

Threat Intelligence (CTI)

Un ensemble de ressources pour la CTI et comprendre les menaces cyber.

- [\[CTI\] Ressources](#)
- [\[CTI\] Nuclei](#)
- [\[CTI\] Shodan](#)

[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 :

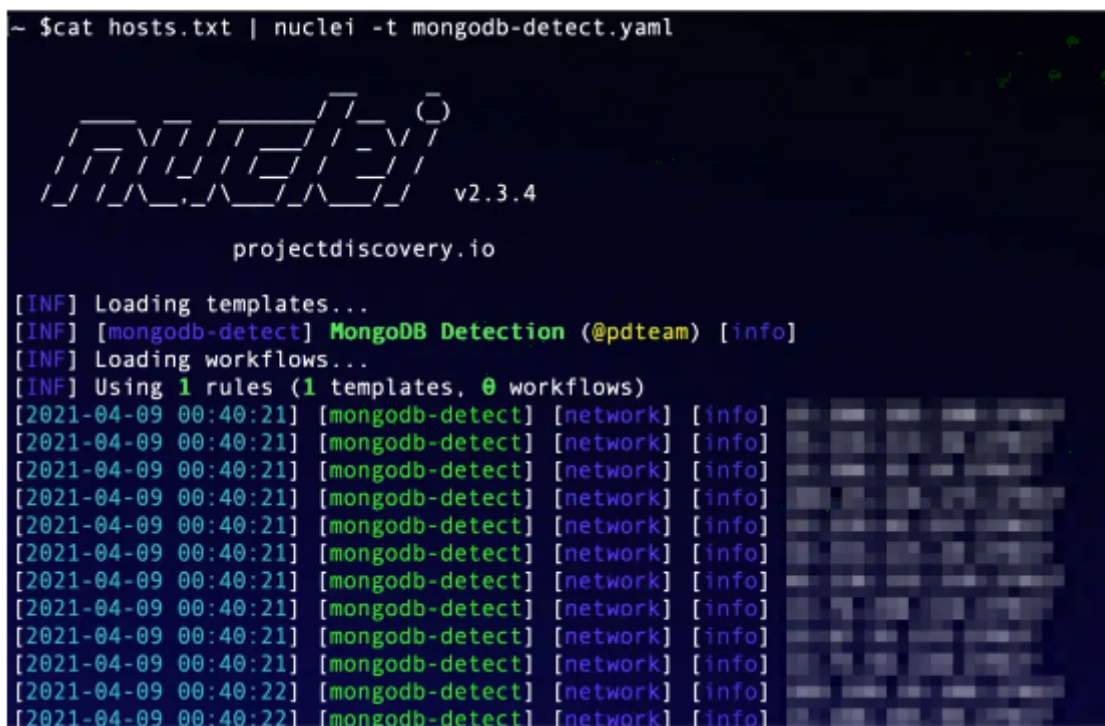
- <https://github.com/fastfire/deepdarkCTI>

[CTI] Nuclei

Introduction

Le logiciel Nuclei permet de tester l'exploitabilité d'une vulnérabilité sur des systèmes grâce à des templates au format YML.

```
~ $cat hosts.txt | nuclei -t mongodb-detect.yaml
```



```
projectdiscovery.io

[INF] Loading templates...
[INF] [mongodb-detect] MongoDB Detection (@pdteam) [info]
[INF] Loading workflows...
[INF] Using 1 rules (1 templates, 0 workflows)
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:21] [mongodb-detect] [network] [info]
[2021-04-09 00:40:22] [mongodb-detect] [network] [info]
[2021-04-09 00:40:22] [mongodb-detect] [network] [info]
```

Installation & MAJ

Projet

- <https://github.com/projectdiscovery/nuclei>

Installation

Pour installer Nuclei (go doit être installé au préalable) :

```
go install -v github.com/projectdiscovery/nuclei/v3/cmd/nuclei@latest
```

MAJ

Pour mettre à jour **Nuclei** :

```
nuclei -update
```

Pour mettre à jour les **templates** :

```
nuclei update
```

Manuel

Exemple template

Voici un exemple de template pour une CVE SSH (**cve-2024-6387.yaml**) :

```
id: CVE-2024-6387
```

```
info:
```

```
  name: RegreSSHion detect (based on software version)
```

```
  author: UnaPibaGeek
```

```
  severity: High
```

```
  description: Regression (CVE-2024-6387) software version checker.
```

```
  classification:
```

```
    cve-id: CVE-2024-6387
```

```
  metadata:
```

```
    max-request: 2
```

```
    vendor: OpenSSH
```

```
    product: OpenSSH
```

```
    tags: cve,cve2024,regression,openssh,ssh
```

```
tcp:
```

```
  - host:
```

```
    - '{{Hostname}}'
```

```
    - '{{Host}}:22'
```

```
  inputs:
```

```
    - data: "SSH-2.0-OpenSSH_9.0\r\n"
```

- 'OpenSSH_(8\.[5-9]p[1-2]?|9\.[0-7]p[1-2]?|[0-3]\.[0-9]p[1-2]?|4\.[0-3]p[1-2]?)'

```
nuclei -t cve-20224-6387.yaml -l ips.txt
```

[CTI] Shodan

Introduction

Shodan est un moteur de recherche permettant de trouver des machines exposées sur Internet avec des filtres.



SHODAN

Manuel

Vous pouvez accéder à l'interface de Shodan :

- <https://www.shodan.io/dashboard>

Usage

<FILTER>:<VALUE>

Filtres

Voici quelques filtres courants :

Filtres
ip
port
org
country
city
product
version
os

Sinon voici la liste complète des filtres :

- <https://www.shodan.io/search/filters>

Exemples

- Chercher des informations sur une IP spécifique :

ip:8.8.8.8

Chercher toutes les machines françaises de l'hébergeur Scaleway :

country:FR org:scaleway

Chercher toutes les machines Ubuntu ayant un service SSH :

os:ubuntu port:22

Vous pouvez retrouver plus d'exemples :

- <https://www.shodan.io/search/examples>
- <https://github.com/BushidoUK/OSINT-SearchOperators/blob/main/ShodanQueriesAppliances.csv>

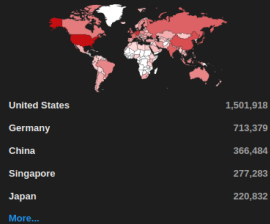
Analyse

Vous pouvez analyser les résultats rapidement grâce à la section **View Report** :

TOTAL RESULTS

5,359,574

TOP COUNTRIES









TOP PORTS










80	1,728,827
22	1,668,706
443	1,301,665
9100	118,159
2222	43,287
More...	

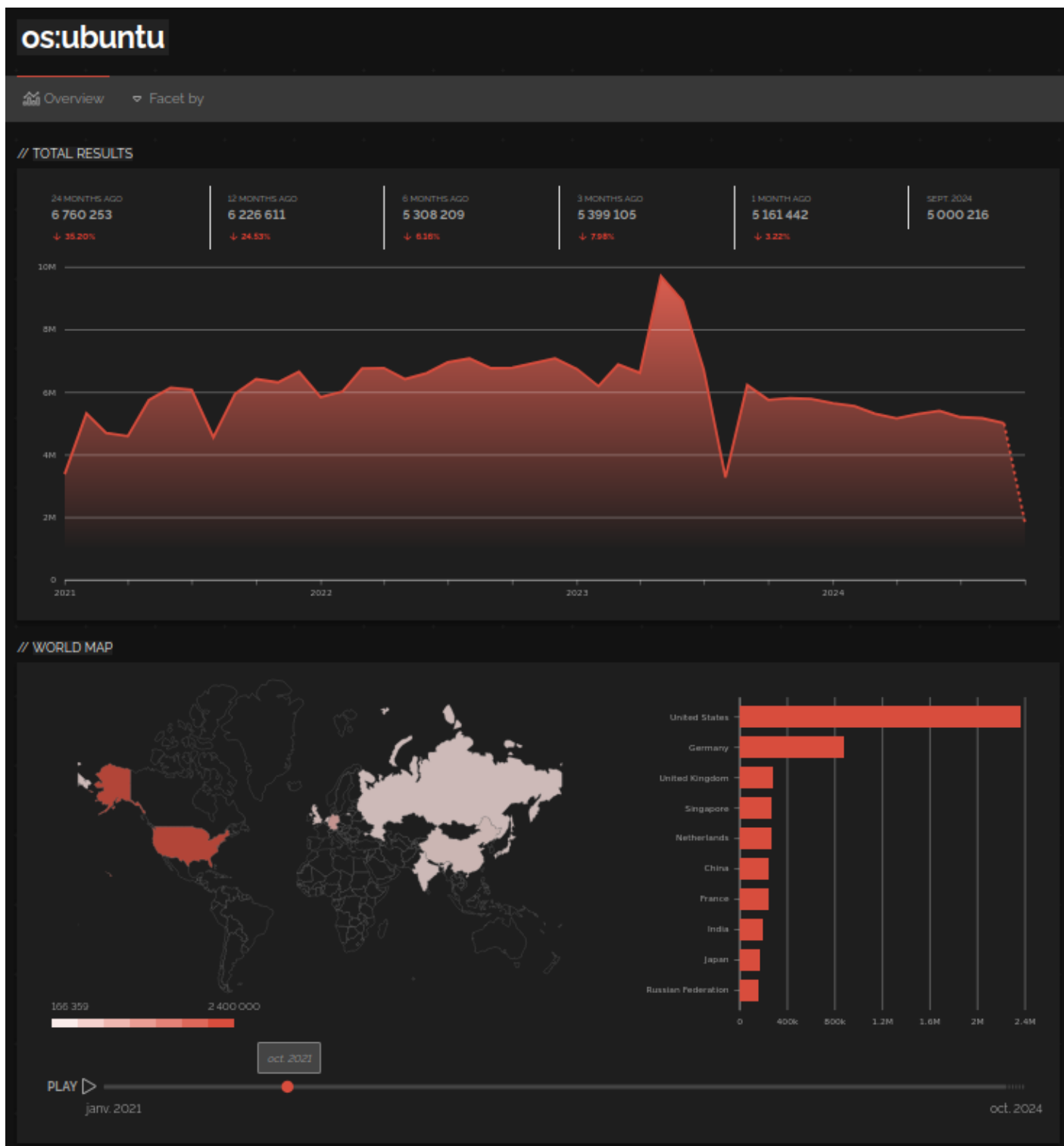
TOP ORGANIZATIONS

DigitalOcean, LLC	796,495
-------------------	---------

 View Report  Download Results  Historical Trend  Browse Images  View on Map  Advanced Search

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out [Gravwell](#)

69.167.49.68  ipinfo.io/ip/69.167.49.68  United States, Orem	SSH-2, 8-OpenSSH_7.6p1_Ubuntu-4ubuntu8.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAQDZBYW7ZJ+oD6JUSY1+9EU0Ht6gTn/ZawJjbra5pTsup98oyIFhgT5Q5oe9RfPqkqtrub2N3DRvGhIqjIrn1NKTG6sluZYfRrdtCz6zRy189W0uequf/nj3Rb6ypsb/Bj5k14yLzXBU1kDwedDqk+Dw75uwSh7t2FVLAnrda3/G8Ky6thGd2n/7AwM761FGz8QjE08...	2024-10-08T07:53:37.27580
97.107.133.136  ipinfo.io/ip/97.107.133.136  United States, Cedar Knolls 	SSH-2, 8-OpenSSH_7.6p1_Ubuntu-4ubuntu8.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAQDuVrJse3kaJZkg3Kj7V6Jzy6H8ancdI3Q0/KT96WlJsup17fx/XD06BvSAvgJvcMvTE+KVVUESuWAZvJM0R680X/ZUtbVoh1Q1N7NunctkyG+eugzYDfp0UhlC71a1fQ3Mj7M0up0FtskIht187vtpPgJdPDcct0UJAjevdXR6Z0BXW0ag5+AtQ+qq3021nEzrkfFKG...	2024-10-08T07:53:35.585771
103.139.175.30  ipinfo.io/ip/103.139.175.30  Indonesia, Jakarta	SSH-2, 8-OpenSSH_7.6p1_Ubuntu-4ubuntu8.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAQDQ5D91ntfTj8Bhmh7TV6DpcNuYU/CdGjHmH100EECIgysHnsSP0wakSL9kQEX8u0b6SgSazAG1lyA8tbo453pR4ch064TF+4tFvG9ekxJHgC+Sp/GJLT9kcp0lag40jjszVypjtnq8IsD1XNMP0wXUqfIn3mD0kC1suwNpFj7TDgPy3f4jy7C13xdE8gsG6F...	2024-10-08T07:53:35.111220
54.36.182.218  ipinfo.io/ip/54.36.182.218  France, Lille	SSH-2, 8-OpenSSH_7.2p2_Ubuntu-4ubuntu2.8 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAQDDIDApC1R/x85FKzsupIrjZw00Q05t21MA+TB5K1z2N6B7z3G2wmiL20WPKs00W0AutC8hJPKgk2wZKXC1LLMP5CnwW7Q29R0Uy+4X1LMj56M5151qz4...	2024-10-08T07:53:34.201552



Tracking de serveurs C2

Certains filtres ont été mis en place pour chercher des serveurs de commande et contrôle (C2) :

- <https://github.com/BushidoUK/OSINT-SearchOperators/blob/main/ShodanAdversaryInfa.md>

Serveurs C2	Filtres
-------------	---------

Metasploit	http.favicon.hash:-12788697 ssl:MetasploitSelfSignedCA http.html:"msf4"
Cobalt Strike	ssl.jarm:07d14d16d21d21d07c42d41d00041d24a458a375 eef0c576d23a7bab9a9fb1 port:443 ssl.cert.serial:146473198 product:"Cobalt Strike Beacon" http.html:"cs4.4"
Brute Ratel	http.html_hash:-1957161625 product:"Brute Ratel C4"

Vous pouvez aussi retrouver des **JARM** de C2 qui sont des empreintes des certificats par défaut :

- <https://github.com/BushidoUK/OSINT-SearchOperators/blob/main/ShodanAdversaryInfra.md>

API

Pour utiliser l'API, il vous faut payer (une version premium à 69\$ payable en une seule fois vous autorise à 100 queries par mois).

Une fois votre clé API récupérée, vous pouvez initialiser shodan :

```
shodan init <API_KEY>
```

Pour faire une recherche :

```
shodan search "<QUERY>"
```

Pour trouver des informations sur une IP :

```
shodan host <IP>
```

Pour télécharger les résultats d'une recherche au format **JSON** :

```
shodan download <OUTPUT>.json "<QUERY>"
```

Pour consulter les résultats :

```
shodan parse <OUTPUT>.json
```

Ou alors :

```
cat <OUTPUT>.json | jq
```