

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 :

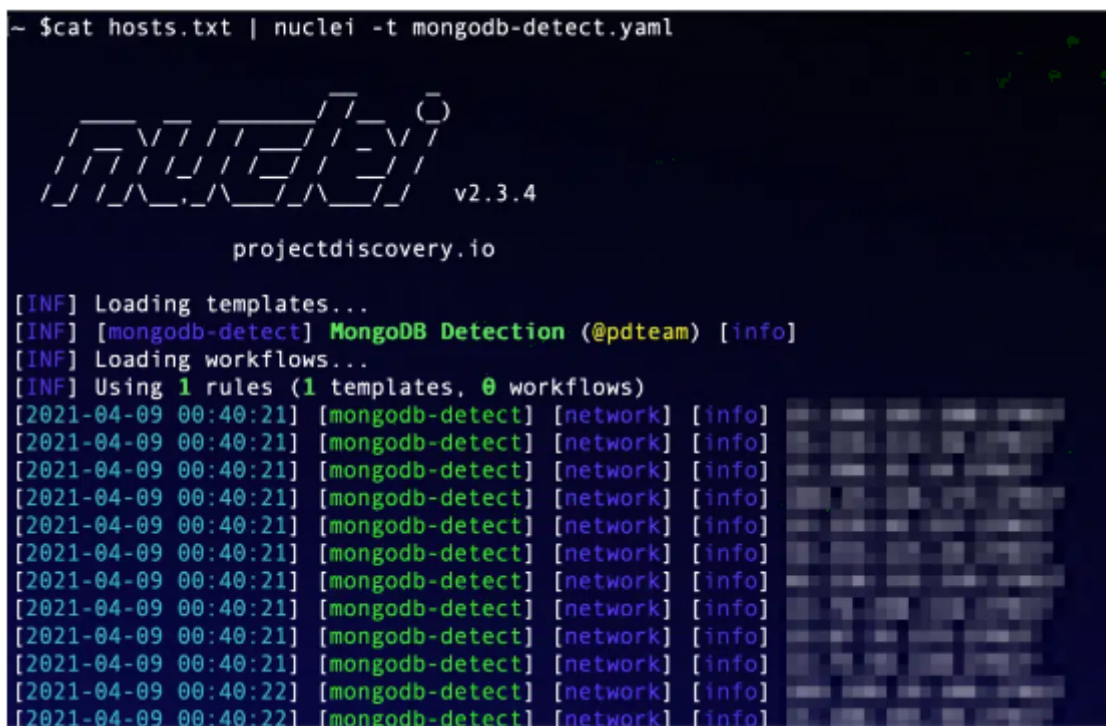
- <https://github.com/fastfire/deepdarkCTI>

[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
```



The screenshot shows a terminal window with the Nuclei logo (a stylized 'N' made of lines) and the version 'v2.3.4'. Below the logo is the text 'projectdiscovery.io'. The terminal output shows the following log messages:

```
[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** :

SHODAN

Explore

Downloads

Pricing

os.ubuntu

Q

Account

TOTAL RESULTS

5,358,841

TOP COUNTRIES

United States	1,501,713
Germany	713,319
China	366,410
Singapore	277,257
Japan	220,784
More...	

TOP PORTS

80	1,726,661
22	1,668,493
443	1,301,521
9100	118,124
2222	43,267
More...	

TOP ORGANIZATIONS

DigitalOcean, LLC	796,421
-------------------	---------

View Report

Download Results

Historical Trend

Browse Images

View on Map

Advanced Search

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

Facultad de Arquitectura y Ambiente Construido FARAC USACH | Inicio - Facultad de Arquitectura y Ambiente Construido FARAC USACH

158.170.66.48

www.arquitectura.usach.cl

arquitectura.usach.cl

SEIGIC USACH LTDA

Chile, Santiago

edit-product

SSL Certificate

Issued By:

Issued To:

Issued To:

Common Name:

Supported SSL Versions:

HTTP/1.1 200 OK

Server: nginx/1.18.0 (Ubuntu)

Date: Tue, 08 Oct 2024 07:15:54 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

X-Powered-By: PHP/8.0.5

Link: <https://arquitectura.usach.cl/wp-json/>; rel="https://api.w.org/"

Link: <https://arquit...

VegaSystems IT Consulting & Solutions Paderborn NRW: Under Construction

80.78.178.85

webredirect.vegasytems.de

www5.vegasytems.de

Vegasytems Core

Germany, Paderborn

edit-product

SSL Certificate

Issued By:

Issued To:

Issued To:

Common Name:

Supported SSL Versions:

HTTP/1.1 200 OK

Server: nginx/1.18.0 (Ubuntu)

Date: Tue, 08 Oct 2024 07:15:53 GMT

Content-Type: text/html

Content-Length: 1436

Last-Modified: Tue, 04 Apr 2017 11:58:46 GMT

Connection: keep-alive

ETag: "58e38a76-59c"

Accept-Ranges: bytes

147.52.205.213

University of Crete

Greece, Gazi

SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQBN7N1+55v+58vfwNub0u+7Dv7H/6B5Cvrr720wudf7

On voit les ports les plus exposés, les services les plus utilisés, les hébergeurs les plus utilisés pour ces machines etc :

SHODAN

Explore

Downloads

Pricing

os.ubuntu

Q

Account

Shodan Report

os.ubuntu

Total: 5,359,080

GENERAL

Countries

United States	1,501,713
Germany	713,319
China	366,410
Singapore	277,257
Japan	220,784

Ports

80	1,726,661
22	1,668,493
443	1,301,521
9100	118,124
2222	43,267

Organization

DigitalOcean, LLC	796,421
Amazon Technologies Inc.	278,124
Microsoft Online GmbH	208,089
Google LLC	158,536
Alipay Computing Co., Ltd	133,368

Vulnerabilities

CVE-2024-23897	2.1%
PHPAN	219
Logjam	183
CVE-2021-43798	181
Heartbleed	21

Products

nginx	3,488,769
OpenSSH	1,702,769
Proxmox/vee Node Exporter	120,874
Grafana Open Source	4,565
jenkins	4,507

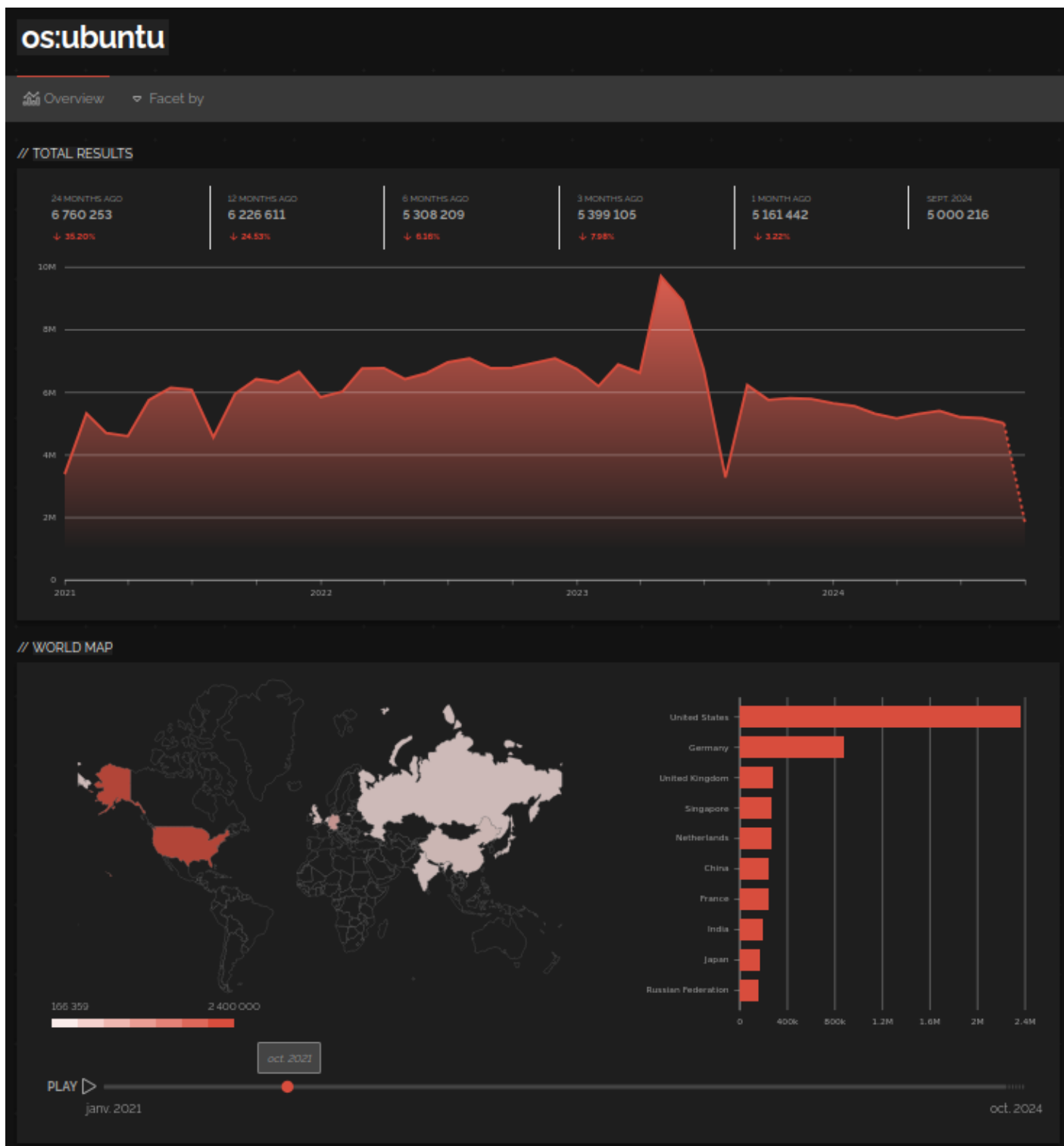
Tags

edit-product	3,488,769
cloud	2,367,062
self-signed	155,150
proxy	110,004
cdn	17,078

Operating Systems

Ubuntu	5,237,077
Ubuntu 20.04 & LTS (Focal Fossa) Lin...	6,054
Ubuntu 22.04 & LTS (Jammy Jellyfish) ...	4,198
Ubuntu 20.04 & LTS (Focal Fossa) Lin...	4,025
Ubuntu 22.04 & LTS (Jammy Jellyfish) ...	4,042

Vous pouvez aussi consulter les statistiques pour cette query dans le temps grâce à l'onglet **Historical Trends** :



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/ShodanAdversaryInfra.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/ShodanAdversaryInfa.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
```