

Sommaire

[1. Découverte de l’outil OpenCTI 1](#_Toc133476599)

[2. Analyse de surfaces d’attaques 1](#_Toc133476600)

[3. Découverte d’outils d’analyses 1](#_Toc133476601)

[4. Analyse d’anomalie 2](#_Toc133476602)

# 1. Découverte de l’outil OpenCTI

**Information sur l’outil :**  
Le projet **OpenCTI** a été initié en septembre 2018 par l'ANSSI et co-développé avec le CERT-EU en l'absence de solutions complètement appropriées pour structurer, stocker, organiser, visualiser et partager la connaissance de l'ANSSI en matière de cybermenace, à tous les niveaux.

Cet outil s’installe généralement dans un environnement cloud sur un cluster kubernetes car il demande beaucoup de ressources et de stockage.

Cet outil peut être lié à un EDR ou un SIEM pour obtenir de meilleurs performances. L’EDR ou le SIEM vont détecter une intrusion ou un comportement suspect et tout sera « loggé » dans l’outil CTI afin d’avoir une traçabilité.

# 2. Analyse de surfaces d’attaques

Une surface d’attaque est une surface d’exposition de l’organisation qu’un attaquant pourrait exploiter.

Il existe différentes façons de réduire la surface d’exposition, par exemple :

* Analyser les services externes
* Analyser les AS
* Analyser les entrées DNS (avec dnsdumpster.com)

# 3. Découverte d’outils d’analyses

**Outil n°1 :** Shodan ([www.shodan.io](http://www.shodan.io))

Shodan est un moteur de recherche créé en 2009 par John Matherly. Ce site référence le résultat de balayages de ports massifs effectués sur le réseau Internet

Exemple de test de port : **« port:161 country:cm »**

**Outil n°2 :** ZoomEye qui est la version Chinoise de Shodan

**Outil n°3 :** LeakIX (leakix.net)

# 4. Analyse d’anomalie

Il est possible de détecter une anomalie de différentes façons grâce à des indices de compromission :

* Charge CPU & Mémoire élevé
* Tentative d’accès à une ressource interne (dossiers partagés, annuaire de l’entreprise, scan du réseau…)

Localisation ou ASN

Sur une IP de l’étranger

Vérifier/Filtrer les sorties

Vigilance permanente sur la création des DNS / Filtrage DNS

Sur un port de destination exotique

Sur un DNS suspect

Connexions réseaux douteuses externes

Appel de DLL

Obfuscation

Comportement de l’executable

Utilisation de mémoire

Structure de l’EXE (UPX) et Entropie

Trace d’encodage (Base64)

Adresse Bitcoin

Nom de domaine

Tous ces indices de compromission permettent de récupérer des signatures de type YARA ou SIGMA ou alors de vérifier le HASH de chaque fichier.

**Remarque : Il existe un outil en ligne pour vérifier tous fichier suspect que nous pouvons recevoir. Si nous ne sommes pas sûr de son authenticité nous pouvons allons sur le site « Virus Total » et y placer le fichier**

**L’outil « Jadx » permet de faire du reverse engineering sur des applications Android. L’objectif est de décompiler le code**