

[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

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
-------------------	---------

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
SEGIC USACH LTDA
Chile, Santiago

VegaSystems IT Consulting & Solutions Paderborn NRW: Under Construction

80.10.176.85
webredirect.vegasytems.de
www6.vegasytems.de
Vegasytems Core
Germany, Paderborn

147,52,205,213
University of Guelph
Greece, Glatzi

SSH-2, 0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
Key: Type: 259-1534
Key: AAAAB3QACI1wZFAAMADAN8AAB8B0D71153YV15BtF7uNodH1rD72H/885Svrr72m0d17

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.	298,134
Microsoft Online Services	208,209
Google LLC	184,536
Allyson Computing Co. LTD	133,256

Vulnerabilities

CVE-2024-23897	2,135
PHPAN	219
Logjam	213
CVE-2021-42988	186
Heartbleed	21

Products

nginx	3,488,740
OpenSSH	1,762,769
Proxmox/ve Node Exporter	120,974
Centreon/Opium Sourcecode	4,953
Ansible	4,937

Tags

web-product	3,644,092
cloud	2,567,042
self-signed	39,530
proxy	31,034
cdn	17,978

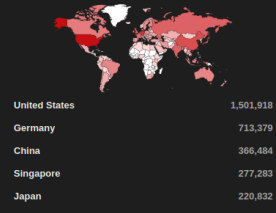
Operating Systems

Ubuntu	5,227,077
Ubuntu 20.04.8 LTS (Focal Fossa) Lin...	5,054
Ubuntu 22.04.4 LTS (Jammy Jellyfish) ...	4,198
Ubuntu 20.04.8 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

os:ubuntu.net
Voicemix Inc.
United States, Orem

SSH-2.0-OpenSSH_7.6p1_Ubuntu-4ubuntu8.5
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQDAQDZBYW7ZJ+oD6JUSY1+9EUWt6gTf/ZawJjbr5pTzup90
oyIFpGt5Q5oeA9RfPqkqru2N3DRvGhIqjIrn1NkT6GslzYfRrtCzbozRy189Mwueqf/nJ3Rb
6y5pb/8J5k14yLzXBUkDwedDqk+Dw75uSh7tZfVLAnrda3/G8KyEtH6dZr/7Am9761FGz8Qj
E08...

2024-10-08T07:53:37.372580

97,107,133.136

653-136.members.linode.com
Linode
United States, Cedar Knolls

SSH-2.0-OpenSSH_7.6p1_Ubuntu-4ubuntu8.7
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQDAuYvJm3kaJZkg3k7VtGzjyG8hamsdI2Q0/KT96W0ljrup
17ft/XD06BrSAvgJvcMvTEqVUE5UwAzvJM0R680X/ZUttVoh1Q1N7MnctkyGueuzYDFp0hJ
C71a1fQ3WU7MUp0FtmkTh187vtPqJdPDCct0UJA1evdXR6Z08W0ag5+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/ZawJjbr5pTzup90
oyIFpGt5Q5oeA9RfPqkqru2N3DRvGhIqjIrn1NkT6GslzYfRrtCzbozRy189Mwueqf/nJ3Rb
6y5pb/8J5k14yLzXBUkDwedDqk+Dw75uSh7tZfVLAnrda3/G8KyEtH6dZr/7Am9761FGz8Qj
E08...

2024-10-08T07:53:35.111220

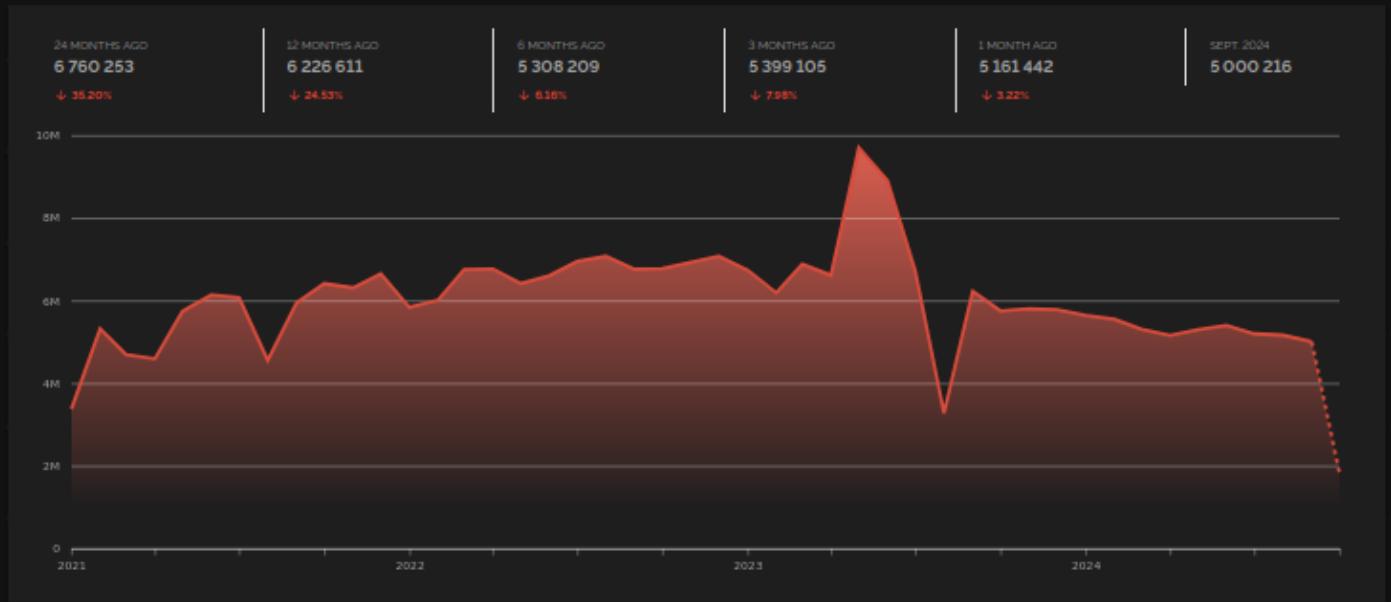
54,36,182,218

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

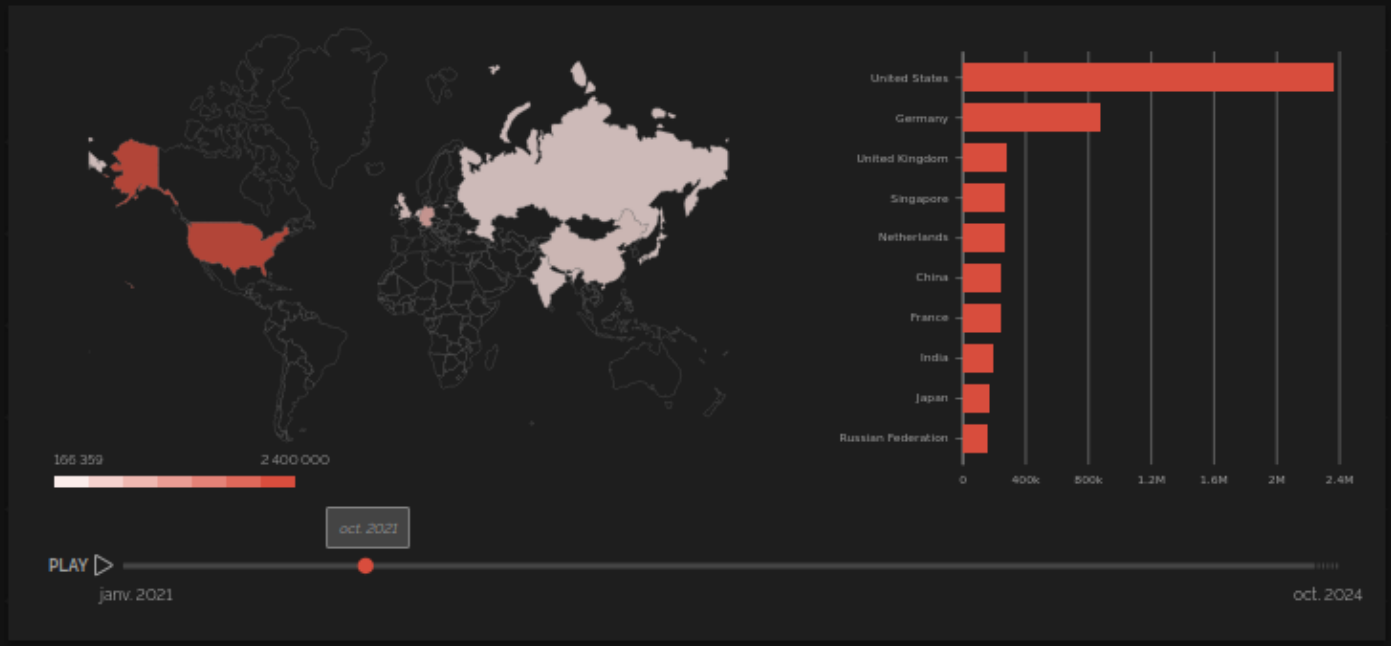
SSH-2.0-OpenSSH_7.2p2_Ubuntu-4ubuntu2.8
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQDAQDZBYW7ZJ+oD6JUSY1+9EUWt6gTf/ZawJjbr5pTzup90
oyIFpGt5Q5oeA9RfPqkqru2N3DRvGhIqjIrn1NkT6GslzYfRrtCzbozRy189Mwueqf/nJ3Rb
6y5pb/8J5k14yLzXBUkDwedDqk+Dw75uSh7tZfVLAnrda3/G8KyEtH6dZr/7Am9761FGz8Qj
E08...

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
```

Revision #5

Created 8 October 2024 06:54:43 by Elieroc

Updated 8 October 2024 07:56:08 by Elieroc