

# 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](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 :

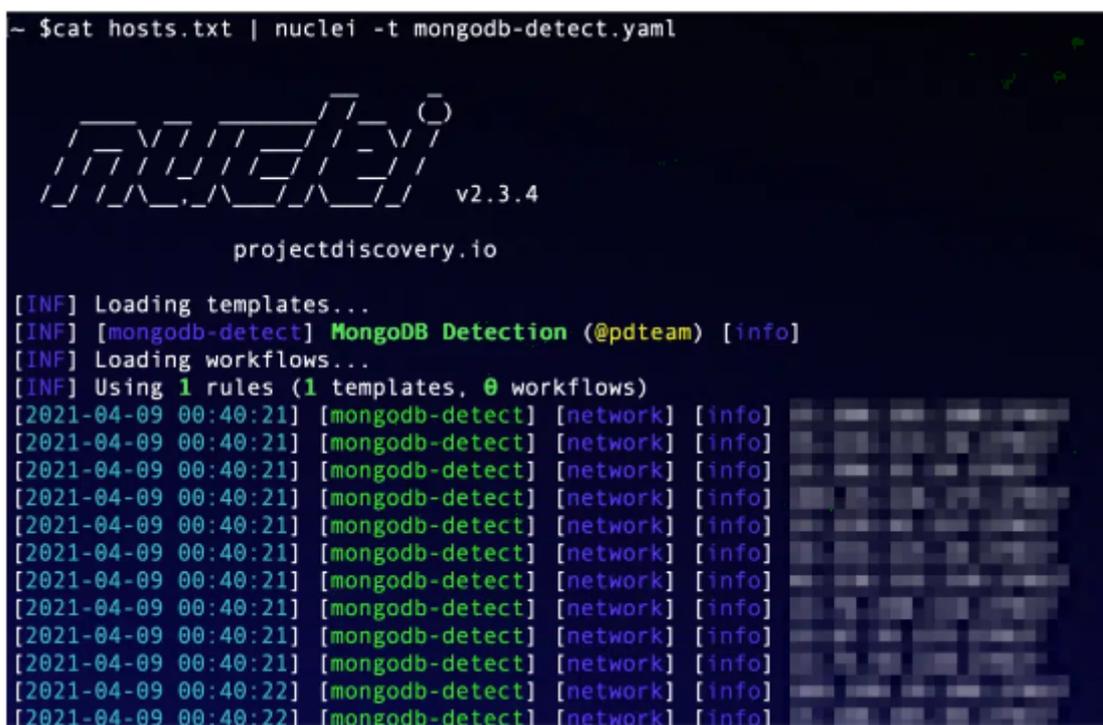
- <https://github.com/fastfire/deepdarkCTI>

# [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
v2.3.4

[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 00:40:22] [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"
```

matchers:

- type: regex

part: body

regex:

- '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]?)'

## Liste des cibles

Ici nous ciblerons des adresses IPs que nous indiquerons dans le fichier **ips.txt** :

```
192.168.5.40
```

En cas d'attaque web, il peut s'agir d'URL et non d'adresse IP.

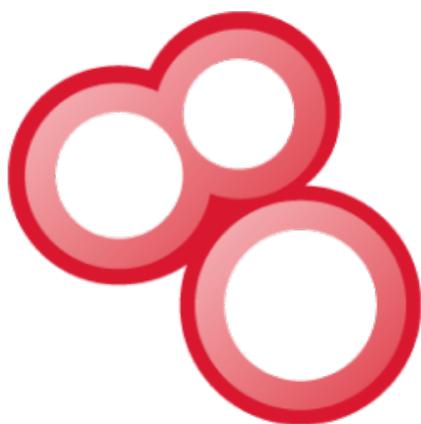
## Exécution d'un template

```
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

TOTAL RESULTS: 5,358,841

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** 2024-10-08T07:20:26.772586

138.170.66.49  
www.arquitectura.usach.cl  
arquitectura.usach.cl  
SEGIC USACH LTDA  
Chile, Santiago

**VegaSystems IT Consulting & Solutions Paderborn NRW: Under Construction** 2024-10-08T07:19:00.749630

147.52.205.213  
University of Crete  
Greece, Giálá

SSH-2, 0-OpenSSH\_7.6p1 Ubuntu-4ubuntu0.7  
Key Type: ssh-rsa  
f00c:44483022c11c2f2a1406a884a880071233v4581ef7a1e0881c720710885c972260d07f

TOP COUNTRIES

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

TOP PORTS

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

TOP ORGANIZATIONS

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

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

**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.	296,124
Mediatech Online GmbH	200,000
Google LLC	198,216
Allyum Computing Co. LTD	133,268

**Vulnerabilities**

CVE-2024-28897	2,195
PHPAN	299
Logjam	229
CVE-2021-43798	882
Heartbleed	21

**Products**

nginx	3,438,740
OpenSSH	1,762,769
Proxmox/Proxmox VE Exporter	100,974
Centreon/Opem Source	4,953
Jenkins	4,937

**Tags**

not-product	3,444,092
cloud	2,967,042
self-signed	39,530
proxy	30,004
cdn	27,978

**Operating Systems**

Ubuntu	5,237,677
Ubuntu 20.04.4 LTS [Focal Fossa] Lin...	6,064
Ubuntu 22.04.4 LTS [Jammy Jellyfish] ...	4,198
Ubuntu 20.04.4 LTS [Focal Fossa] Lin...	4,105
Ubuntu 22.04.4 LTS [Jammy Jellyfish] ...	4,042

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

TOTAL RESULTS

5,359,574

TOP COUNTRIES



TOP PORTS

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

TOP ORGANIZATIONS

Organization	Count
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

9ym@shodan.net  
Voicemix Inc.  
United States, Orem

SSH-2, 0-OpenSSH\_7.6p1\_Ubuntu-4ubuntu8.5  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAADAQABAAQDAQDZBYW7ZJ+oD6JUSY1+9EUWt6gTf/ZawJjbra5pTzup90  
oyIFpGt5Q5oeA9RfPqkqru2N3DRvGhIqjIrn1NkT6GslzYfRrtCzbozRy189Mwueqf/nJ3Bb  
6y5pb/8J5k14yLzXBUkDwedDqk+Dw75uSh7tZfVLAnrda3/G8KyEtH6dZr/7Am9761FGz8Qj  
E08 ...

2024-10-08T07:53:37:372580

97,107,133.136

l63-136.members.linode.com  
Linode  
United States, Cedar Knolls

SSH-2, 0-OpenSSH\_7.6p1\_Ubuntu-4ubuntu8.7  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAADAQABAAQDAuYvJm3kaJZkg3k7JVCJzyGHRamsdI2Q0/KT96W0ljrup  
17ft/X0D6BrSAvgJvcMvTEqVUE5UwAZvJM0R680X/ZUttVoh1Q1N7MnctkyGueuzYDFp0hJ  
C71a1fQ3WU7MUpUftmkTh187vtPqJdPDcct0UJA1evdXR6Z08W0ag5+AtQ+qq3021nEzrkf  
fk6 ...

2024-10-08T07:53:35:585771

103,139,175.30

CV Mitra Teknologi Indonesia  
CV Mitra Teknologi  
Indonesia, Jakarta

SSH-2, 0-OpenSSH\_7.6p1\_Ubuntu-4ubuntu8.7  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAADAQABAAQDAQDZBYW7ZJ+oD6JUSY1+9EUWt6gTf/ZawJjbra5pTzup90  
oyIFpGt5Q5oeA9RfPqkqru2N3DRvGhIqjIrn1NkT6GslzYfRrtCzbozRy189Mwueqf/nJ3Bb  
6y5pb/8J5k14yLzXBUkDwedDqk+Dw75uSh7tZfVLAnrda3/G8KyEtH6dZr/7Am9761FGz8Qj  
E08 ...

2024-10-08T07:53:35:111220

54,36,182,218

218.jp-54-36-182.eu  
OVH SAS  
France, Lille

SSH-2, 0-OpenSSH\_7.2p2\_Ubuntu-4ubuntu2.8  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAADAQABAAQDAQDZBYW7ZJ+oD6JUSY1+9EUWt6gTf/ZawJjbra5pTzup90  
oyIFpGt5Q5oeA9RfPqkqru2N3DRvGhIqjIrn1NkT6GslzYfRrtCzbozRy189Mwueqf/nJ3Bb  
6y5pb/8J5k14yLzXBUkDwedDqk+Dw75uSh7tZfVLAnrda3/G8KyEtH6dZr/7Am9761FGz8Qj  
E08 ...

2024-10-08T07:53:34:201552

// TOTAL RESULTS



// WORLD MAP



## 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
```