Description
- Auteur
- Labels
- Marquage



10.3.3.3 Indicateurs

Les indicateurs peuvent être triés via les colonnes suivantes :

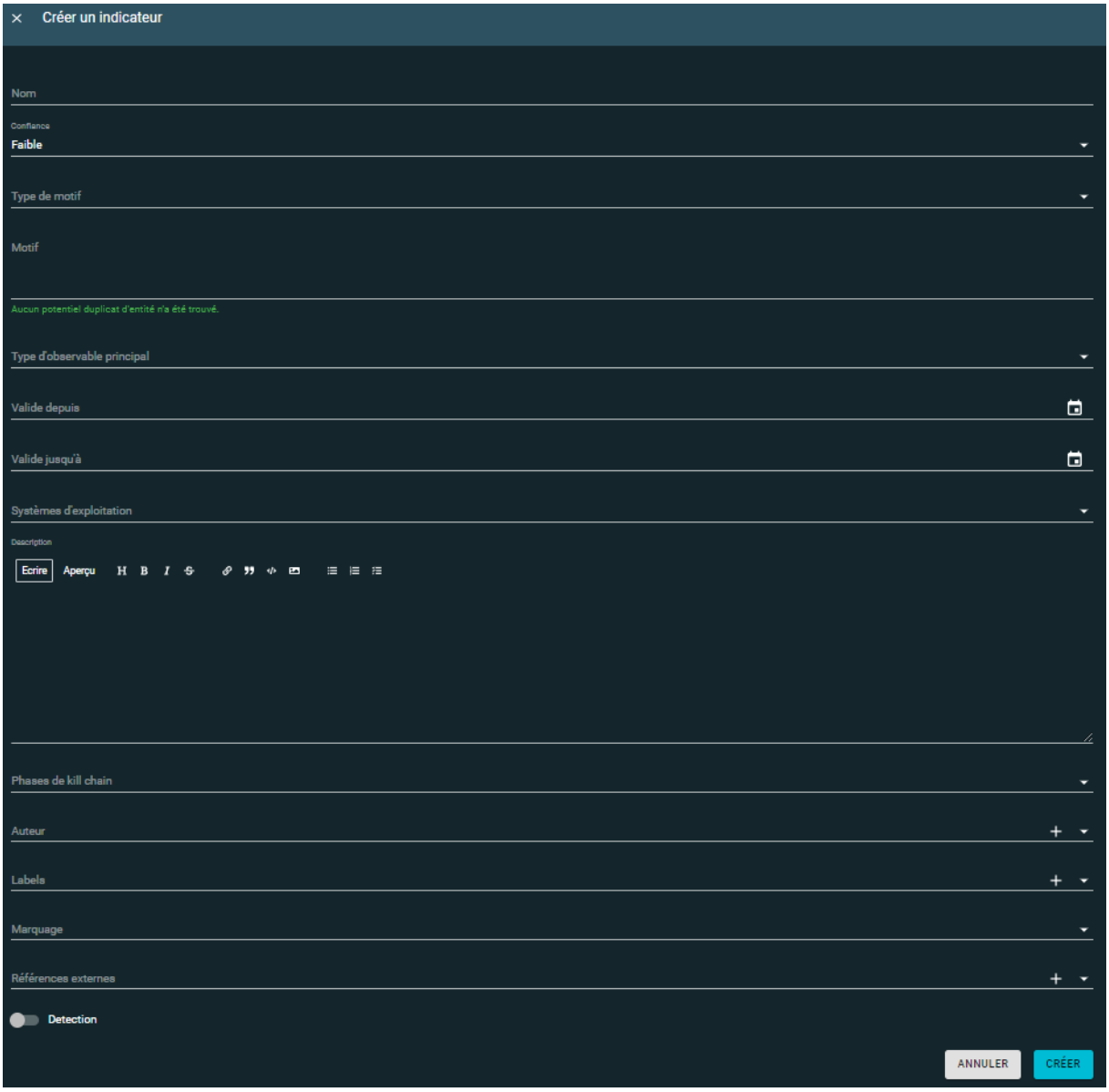
- Type de motif
- Nom
- Labels
- Date de création
- Valide jusqu'à
- Marquage



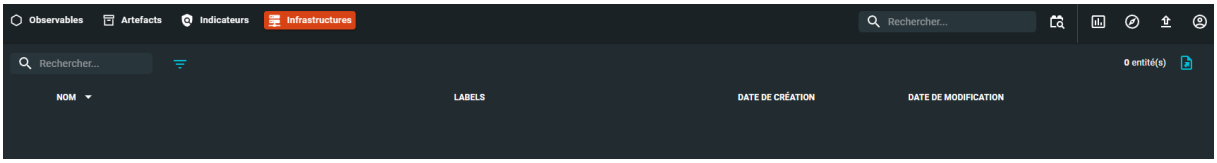
Il est possible de créer un indicateur en remplissant les champs suivants :

- 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

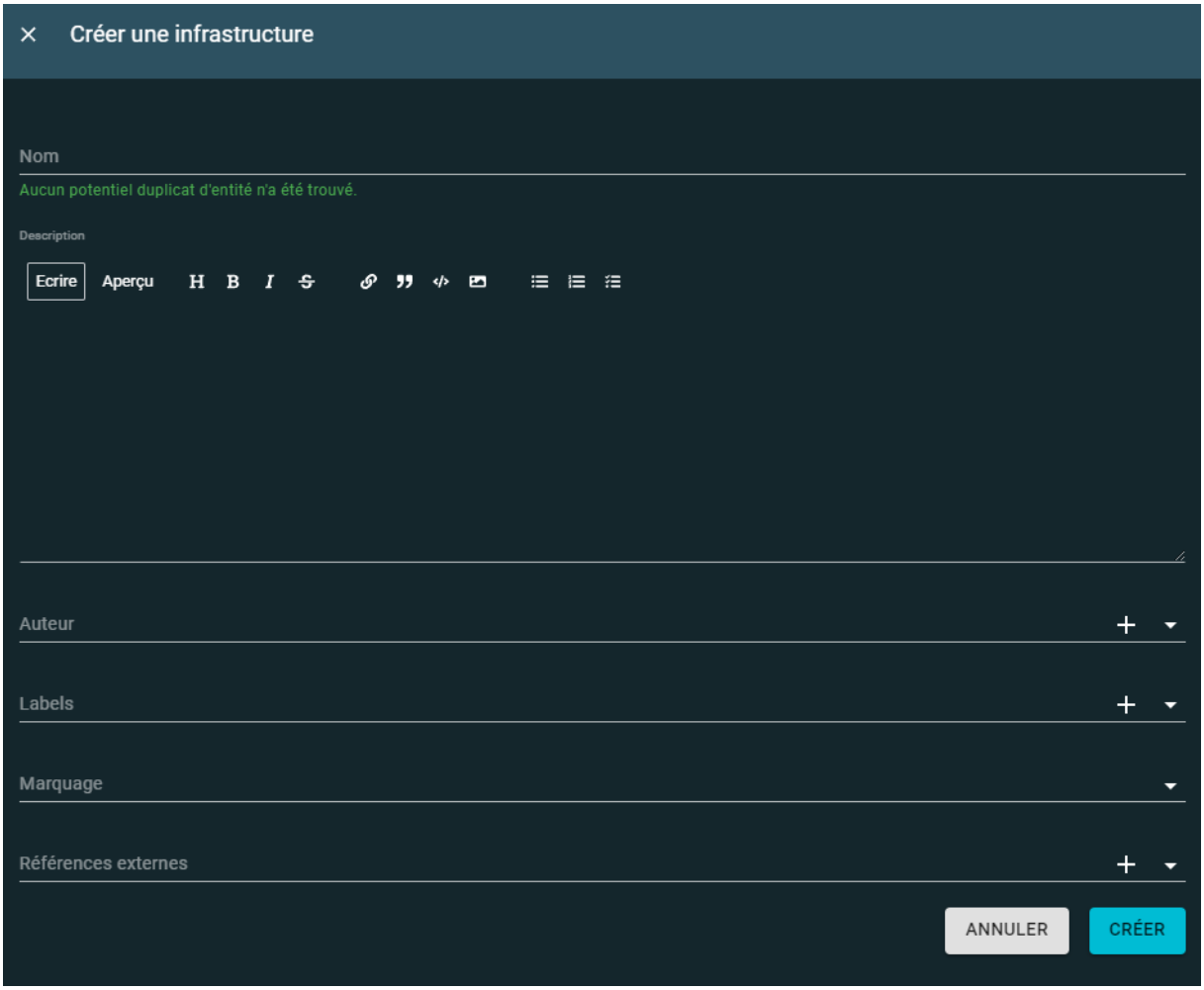


10.3.3.4 Infrastructures



Pour créer une infrastructure il faut remplir les champs suivants :

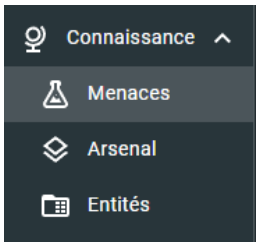
- Nom
- Description
- Auteur
- Labels
- Marquage
- Références externes



10.4 Connaissances

Il y a différents types de connaissances

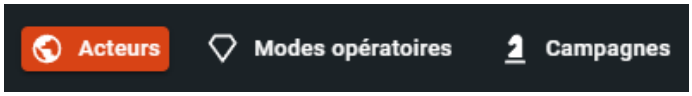
- Menaces
- Arsenal
- Entités



10.4.1 Menaces

Il y a différents types de menaces

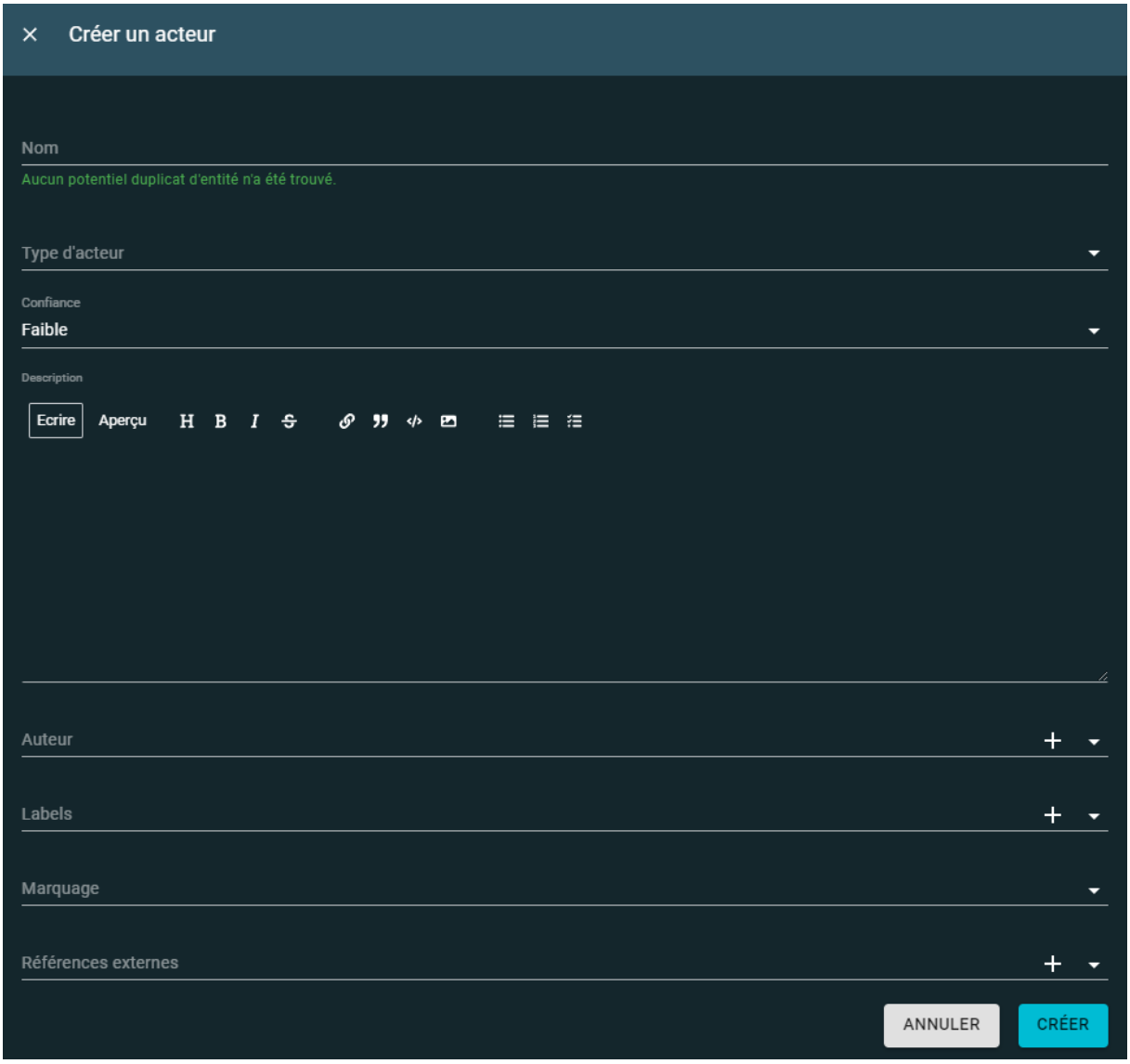
- Acteurs
- Modes opératoires
- Campagnes



10.4.1.1 Acteurs

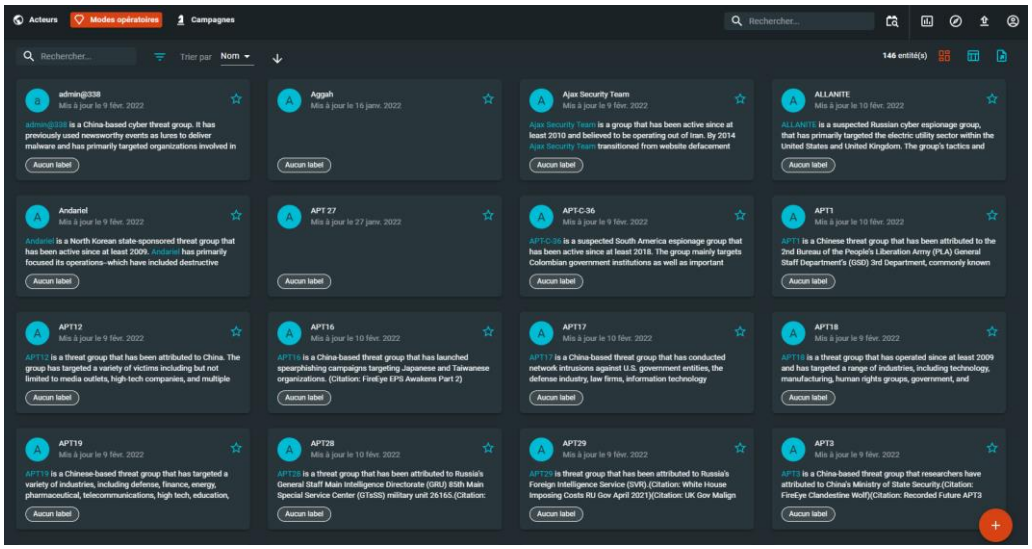
Pour créer un acteur il faut remplir les champs suivants :

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



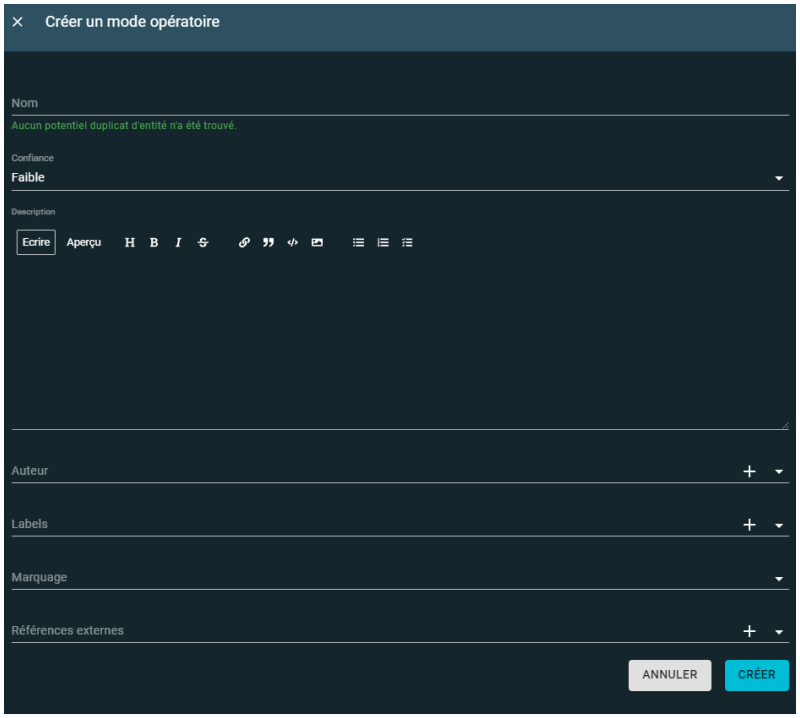
10.4.1.2 Modes opératoires

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 :

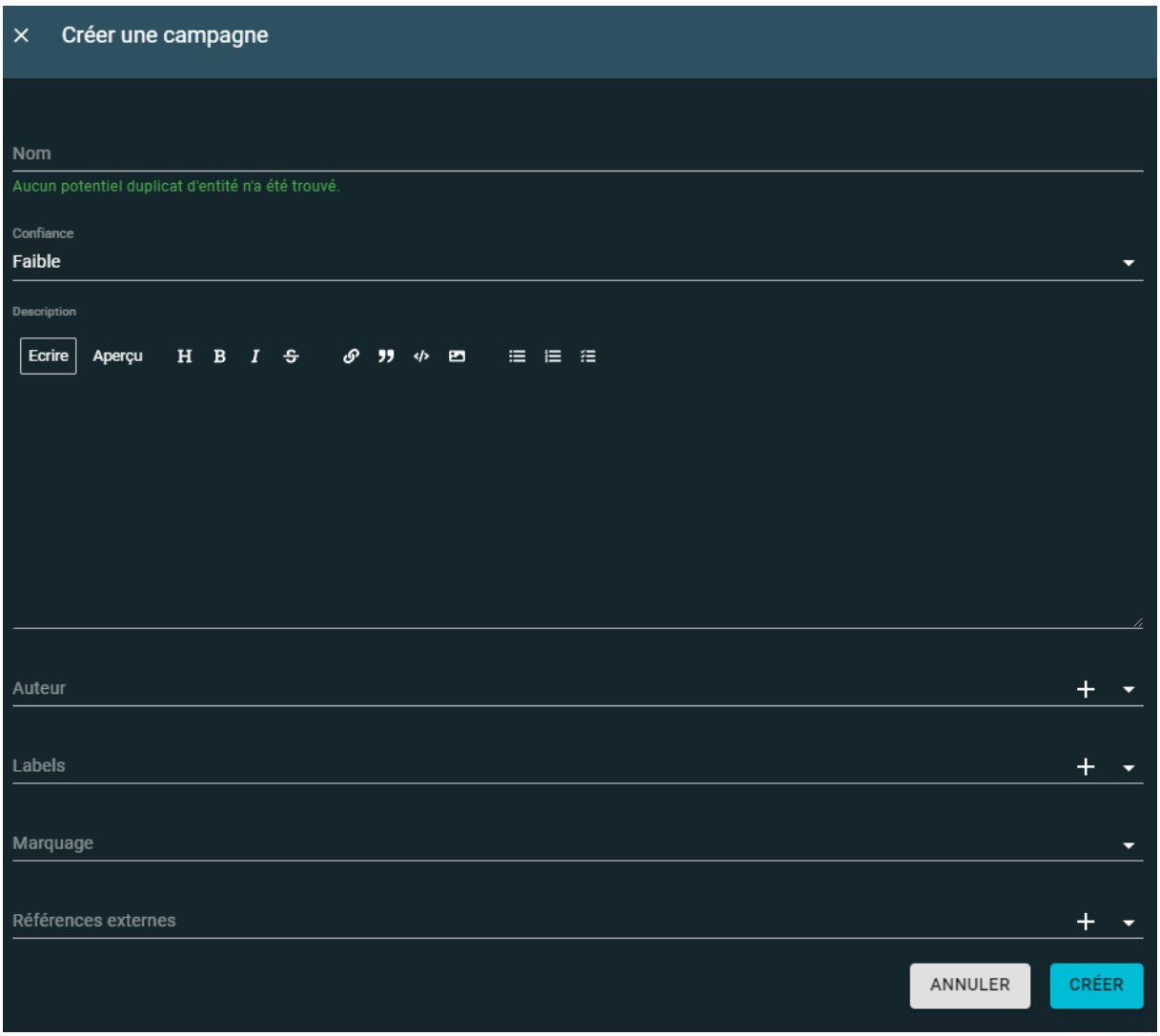
- Nom
- Confiance
- Description
- Auteur
- Labels
- Marquage
- Références externes



10.4.1.3 Campagnes

Pour créer des campagnes il faut remplir les champs suivants :

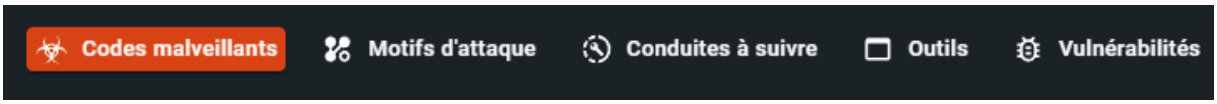
- Nom
- Confiance
- Description
- Auteur
- Labels
- Marquage
- Références externes



10.4.2 Arsenal

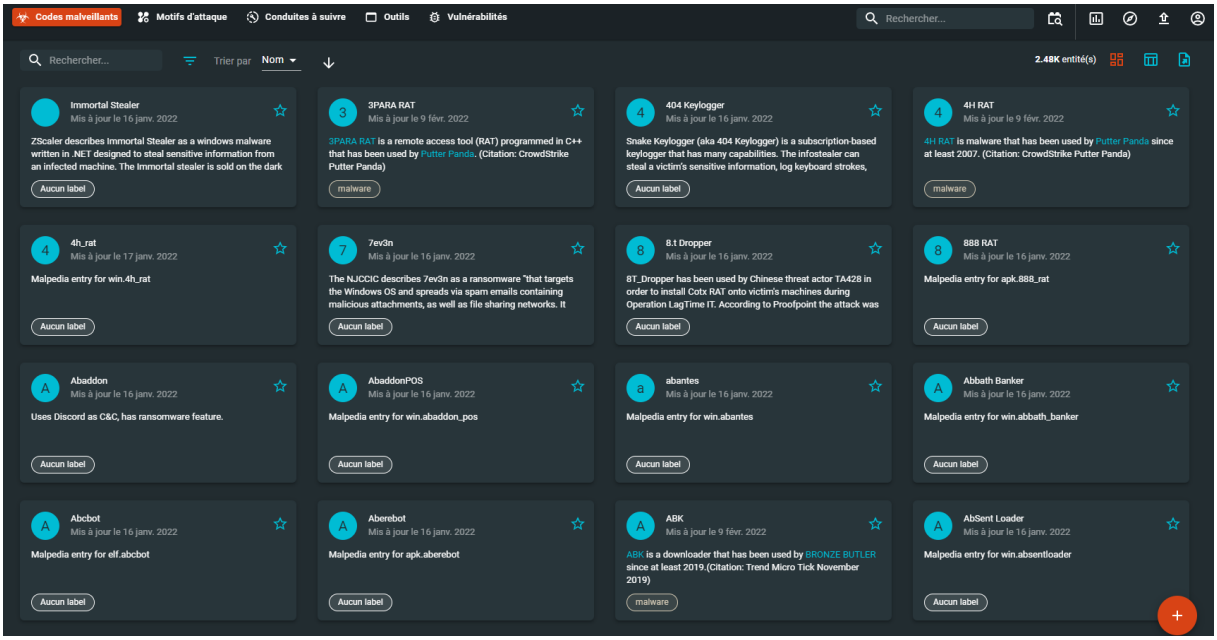
Il y a différents types d'éléments dans la catégorie Arsenal :

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



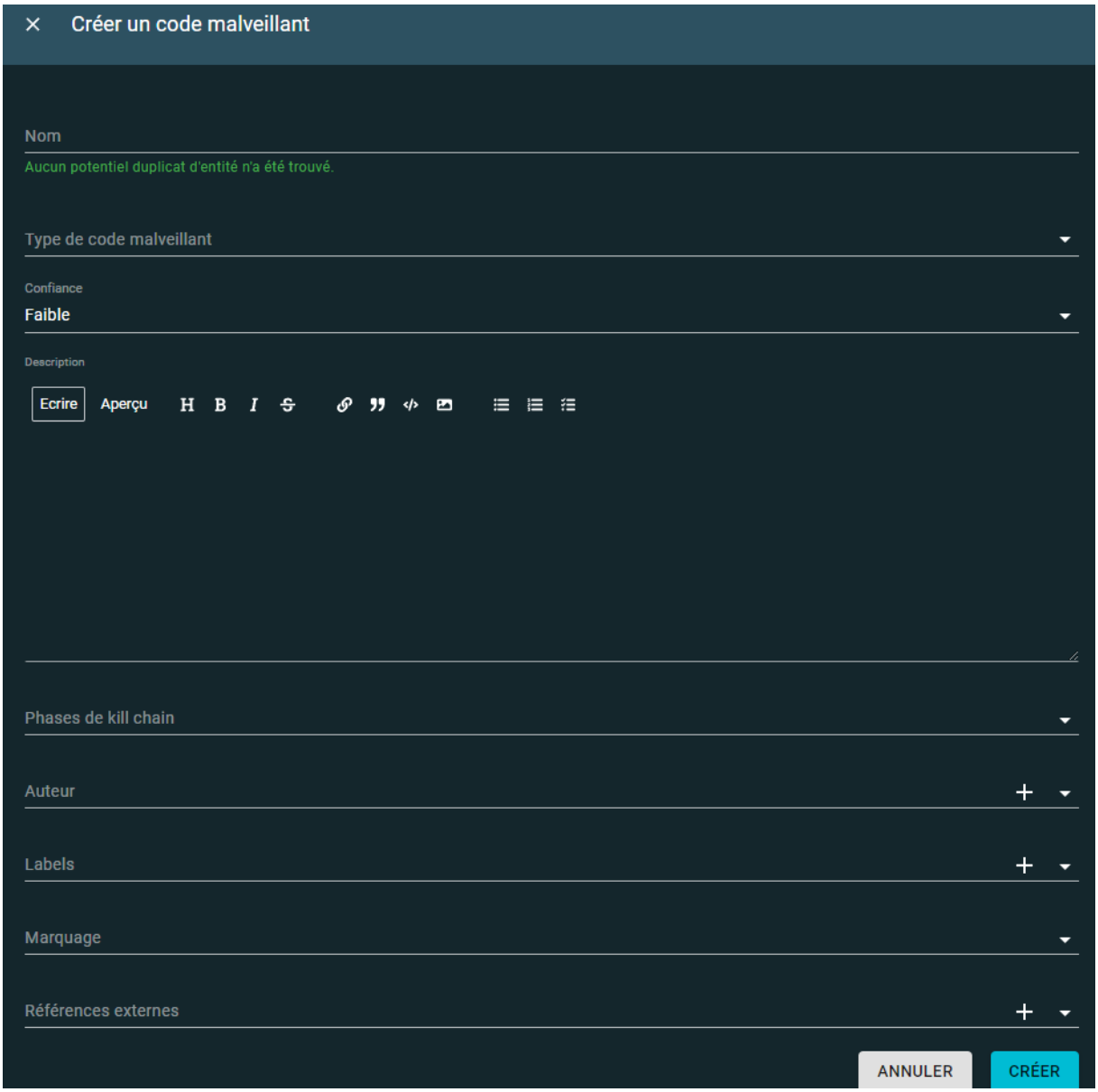
10.4.2.1 Codes malveillants

Cette catégorie recense les codes utilisés par les acteurs malveillants :



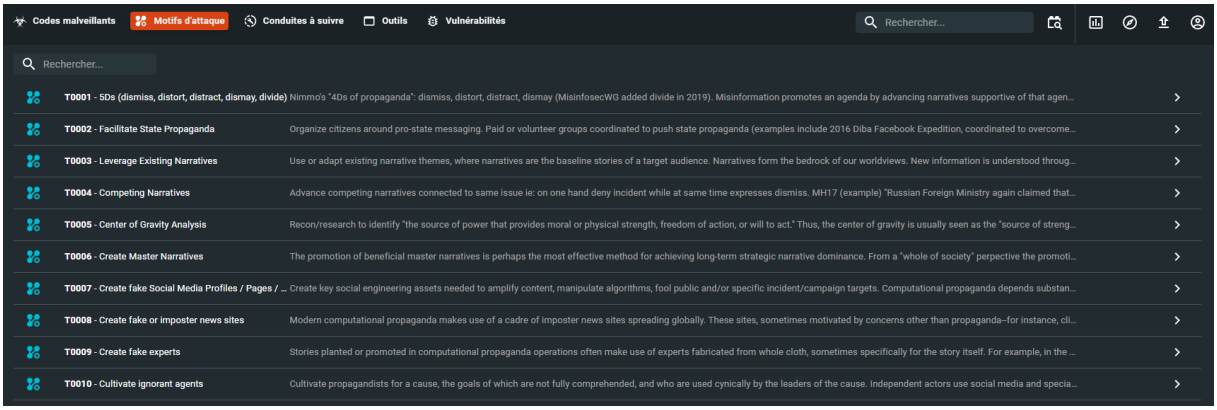
Pour ajouter un élément de type code malveillant, il faut remplir les champs suivants :

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



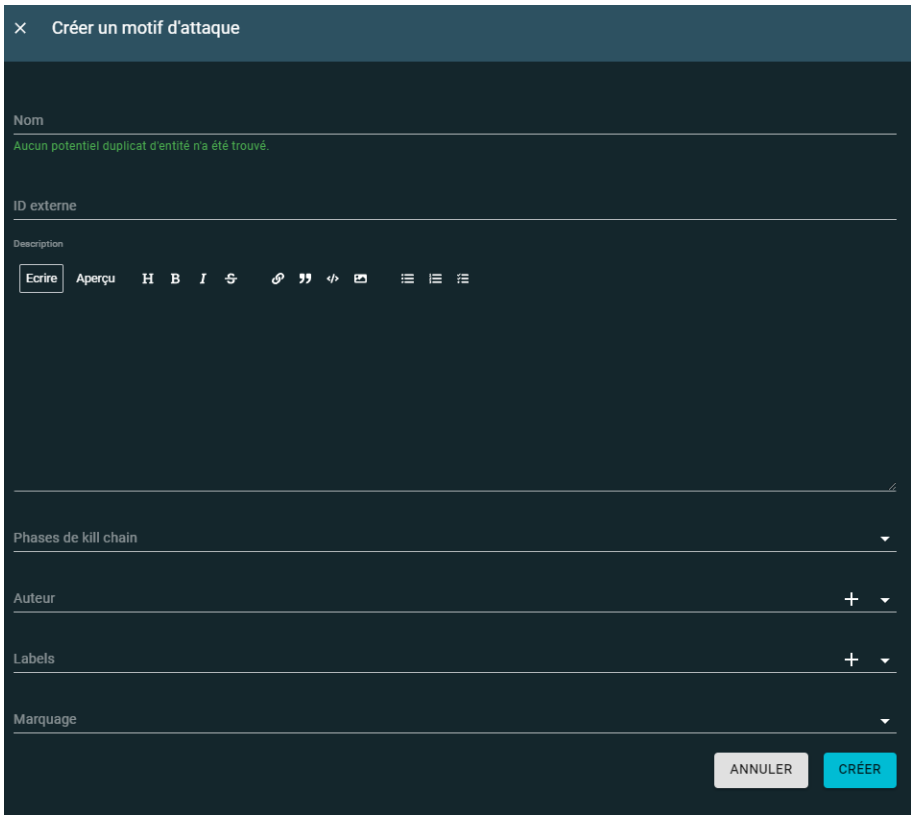
10.4.2.2 Motifs d'attaques

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



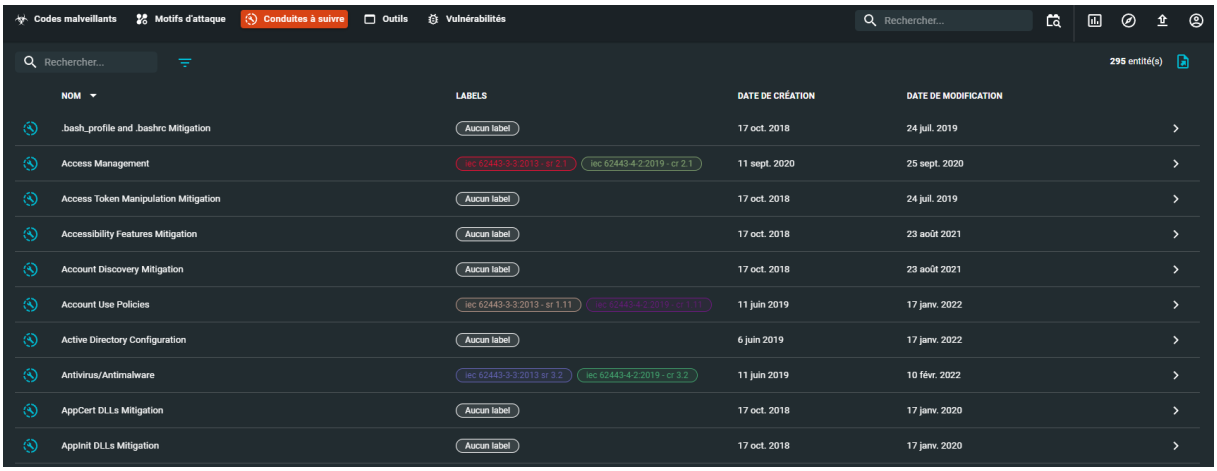
Pour ajouter un nouveau motif d'attaque il faut remplir les champs suivants :

- 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



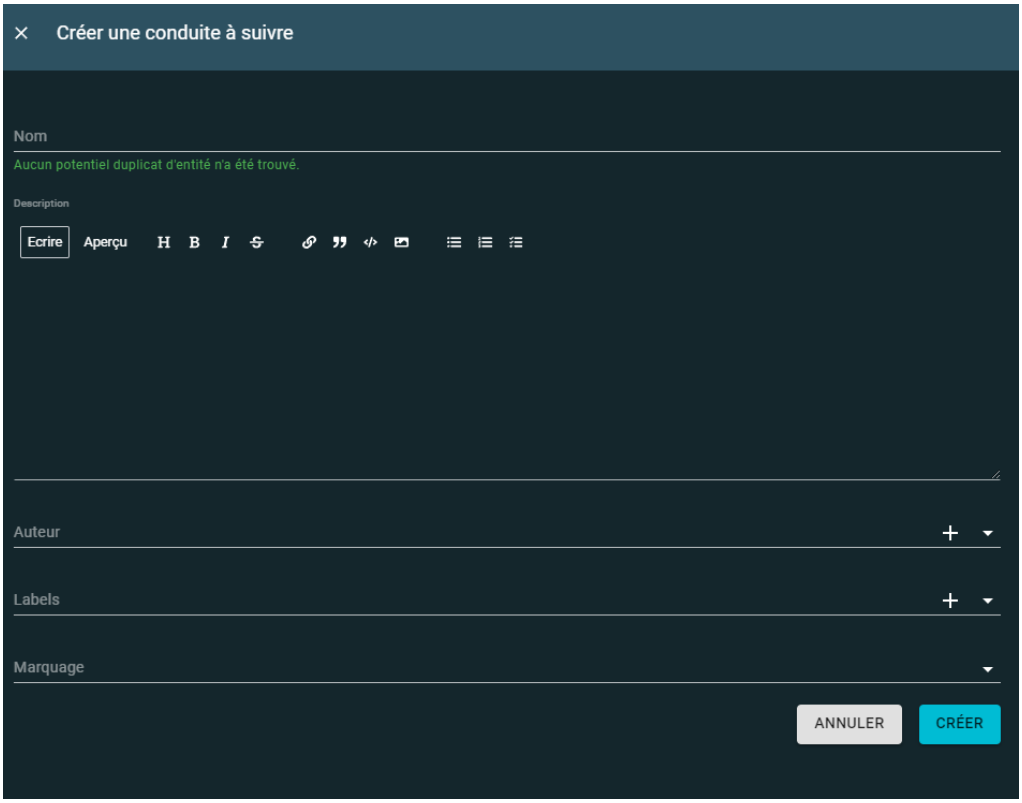
10.4.2.3 Conduites à suivre

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



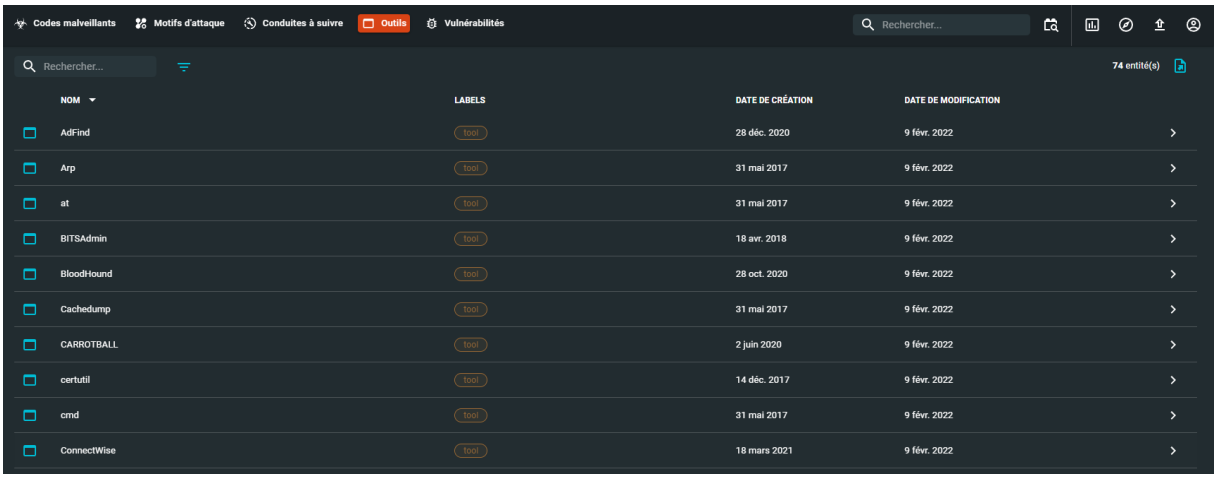
Pour ajouter une conduire à suivre il faut remplir les champs suivants :

- Nom
- Description
- Auteur
- Labels
- Marquage



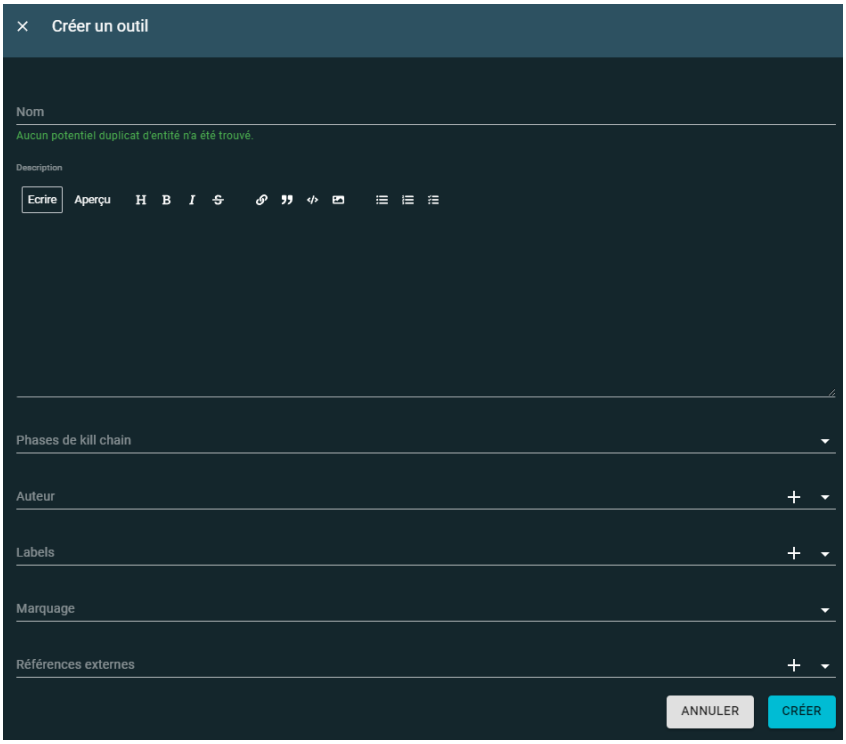
10.4.2.4 Outils

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 :



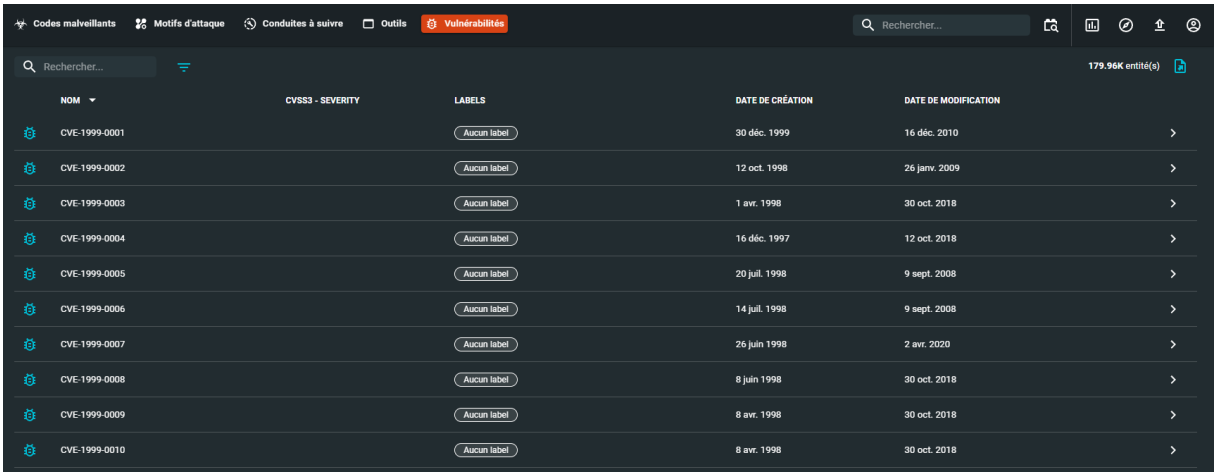
Pour ajouter un outil il faut remplir les champs suivants :

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



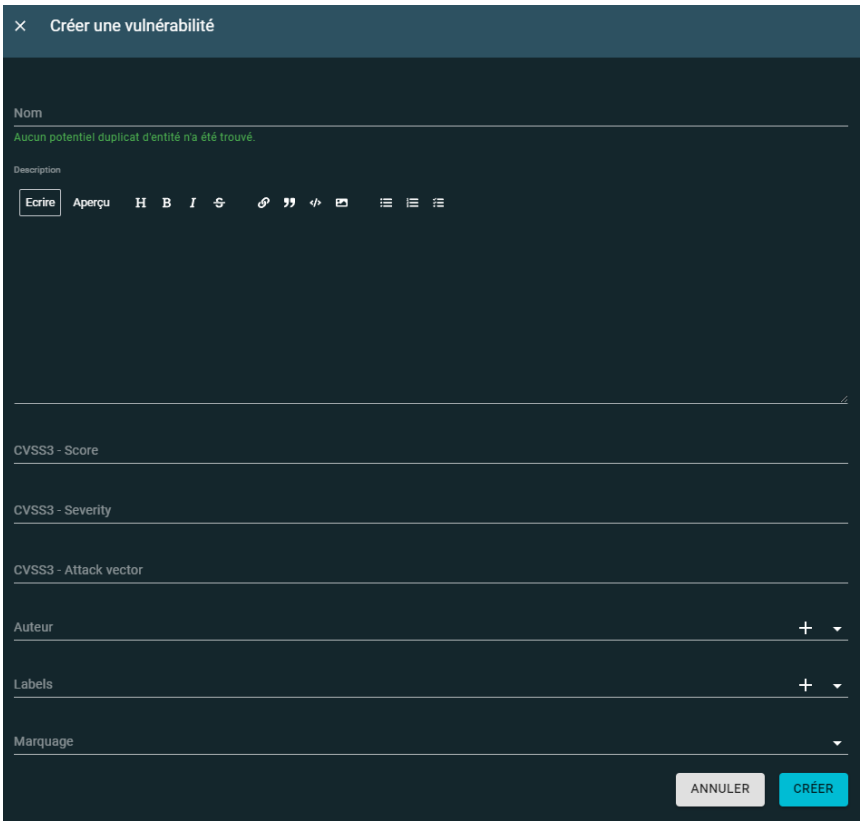
10.4.2.5 Vulnérabilités

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



Pour ajouter une vulnérabilité il faut remplir les champs suivants :

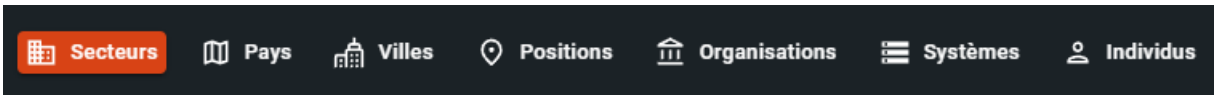
- Nom
- CVSS3 – Score : le score correspondant à la vulnérabilité avec l'échelle CVSS3
- CVSS3 – Severity : le niveau de criticité correspondant à la vulnérabilité avec l'échelle CVSS3
- CVSS3 – Attack vector : le vecteur d'attaque utilisé en se basant sur l'échelle CVSS3
- Auteur
- Labels
- Marquage



10.4.3 Entités

Il y a différents types d'entités

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



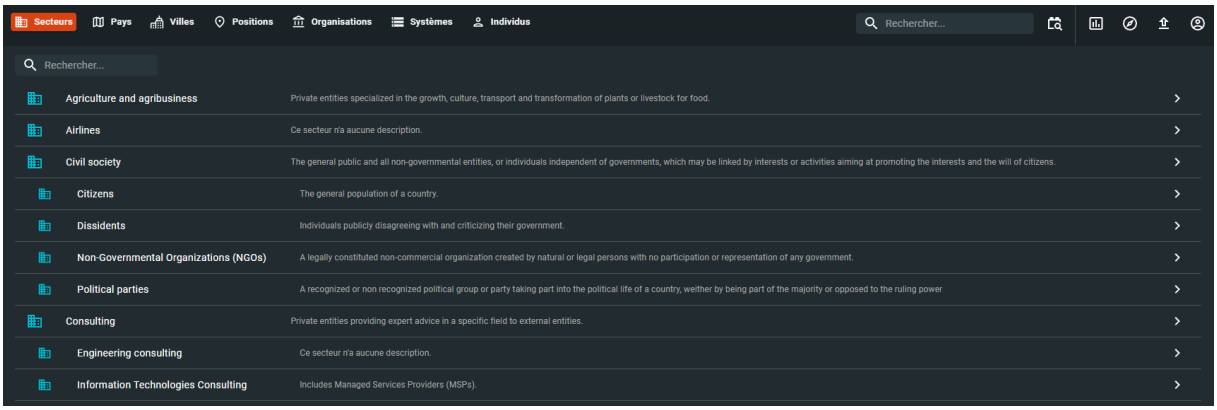
Parmi la liste ci-dessus on peut s'étonner de voir des villes, positions, et mêmes individus !

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.

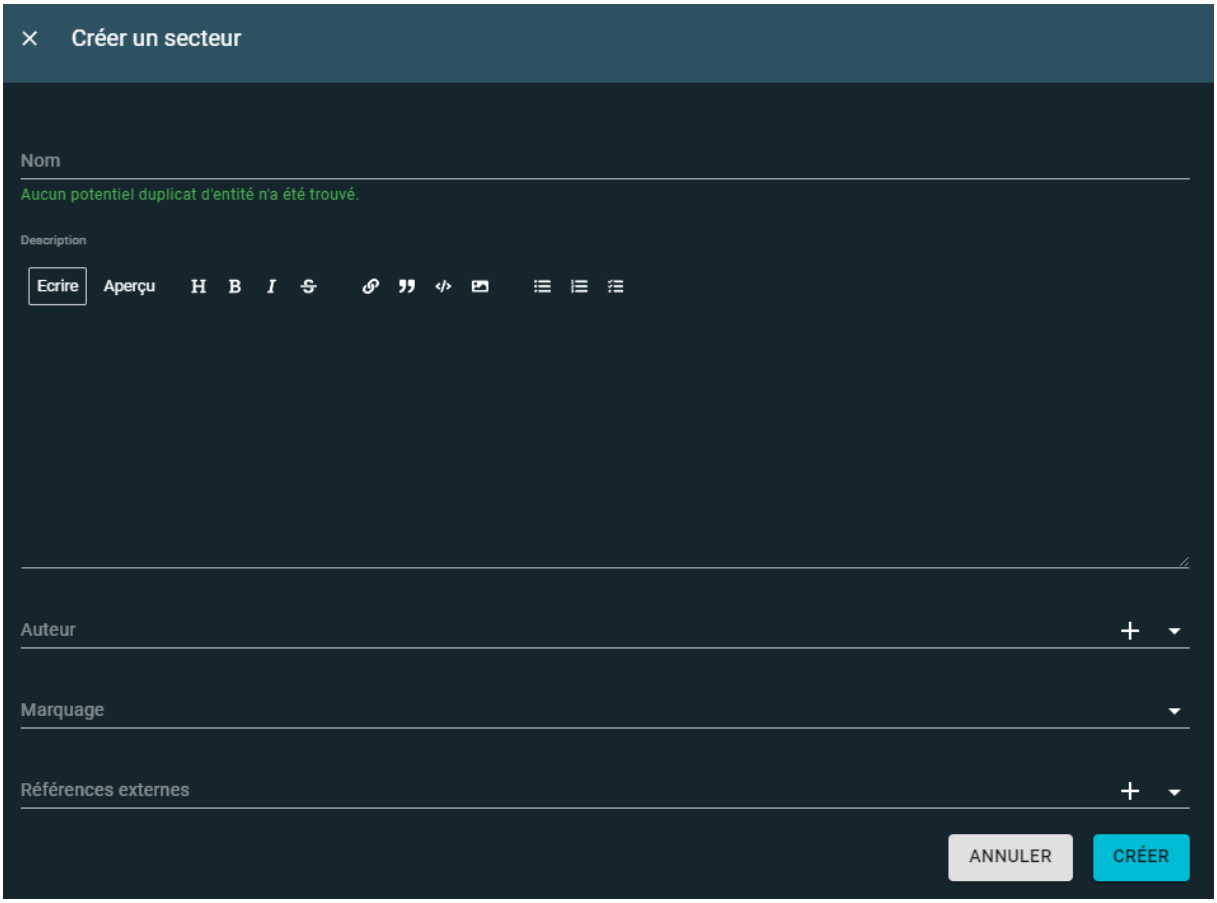
10.4.3.1 Secteurs

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



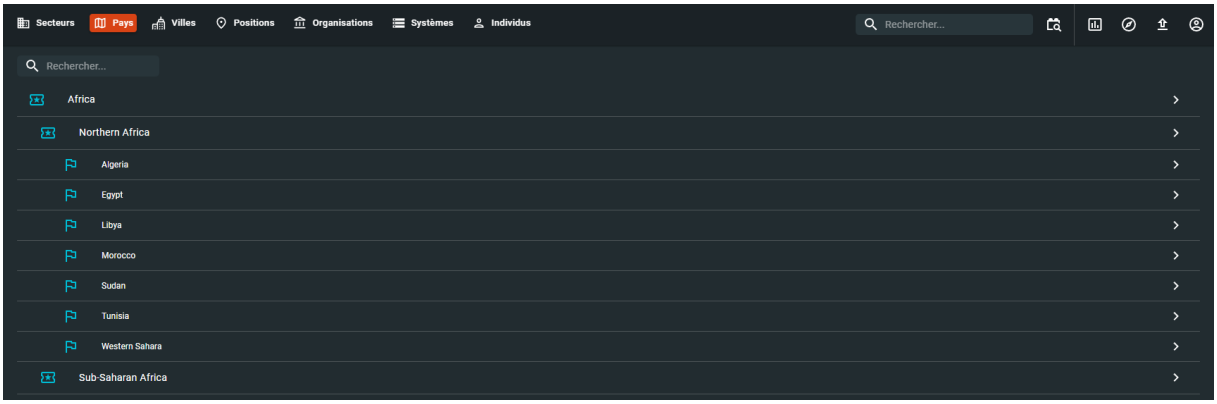
Si vous souhaitez ajouter un secteur il faut remplir les champs suivants :

- Nom
- Description
- Auteur
- Marquage
- Références externes



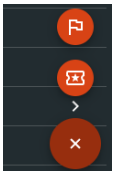
10.4.3.2 Pays

La liste des pays du monde est présente par défaut :



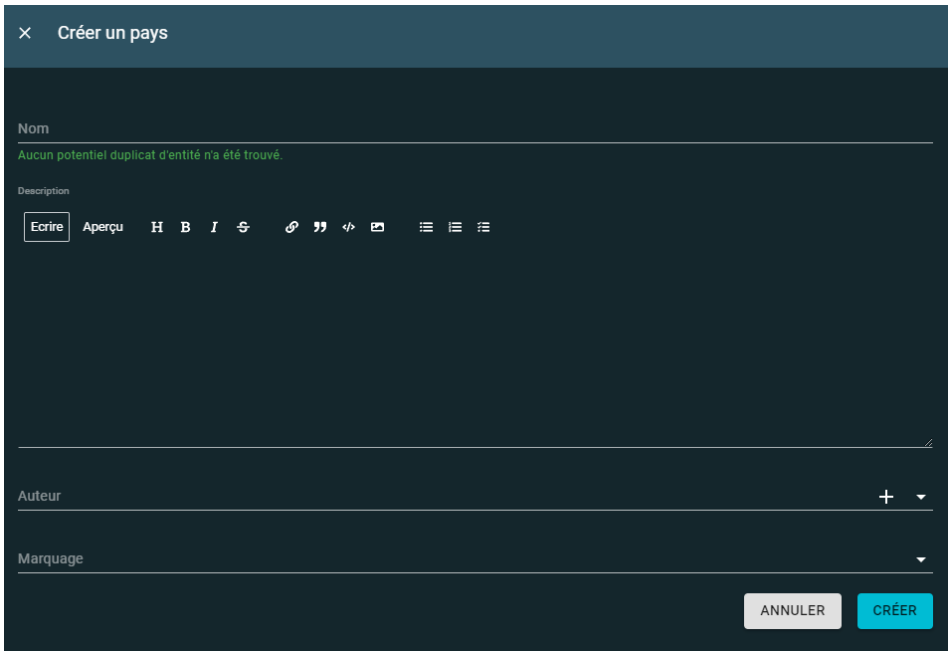
Nous pouvons

- Créer un pays
- Créer une région



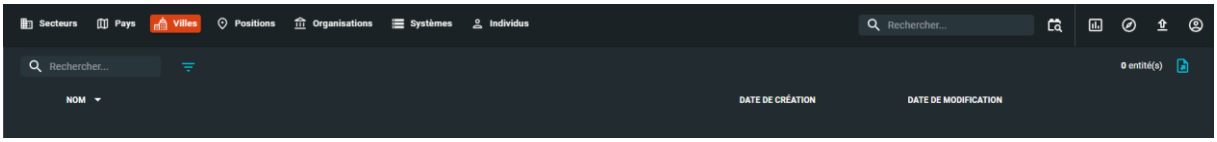
Pour créer un pays il faut remplir les champs suivants :

- Nom
- Description
- Auteur
- Marquage



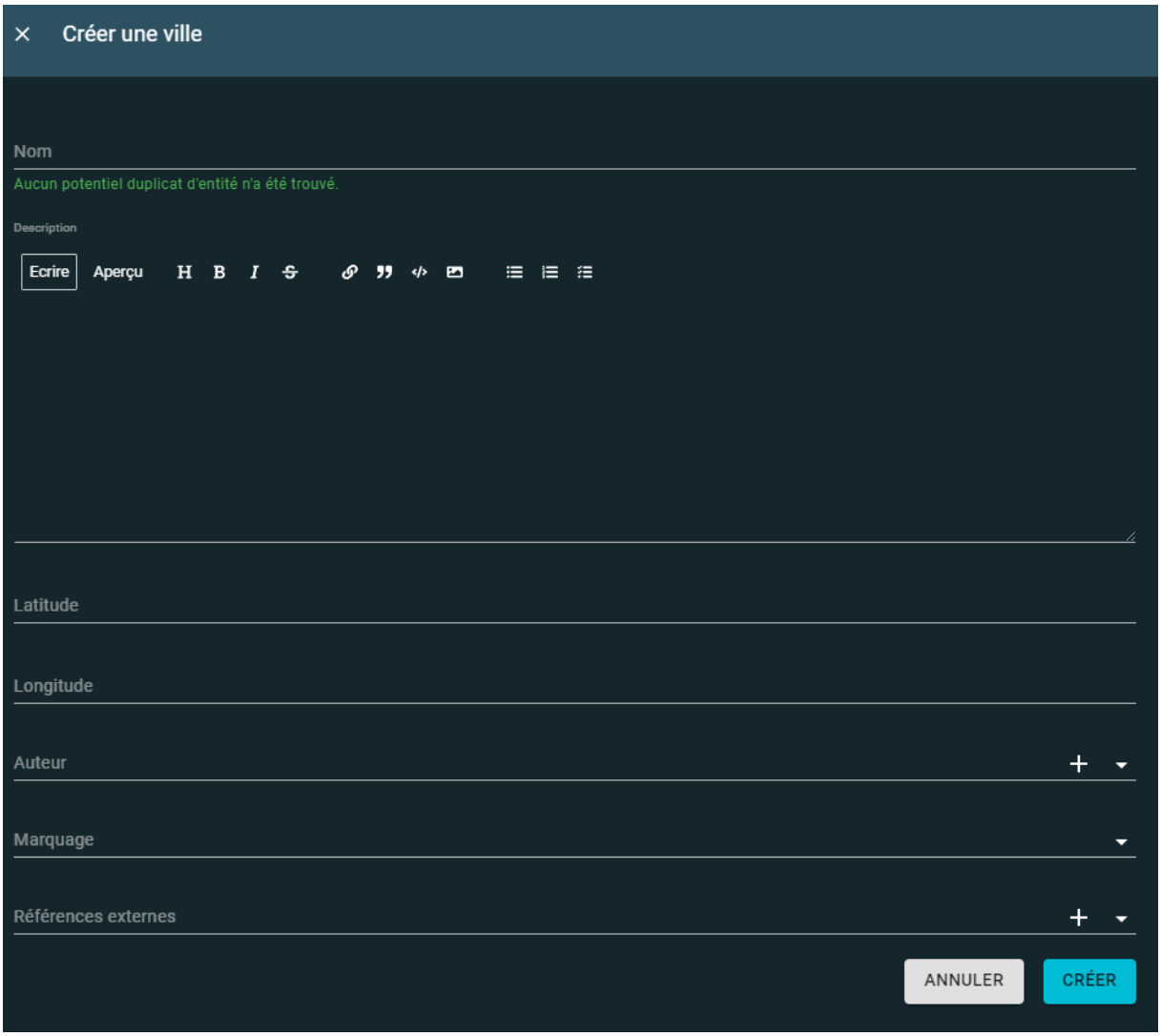
10.4.3.3 Villes

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

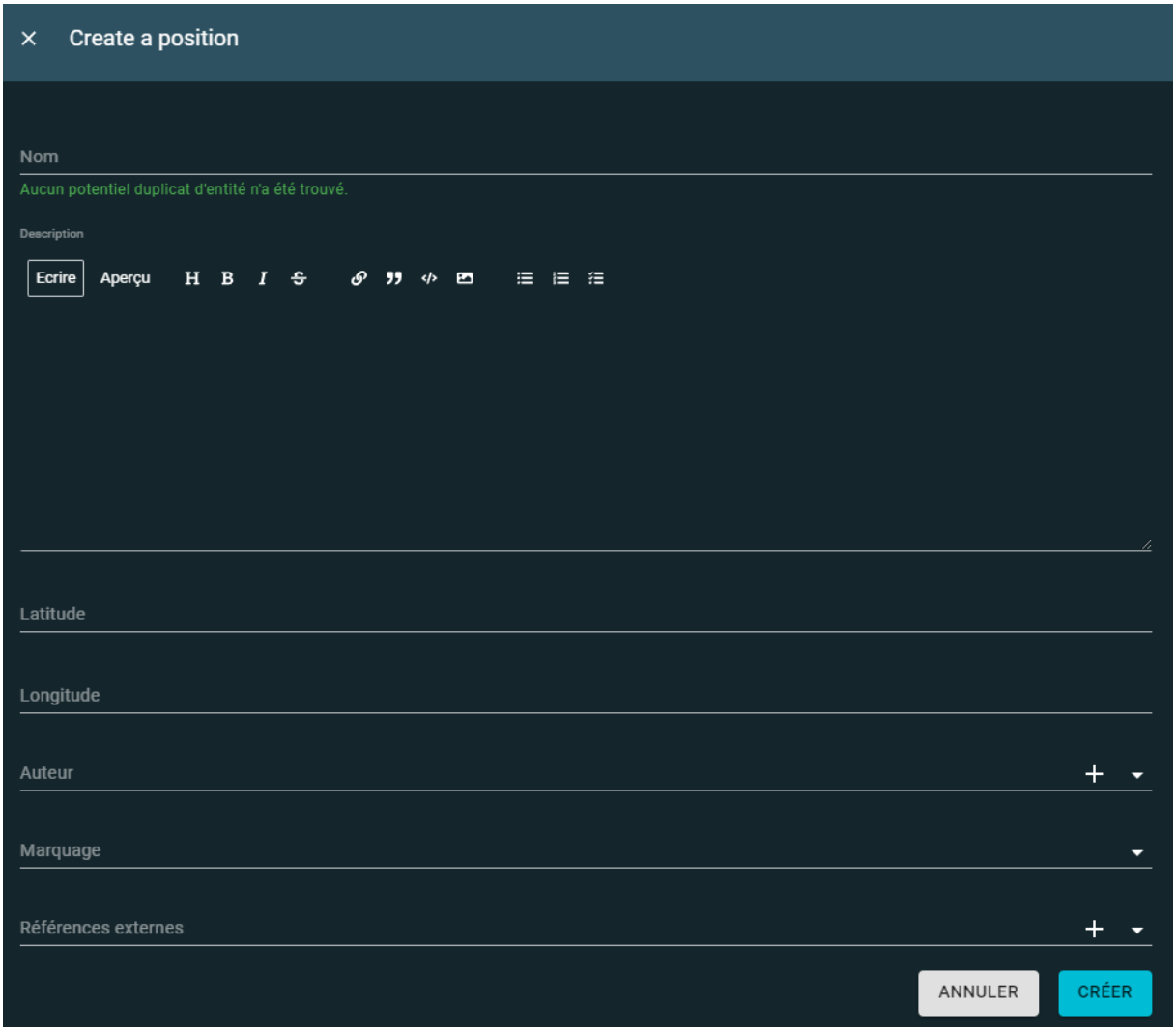


10.4.3.4 Positions

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

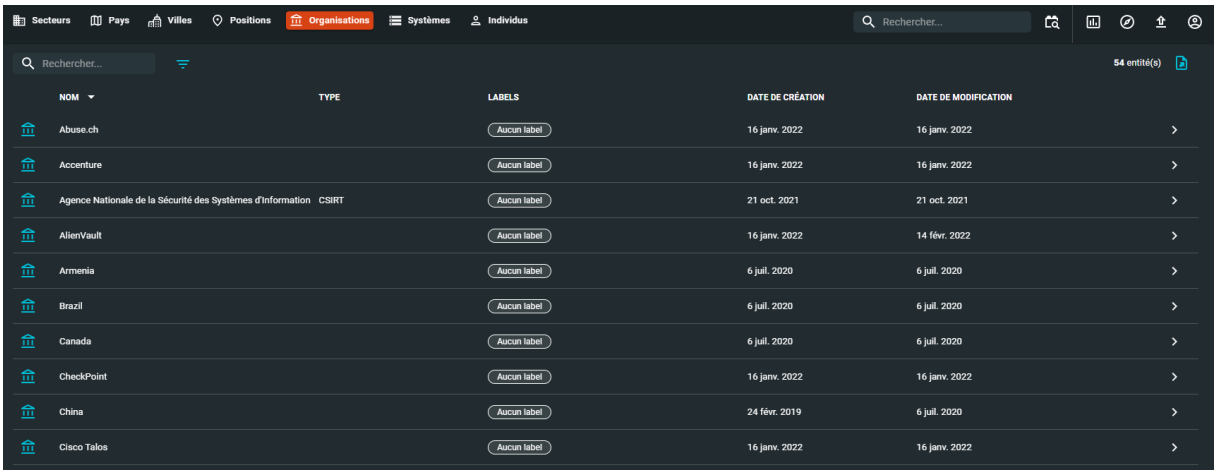
Pour ajouter une position il faut remplir les champs suivants :

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



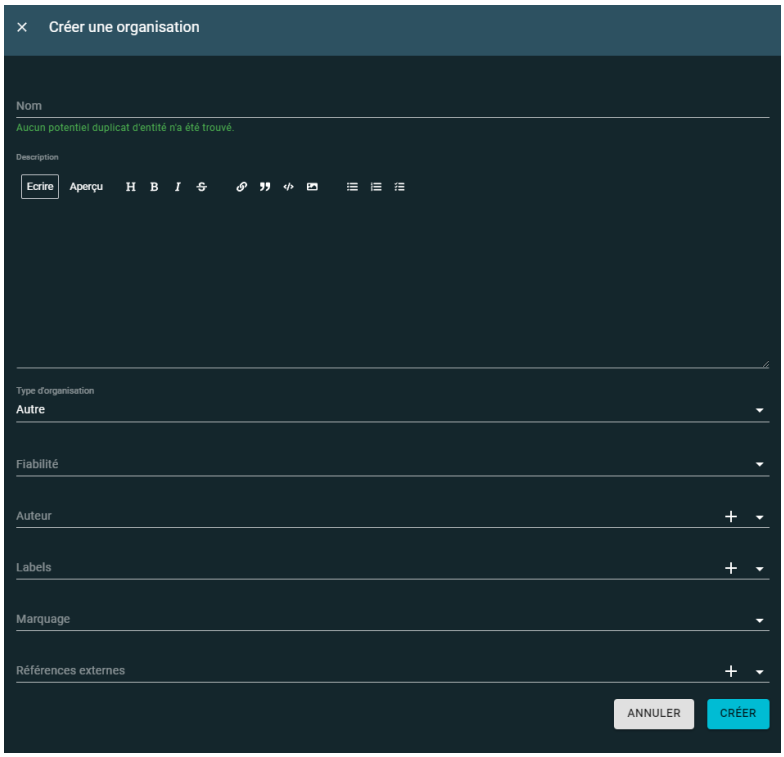
10.4.3.5 Organisations

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

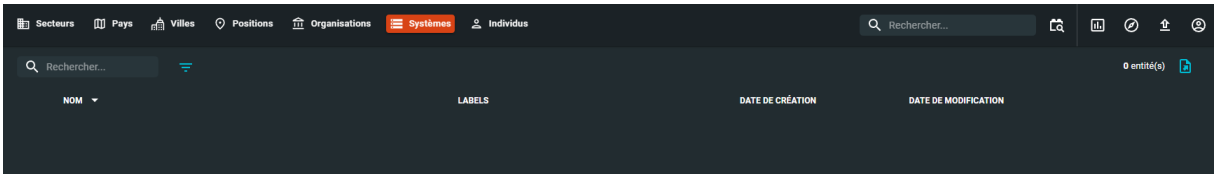


Pour ajouter manuellement une organisation il faut remplir les champs suivants :

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

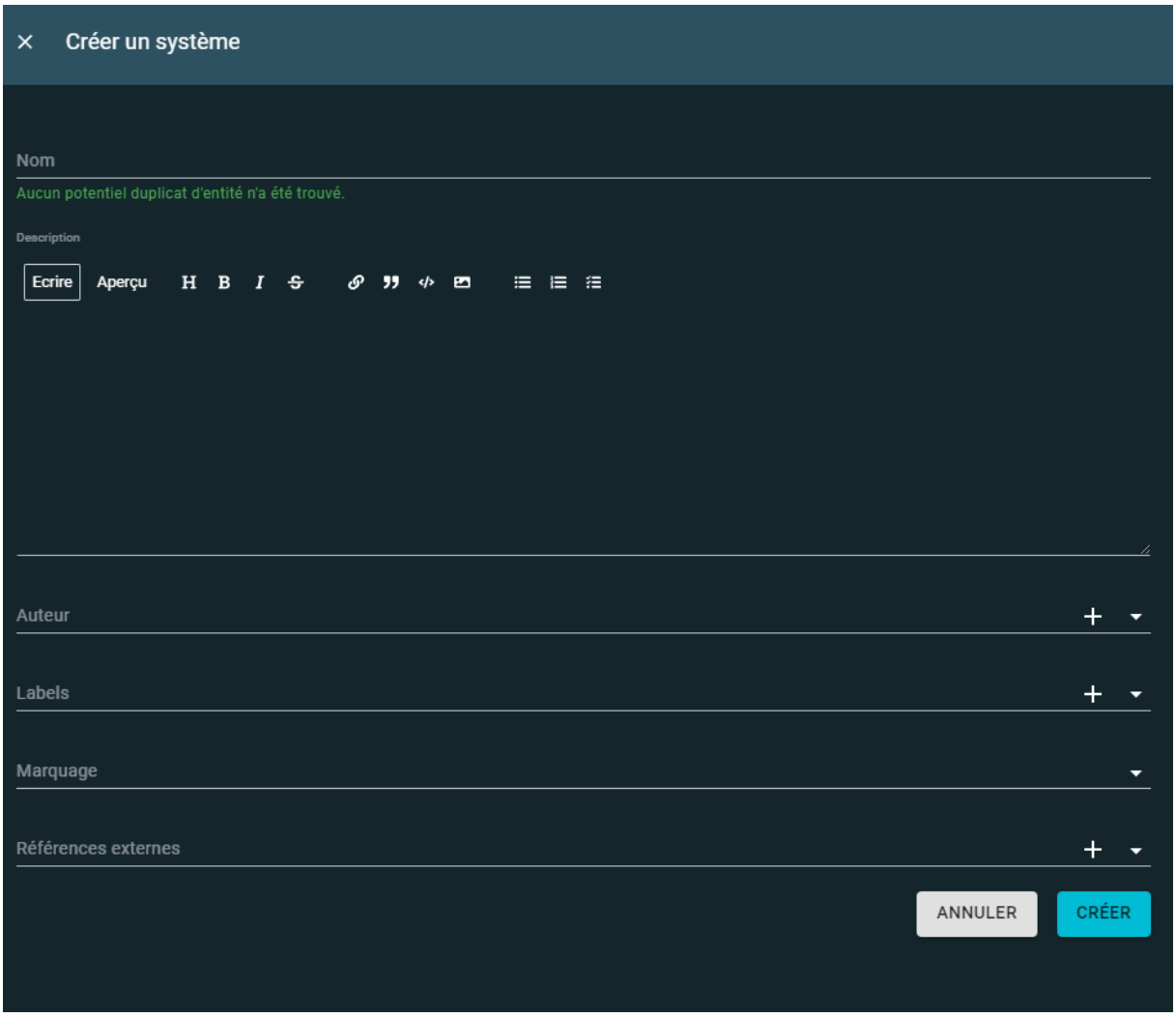


10.4.3.6 Systèmes



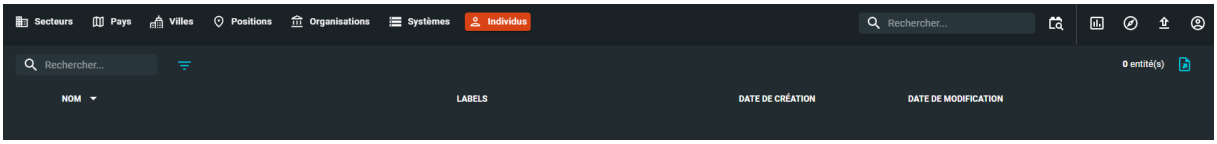
Pour ajouter un système il faut remplir les champs suivants :

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



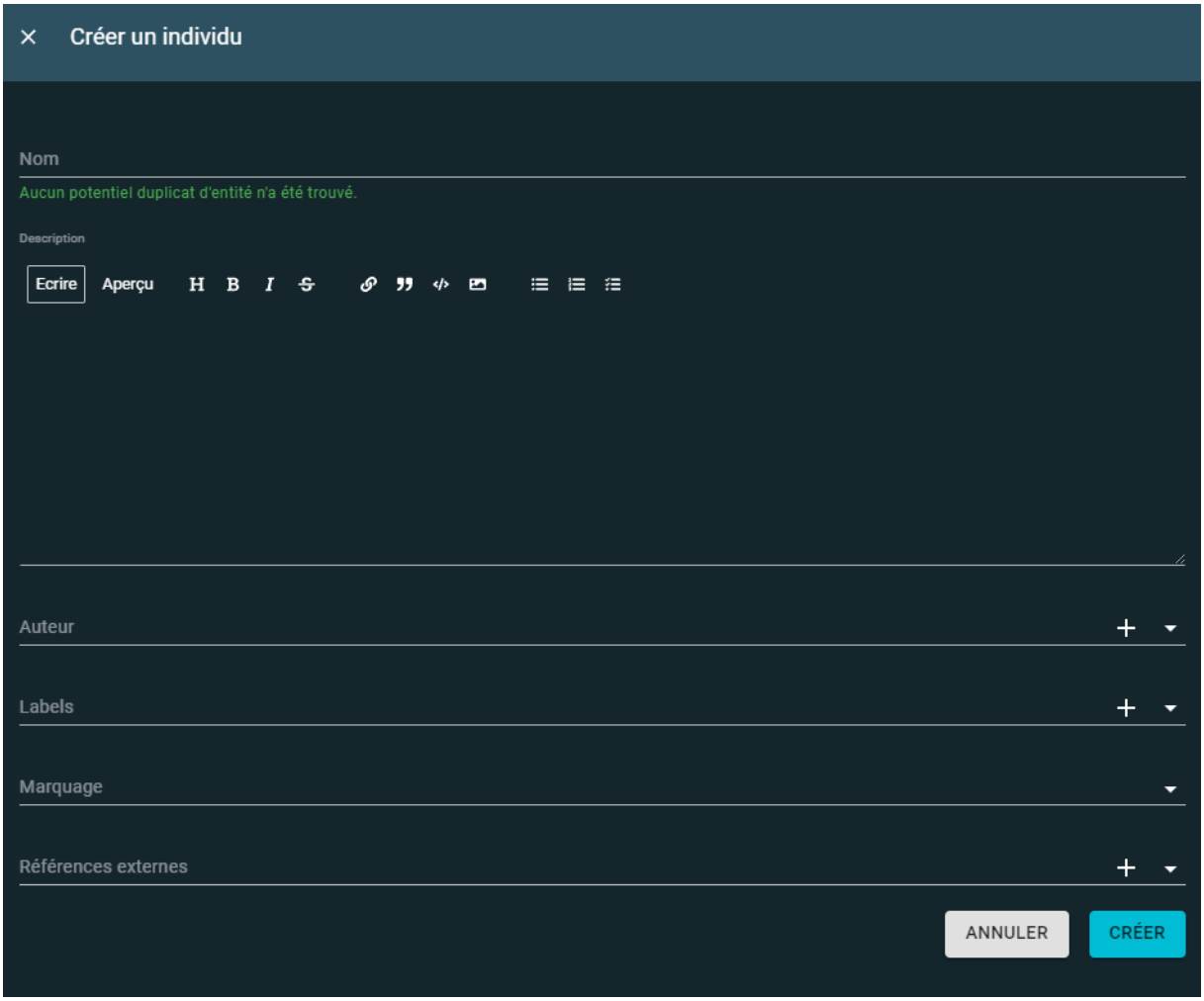
10.4.3.7 Individus

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



Pour ajouter un individu il faut remplir les champs suivants :

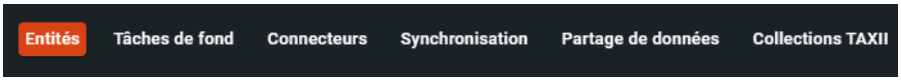
- Nom
- Description
- Auteur
- Labels
- Marquage
- Références externes



10.5 Données

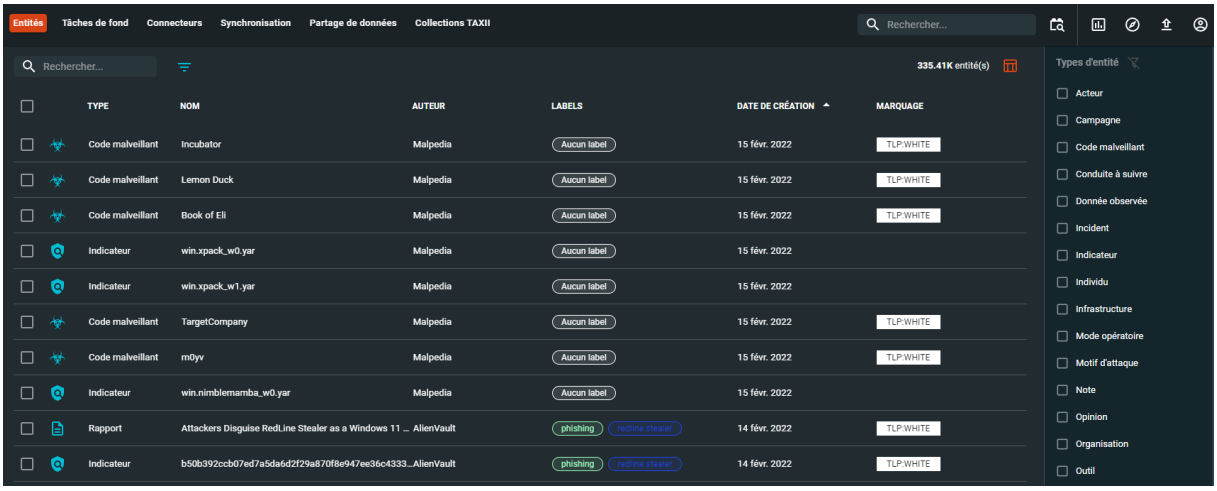
Dans ce menu se trouvent différents sous-menus :

- 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.



10.5.2 Tâches de fond

Les tâches de fond sont consultables depuis ce menu :

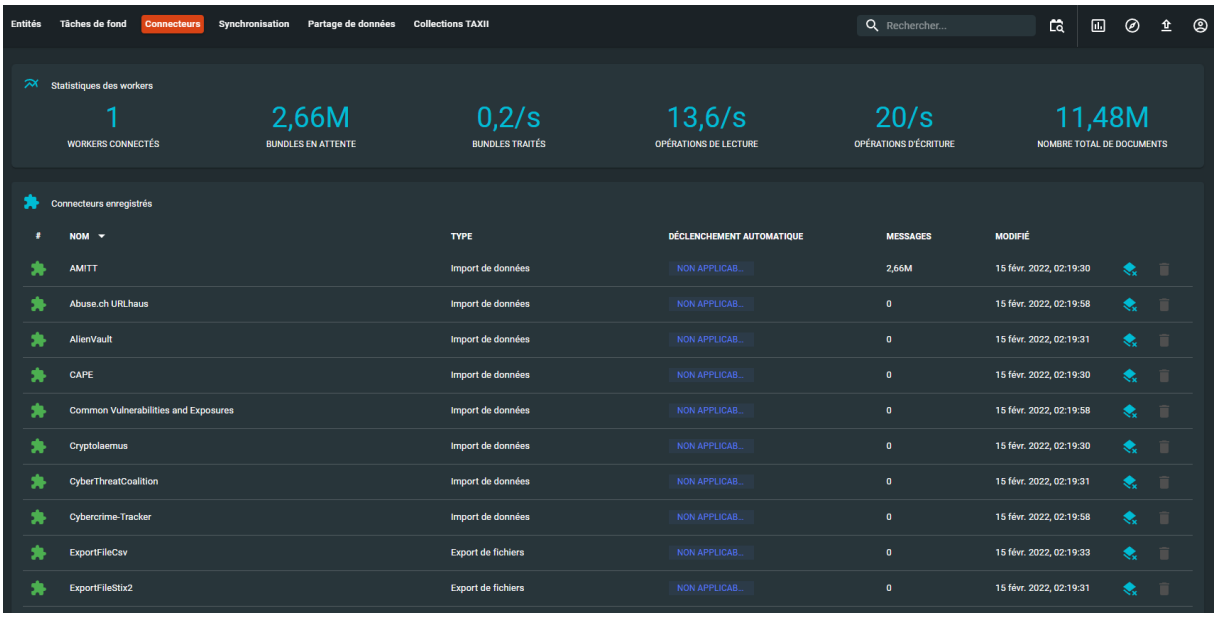
10.5.3 Connecteurs

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 :

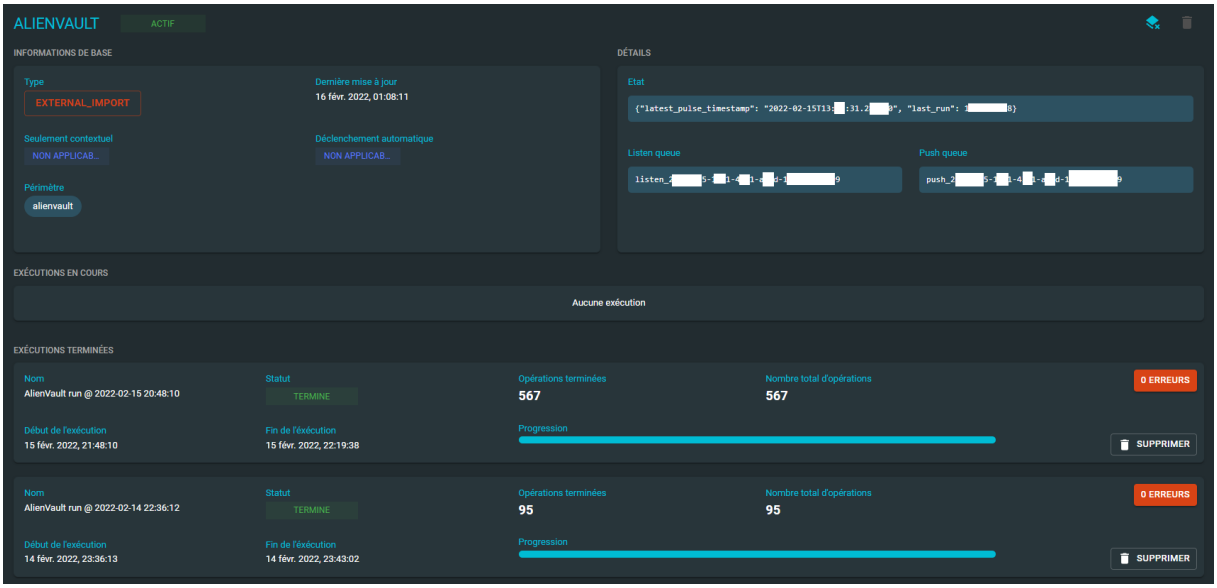
- Les noms des connecteurs
- Le type de connecteur
- Le type de déclenchement
- Le nombre de messages en attente d'import vers notre OpenCTI
- La date de la dernière modification apportée par le connecteur
- Réinitialiser l'état du connecteur
- Supprimer le connecteur



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

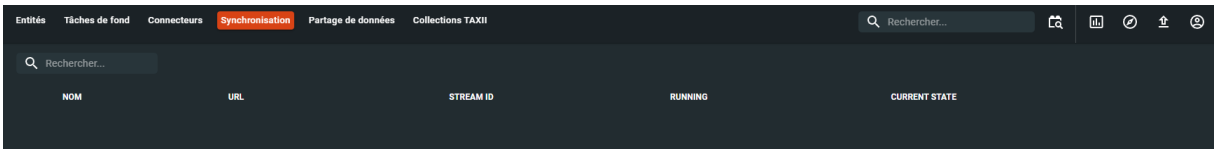
- Informations de base :
  - Un état général du connecteur
  - Quel type d'import est effectué ?
  - La date de la dernière mise à jour
- Détails
  - L'état du connecteur avec les paramètres d'horodatage
  - Listen queue : informations techniques liées à rabbitmq
  - Push queue : informations techniques 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.



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.

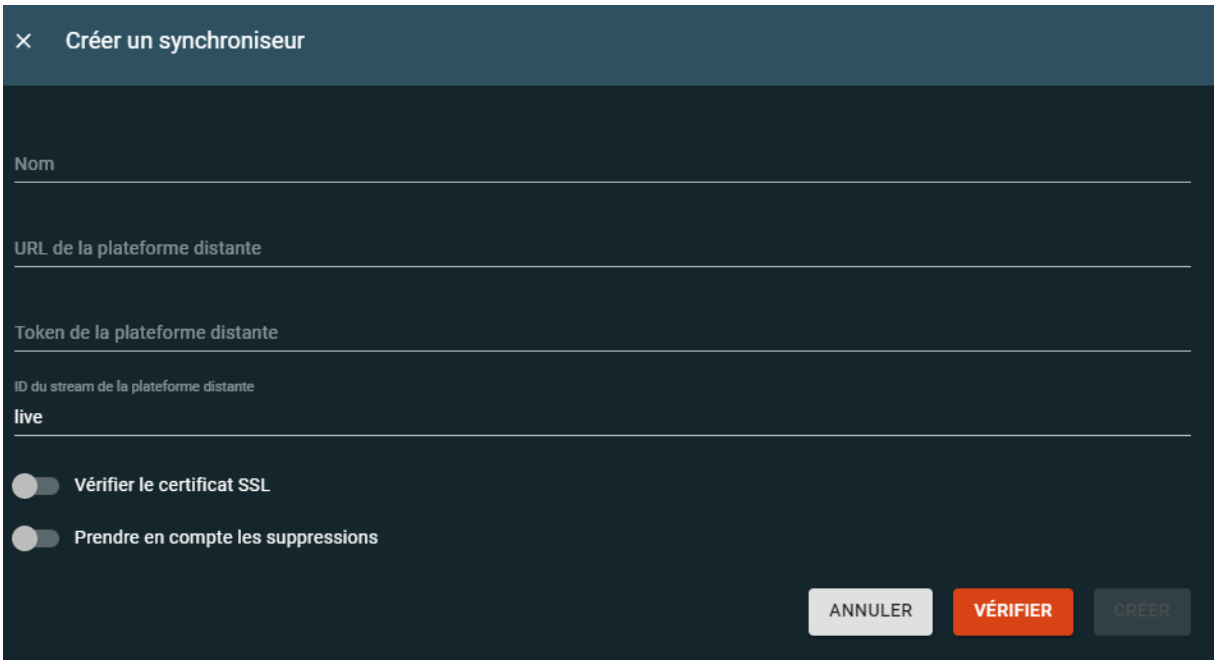


Pour créer un synchroniseur il faut remplir les champs suivants :

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

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

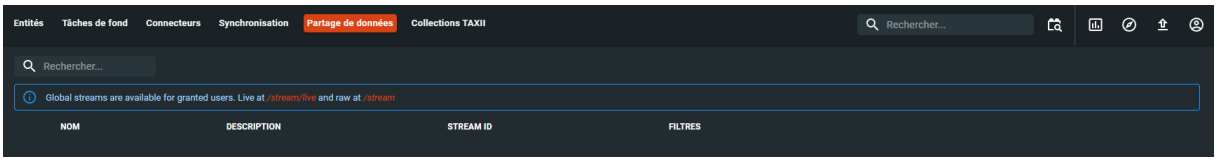
- VÉRIFIER



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 » :

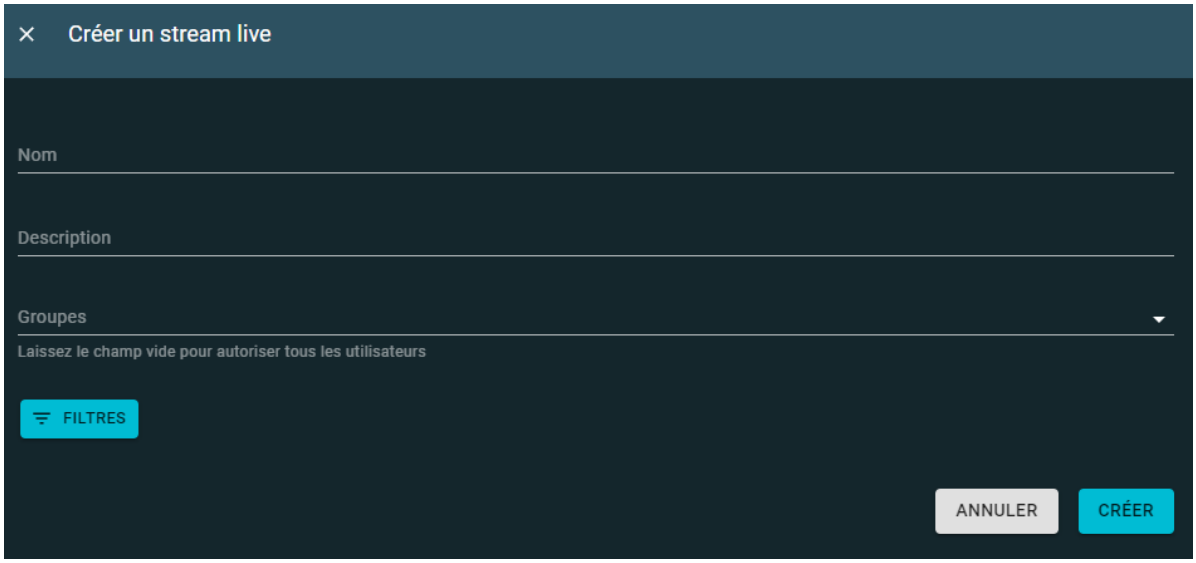

```
event: connected
data: {"lastEventId":"1          7-0","firstEventId":"1          7-0","firstEventDate":"                    :","lastEventDate":"                    ","streamSize":1977926,"connectionId":"d      6-3  6-4  e-8  9-4          1"}

id: 1          9-0
event: create
data: {"data":{"id":"marking-definition--6          d-4  7-9  a-b          9","definition_type":"tlp","definition":{"tlp":"WHITE"},"x_opencti_color":"#ffffff","x_opencti_order":1,"x_opencti_stix_ids":["marking-definition--0                    ,
5          e"],"spec_version":"2.1","created_at":"2021                    Z","updated_at":"2021                    Z","created":"2021-                    Z","modified":"2021-                    Z","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_ids":["marking-definition--                    ,
f          a"],"spec_version":"2.1","created_at":"2  1-  -  :T22:36:29.003Z","updated_at":"2021                    Z","created":"2021                    Z","modified":"2021-                    Z","x_opencti_id":"5                    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--                    ","definition_type":"tlp","definition":{"tlp":"RED"},"x_opencti_color":"#c62828","x_opencti_order":4,"x_opencti_stix_ids":["marking-definition-
          1"],"spec_version":"2.1","created_at":"                    ","updated_at":"                    ","created":"                    ","modified":"                    ","x_opencti_id":"                    ","type":"marking-
definition","x_opencti_type":"Marking-Definition","name":"TLP:RED"},"markings":[],"message":"creates a Marking-Definition `TLP:RED`","version":3}
```


Voici un exemple de « stream brut » :


```
event: connected
data: {"lastEventId":"1          7-0","firstEventId":"1          7-0","firstEventDate":"                    Z","lastEventDate":"                    Z","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



10.5.6 Collections TAXII

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

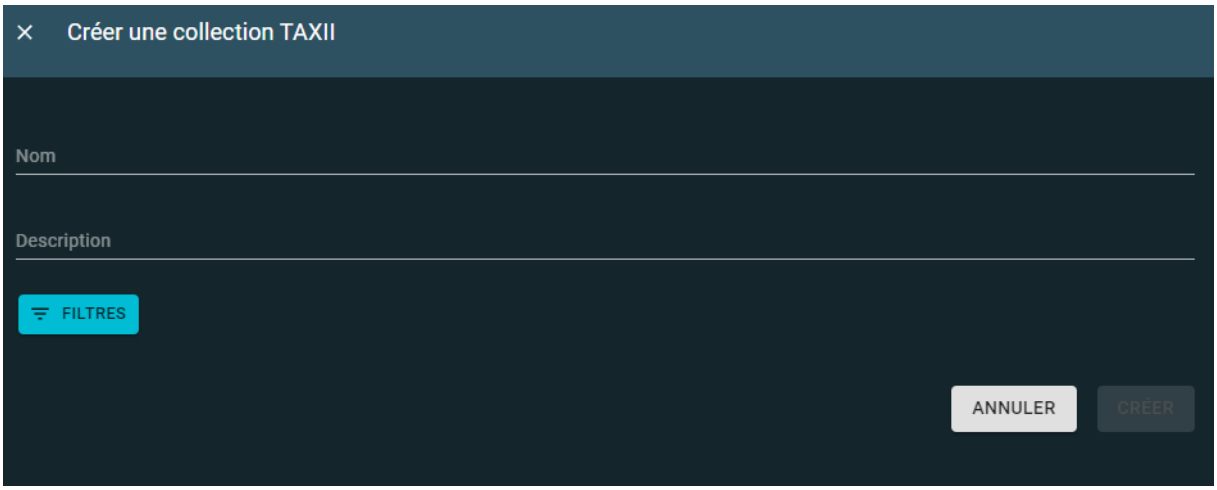
- https://oasis-open.github.io/cti-documentation/taxii/intro.html

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 :

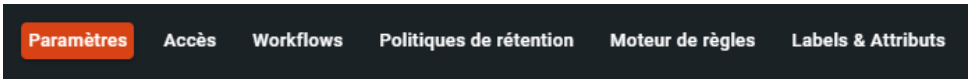
- Nom
- Description
- Filtres



10.6 Paramètres

Cette partie contiens différents menus qui sont les suivants :

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



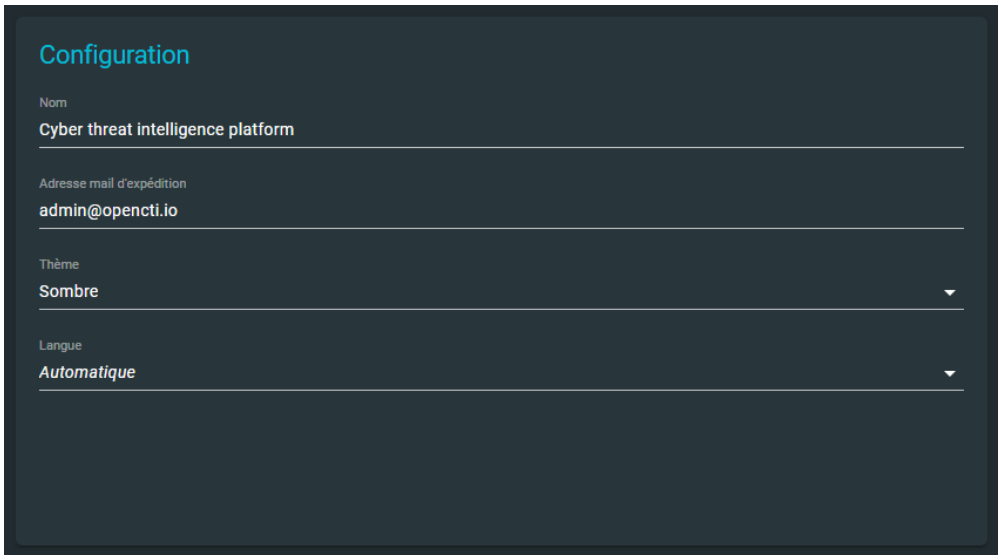
10.6.1 Paramètres

Le menu paramètre contiens différentes parties.

10.6.1.1 Configuration

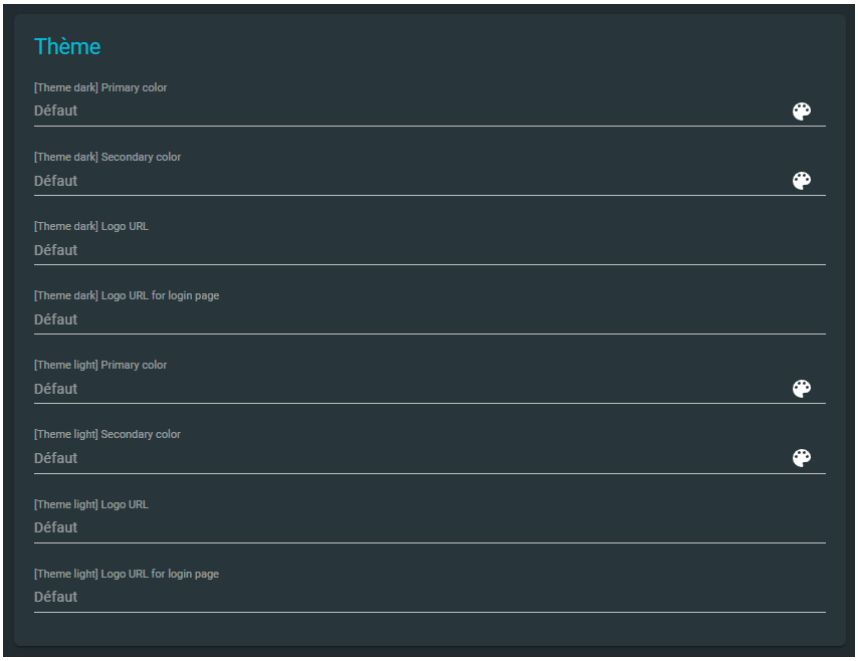
Dans cette partie nous avons les champs suivants :

- 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.



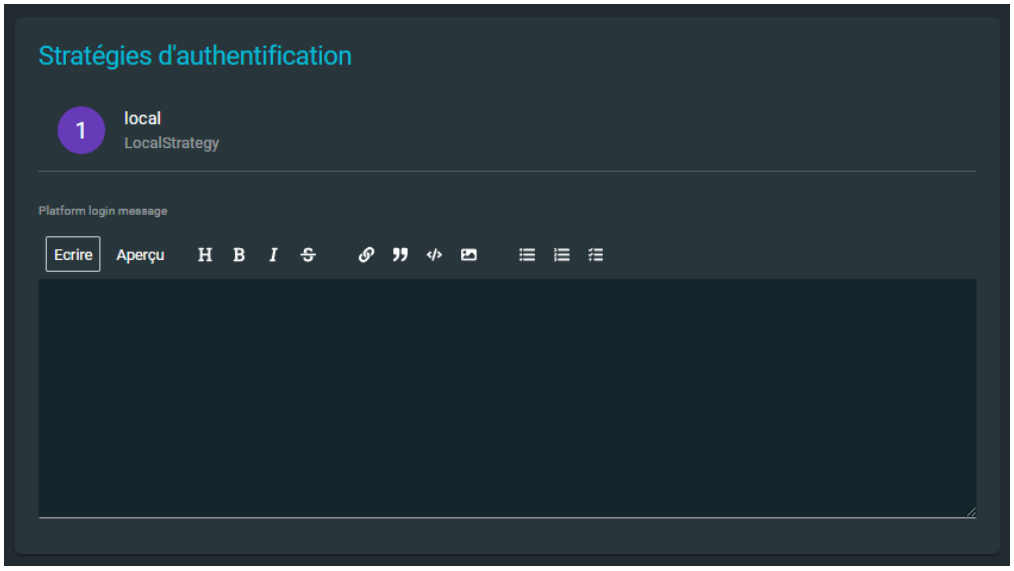
10.6.1.2 Thème

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



10.6.1.3 Stratégies d'authentification

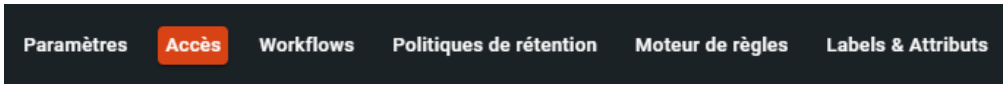
Nous pouvons définir un message à afficher lorsqu'on arrive sur la page d'authentification :



10.6.1.4 Outils

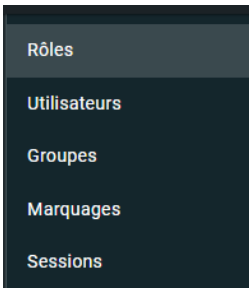
La liste des outils et leur état est affiché :

10.6.2 Accès



Le menu « Accès » est composé de différentes parties :

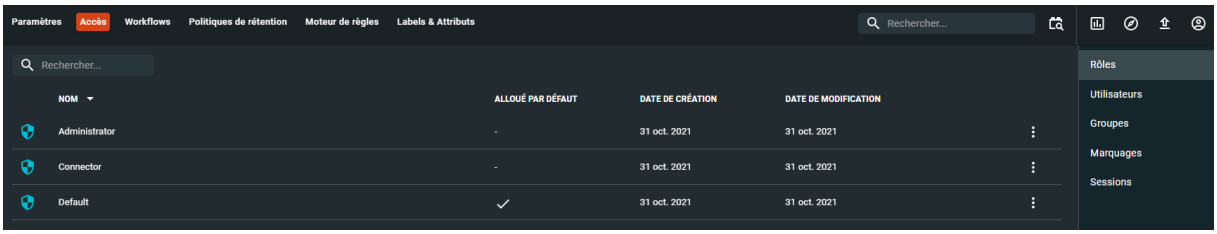
- Rôles
- Utilisateurs
- Groupes
- Marquages
- Sessions



10.6.2.1 Rôles

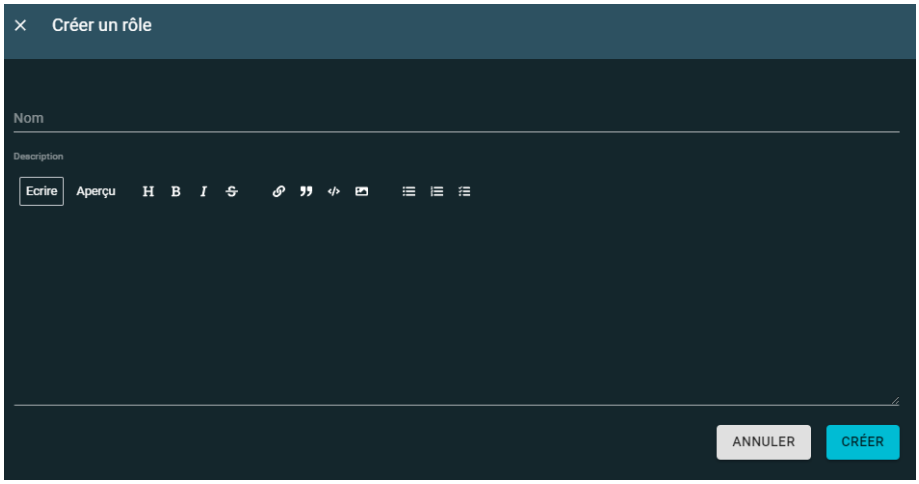
Différents types de rôles sont par défaut existants :

- 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



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

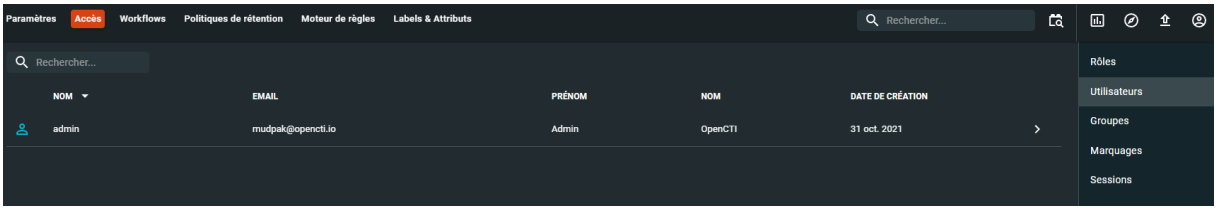
- Nom
- Description



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

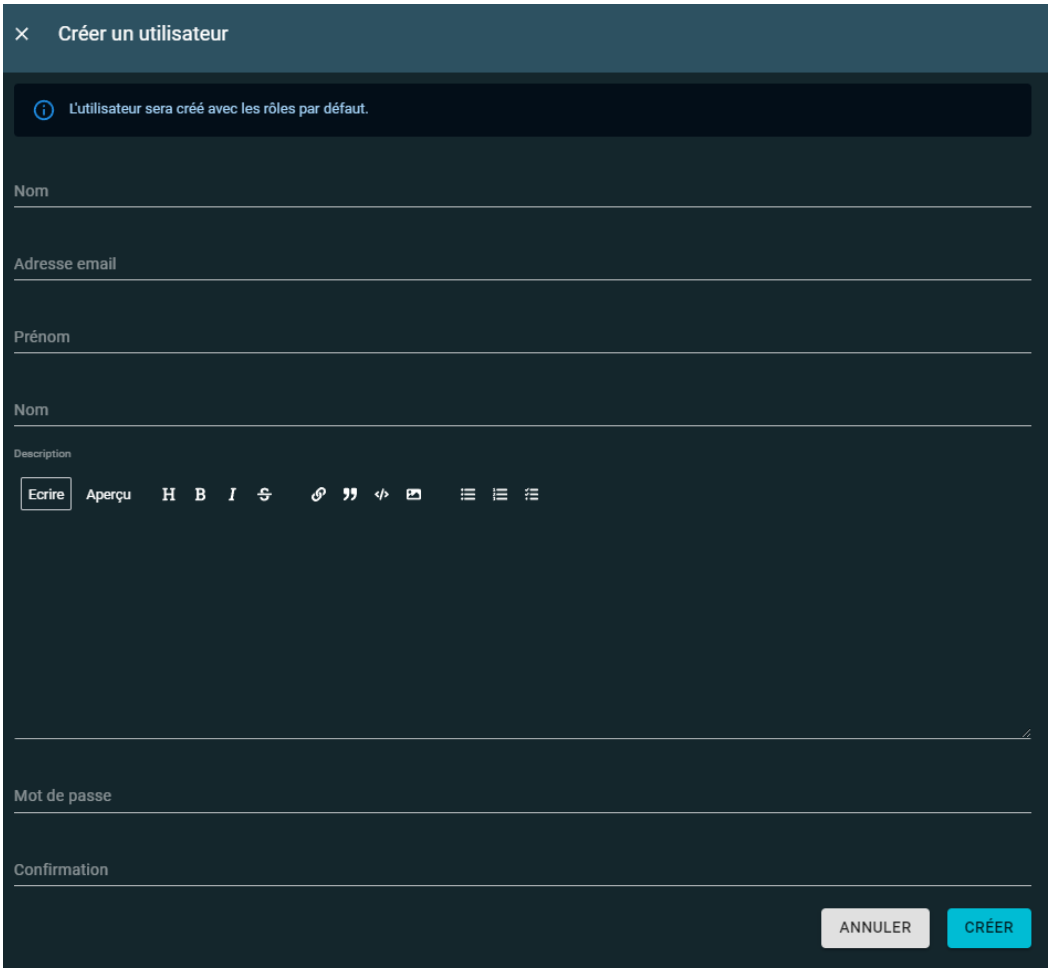
10.6.2.2 Utilisateurs

Par défaut un compte de type administrateur est présent :



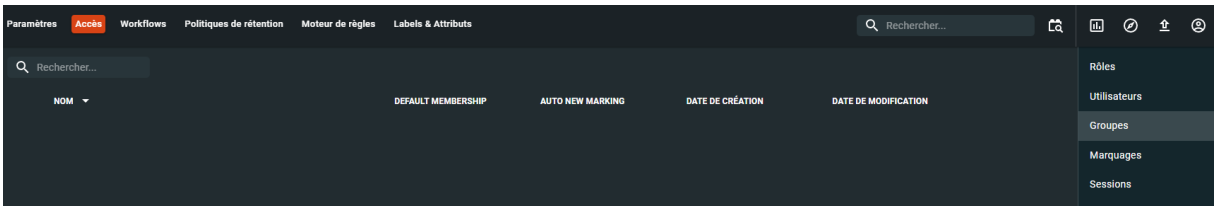
Pour créer un nouveau compte il faut remplir les champs suivants :

- Nom
- Adresse email
    - Il est important de noter que nous n'avons pas traité la partie emailing, ainsi l'utilisateur aura beau se connecteur 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



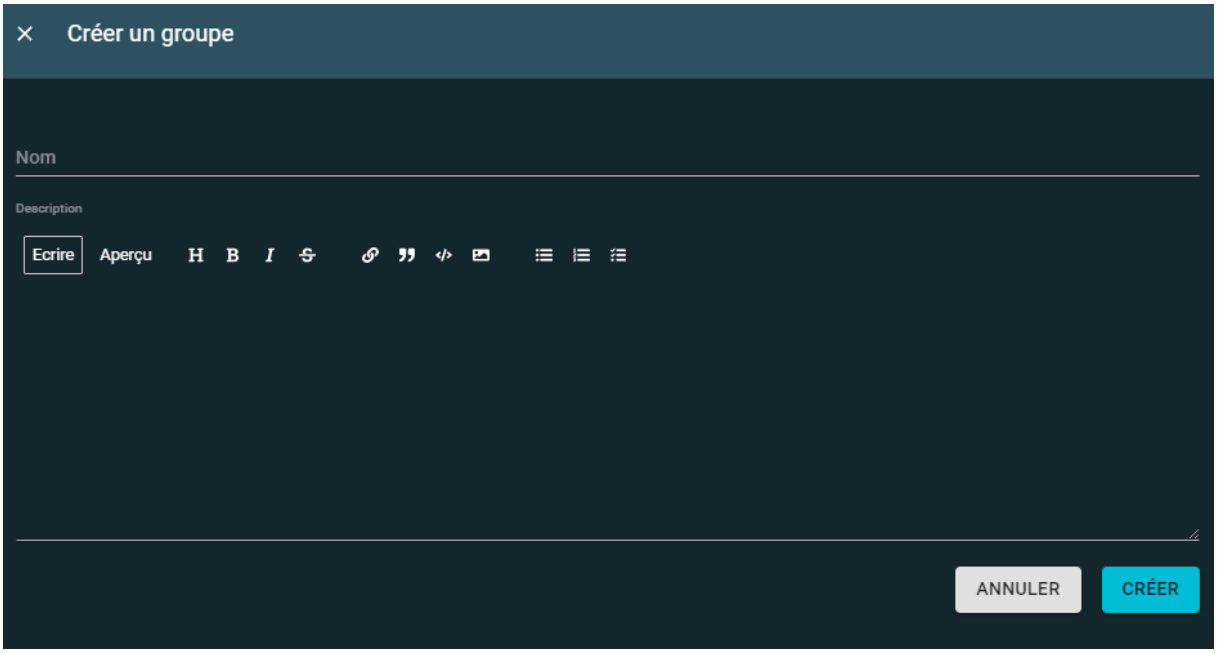
10.6.2.3 Groupes

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 :



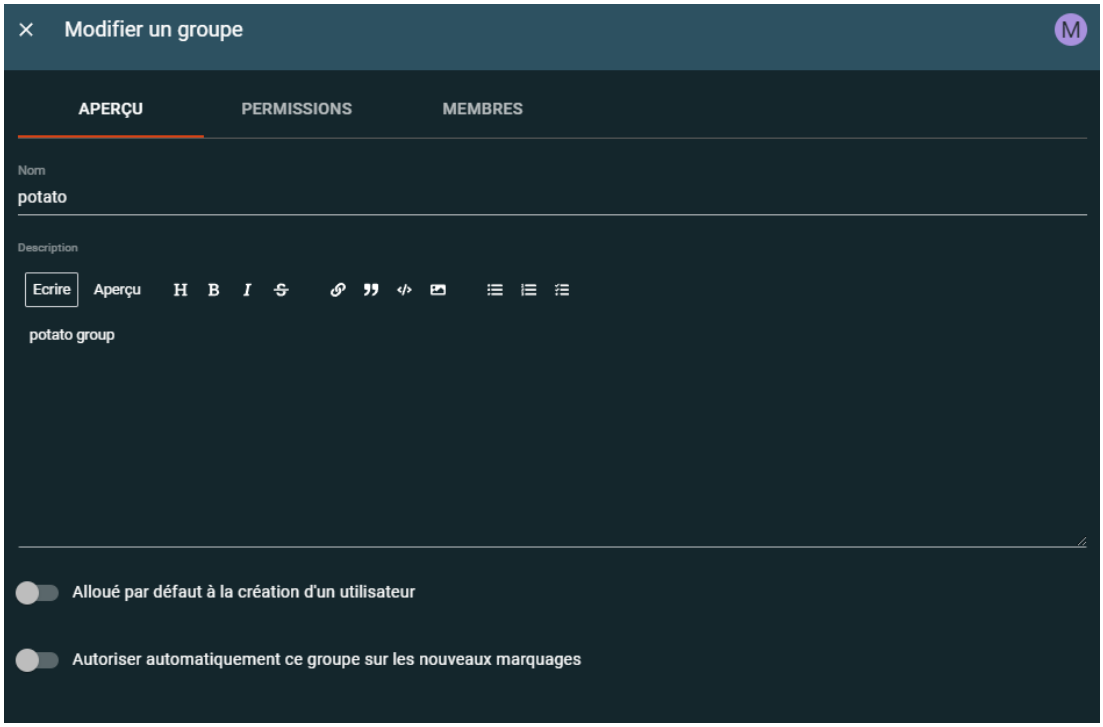
Pour créer un groupe il faut remplir les champs suivants :

- Nom
- Description

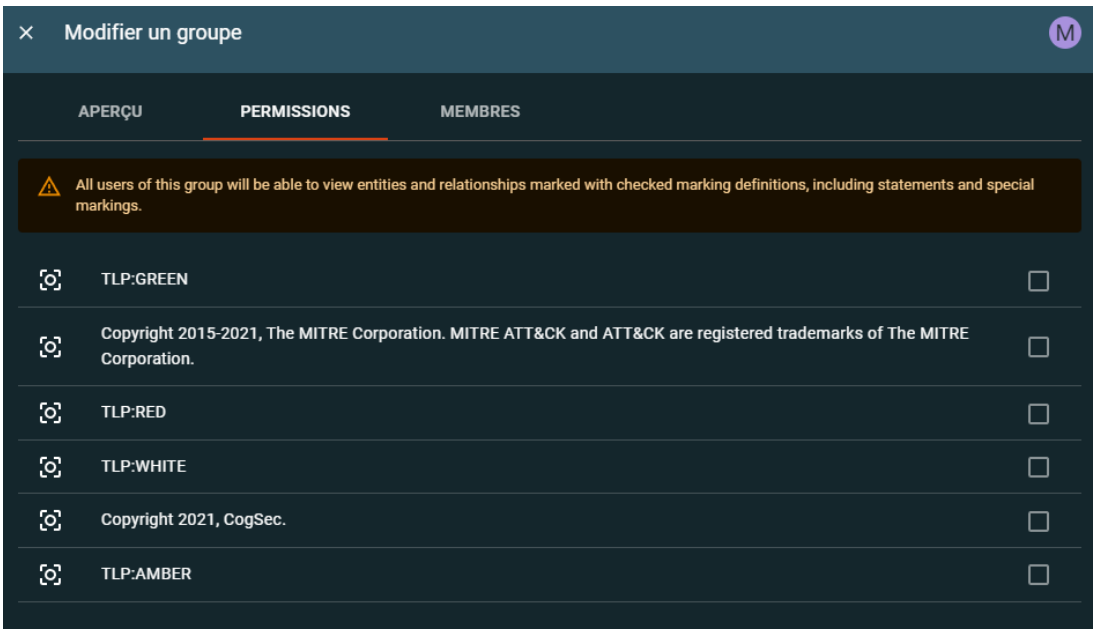


Lorsque le groupe est créé il faut modifier les paramètres :

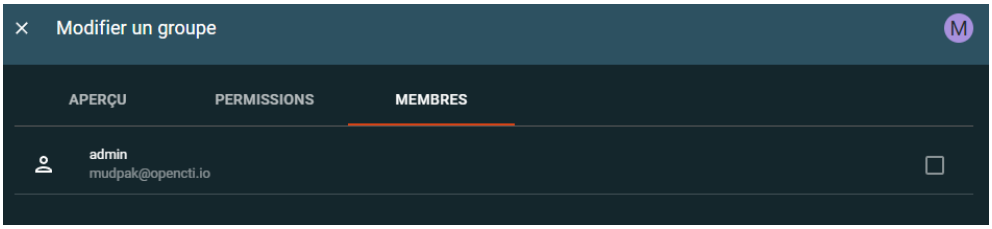
- Alloué par défaut à la création d'un utilisateur : est-ce qu'on souhaite ajouter tous les nouveaux comptes crée à ce groupe ?
- Autoriser automatiquement ce groupe sur les nouveaux marquages : est-ce qu'on ajoute ce groupe sur tous les nouveaux marquages ?



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



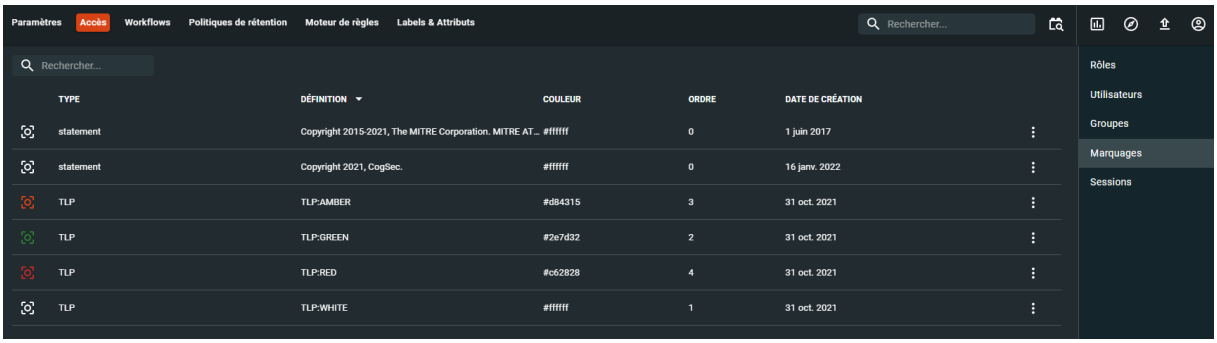
Dans le dernier onglet on peut voir ou ajouter des membres à ce groupe :



10.6.2.4 Marquages

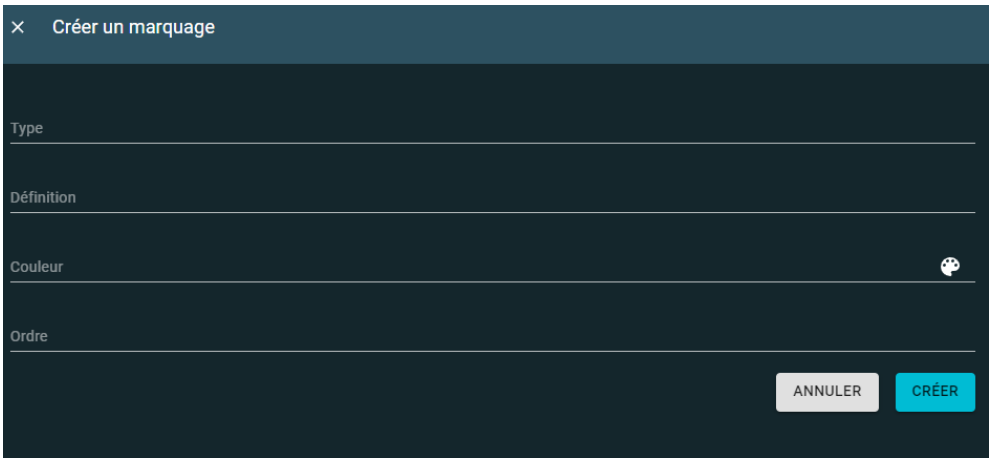
Tout au long du document j'ai évoqué les « TLP », voici donc les différents types de TLP du niveau le plus critique au moins critique :

- RED
- AMBER
- GREEN
- WHITE



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

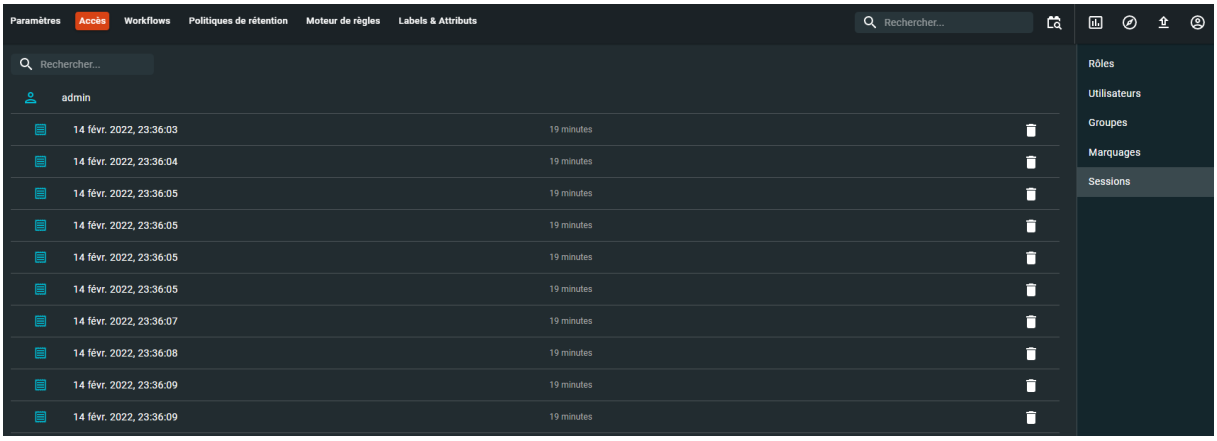
- Type
- Définition
- Couleur
- Ordre



10.6.2.5 Sessions

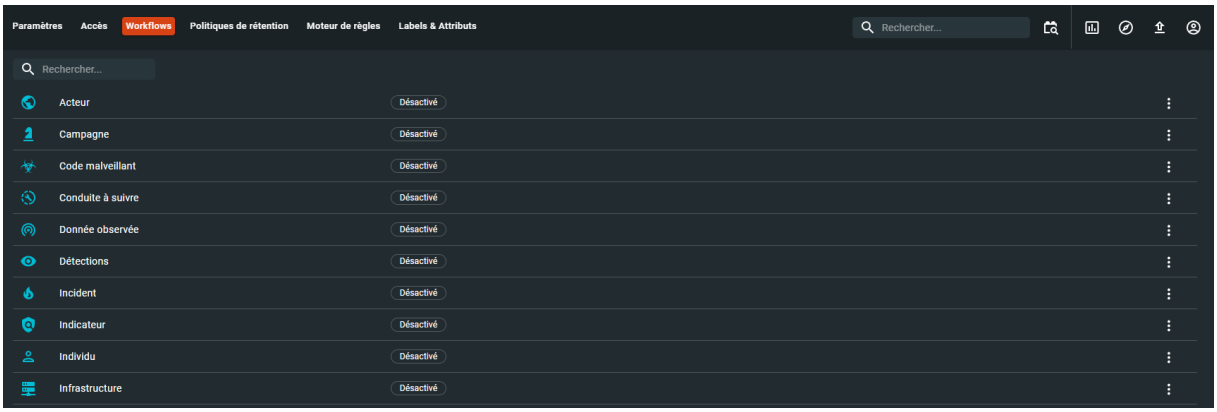
Dans cette partie nous pouvons voir l'historique des connexions des différents utilisateurs.

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



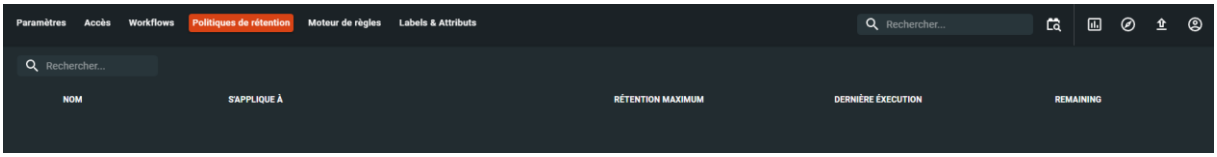
10.6.3 Workflows

Permet d'associer un workflow manuel.



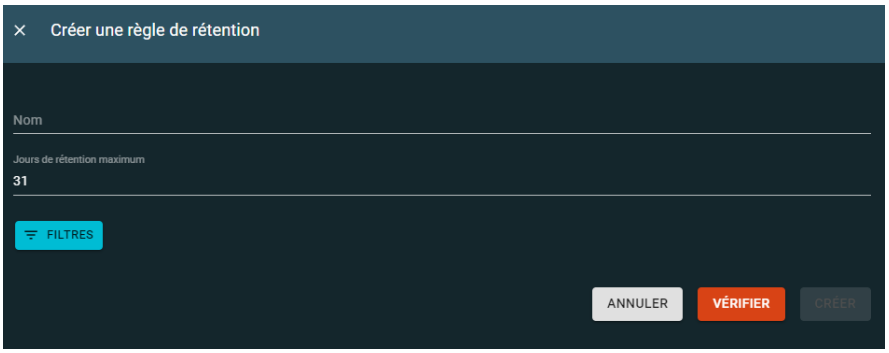
10.6.4 Politique de rétention

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 :

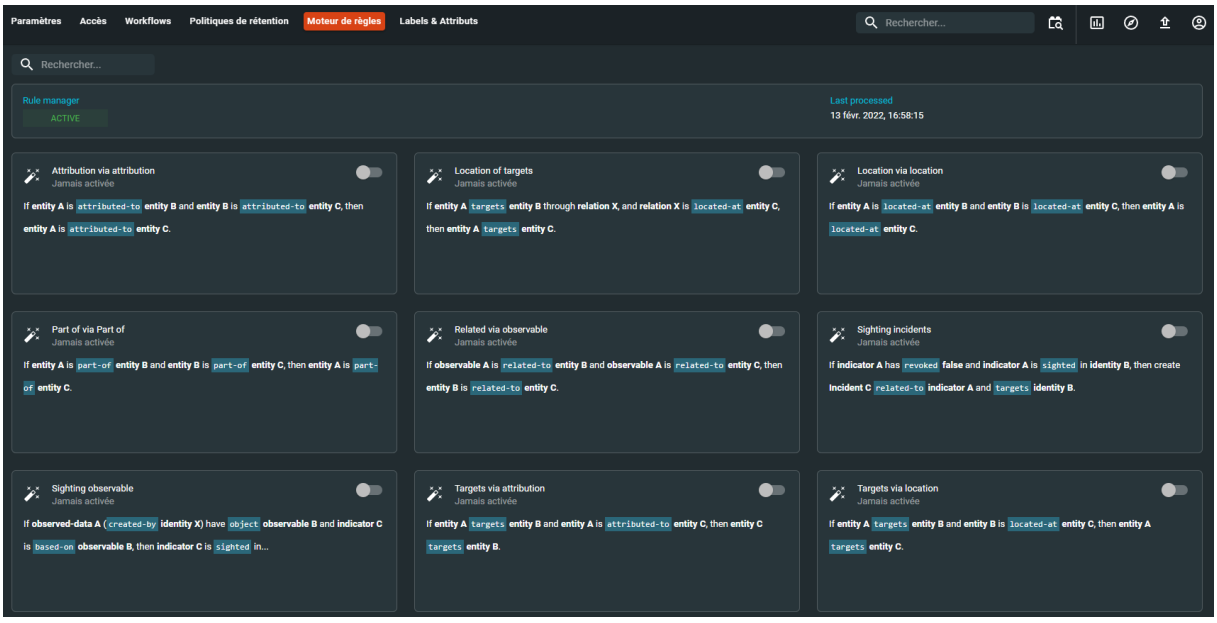
- Nom
- Jours de rétention maximum : durée après laquelle les données peuvent être supprimées
- Filtres : ces filtres vous permettront de sélectionner précisément par exemple quels niveaux de TLP sélectionner pour la conservation



10.6.5 Moteur de règles

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

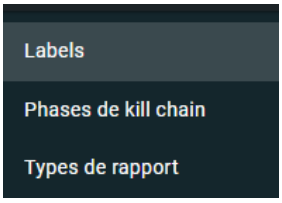
Par exemple si MALWARE1 target CITY et CITY part-of COUNTRY alors MALWARE1 target COUNTRY.



10.6.6 Labels & attributs

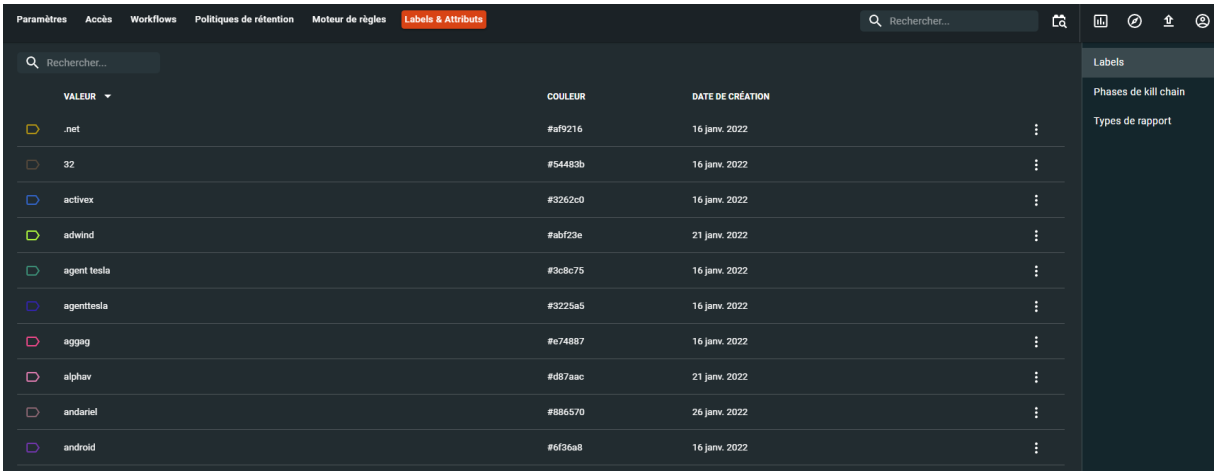
Ce menu est composé de différents onglets :

- 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.

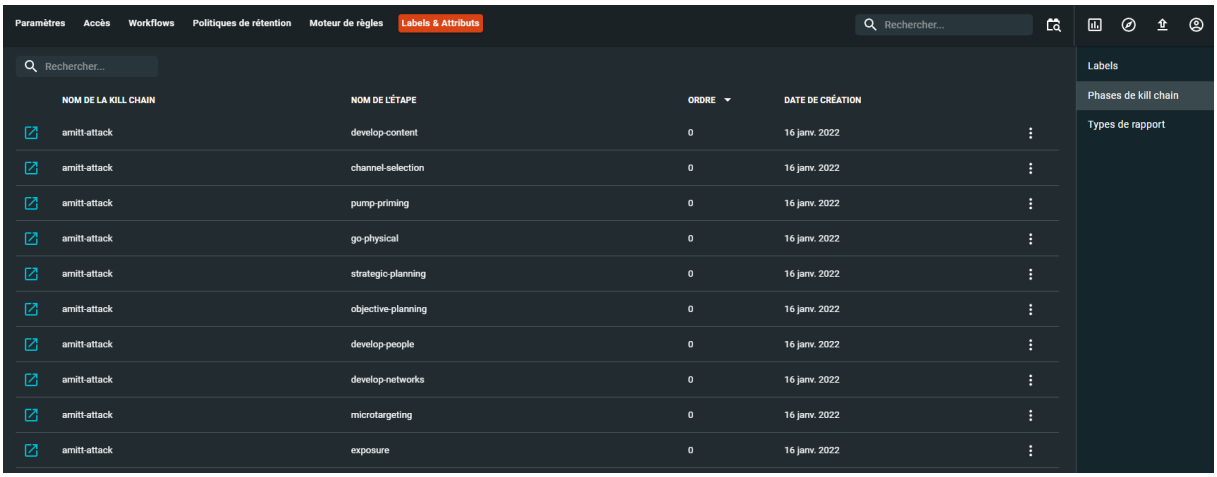


Pour créer un attribut il faut remplir le champ suivant :

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

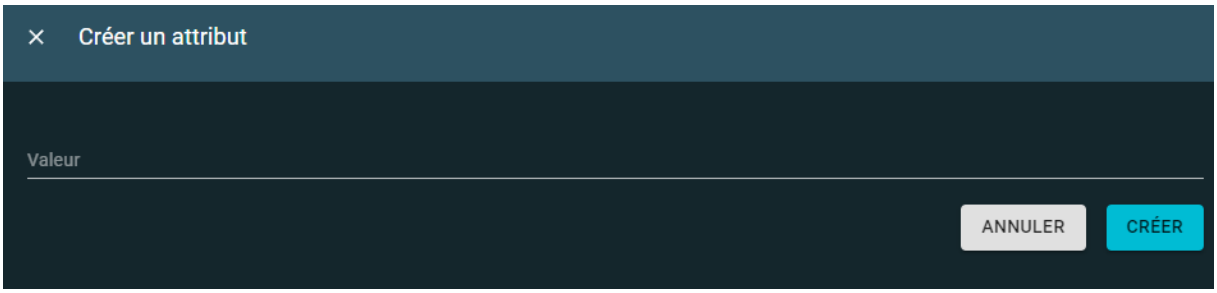
10.6.6.2 Phases de kill chain

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



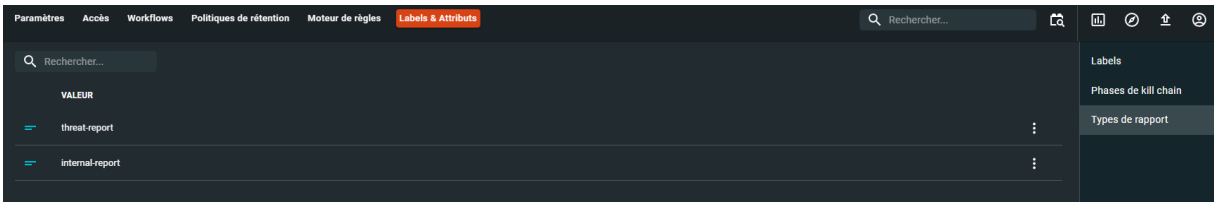
Pour créer un nouvel attribut il faut remplir le champ suivant :

- Valeur



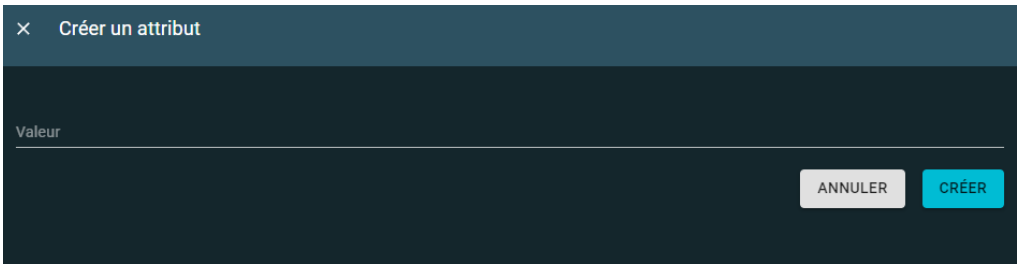
10.6.6.3 Types de rapport

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



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

- Valeur



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 à 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 a bien 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