

[SOC] Outils de cyber défense

Introduction

Cette page répertorie une base d'outils de cyber défense utile à un SOC ou même à un administrateur aguerri et conscient des enjeux cyber.



Scanner d'URL

Une multitude d'outils existent pour scanner les URL grâce à leur réputation.

Voici une liste d'outils :

- [VirusTotal](#)
- [MetaDefender Cloud - OPSWAT](#)
- [URLscan.io](#)
- [URLhaus](#)
- [Whols](#)
- [Cisco Talos Intelligence](#)
- [ThreatMiner](#)
- [Brightcloud](#)

Scanner d'adresse IP

Voici une liste d'outils en ligne pour analyser la réputation des adresses IP :

- [AbuseIPDB](#)
- [MetaDefender Cloud - OPSWAT](#)
- [Cisco Talos Intelligence](#)
- [Feodo Tracker](#)
- [Threatbook](#)
- [Pulsedive](#)
- [Shodan](#)
- [XForceIBM](#)
- [Alienvault](#)
- [GreyNoise](#)

Scanner de fichier et de hash

Voici une liste d'outils en ligne pour analyser des fichiers et des hashes de fichiers :

- [VirusTotal](#)
- [MetaDefender Cloud - OPSWAT](#)
- [MalwareBazaar](#)
- [Malshare](#)
- [Cisco Talos Intelligence](#)

- [HybridAnalysis](#)

Règles de détection

- [SOC Prime Threat Detection Marketplace](#)

Blacklist d'empreintes de certificats SSL

- [SSL Blacklist](#)

Scanner de mail

Pour se protéger du phishing, il peut être utile d'utiliser des outils qui vont décortiquer le mail afin de potentiellement trouver des IOC.

- [PhishTool](#)

Sandbox

Les sandboxes permettent de tester le comportement de fichier ou de site web afin de détecter un comportement malveillant dans un environnement protégé.

- [Browserling](#) : Accéder à un site web dans une sandbox.
- [AnyRun](#) : Lancer un exécutable Windows dans une sandbox.
- [Wannabrowser](#) : Accéder à un site web dans une sandbox.

Matrice MITRE ATT&CK

Framework permettant notamment de lister les TTPs et les APT.

- [MITRE ATT&CK](#)

Liste d'IOC multiples

- [ThreatFox](#) : MISP events, Suricata IDS Ruleset, Domain Host files, DNS Response Policy Zone, JSON files and CSV files.

PS - Obtenir le hash d'un fichier

```
Get-FileHash <FILE> -Algorithm MD5
```

Revision #9

Created 6 September 2023 12:29:23 by Elieroc

Updated 23 May 2024 14:18:44 by Elieroc