[CTI] Ressources

Introduction

Plusieurs types de ressources sont nécessaires en CTI, notamment les outils et les frameworks pour collecter ou enrichir vos listes d'IOCs, et les ressources pour comprendre les menaces et connaître les acteurs malveillants.

IOCs

CI Bad Guys

- https://threatfeeds.io/?feed=CI%20Bad%20Guys

Duggytuxy

- https://github.com/duggytuxy/malicious_ip_addresses

Actualités des menaces et CVE

Awesome annual reports

Repos Github actualisé avec les derniers rapports de threat intelligence :

- https://github.com/jacobdjwilson/awesome-annual-security-reports

Malpedia

- https://malpedia.caad.fkie.fraunhofer.de/library

AttackerKB

- https://attackerkb.com/

Krebs on Security

- https://krebsonsecurity.com/

The Hacker News

- https://thehackernews.com/

ThreatPost

- https://threatpost.com/

Dark Reading

- https://www.darkreading.com/

Zeroday Initiative

Permet de suivre les dernières CVE sorties :

- https://www.zerodayinitiative.com/advisories/published/

Onion 666

Permet de trouver les liens vers le dark net

- https://onion666.com/ON66IkM6Ybnv.html
- https://darknet-tor.com/meilleurs-sites-onion-deepweb.php

DeepDarkCTI

Donne des feeds sombres à suivre vers le darknet, Telegram et autres :

- https://github.com/fastfire/deepdarkCTI

Revision #6
Created 22 May 2024 12:55:56 by Elieroc
Updated 6 August 2024 09:33:13 by Elieroc