

# [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 States1,501,713

Germany713,319

China366,410

Singapore277,257

Japan220,784

More...

TOP PORTS

801,726,661

221,668,493

4431,301,521

9100118,124

222243,267

More...

TOP ORGANIZATIONS

DigitalOcean, LLC796,421

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

arquitectura.usach.cl

SEGIC USACH LTDA

Chile, Santiago

end-product

SSL Certificate

Issued By: R11

Common Name: arquitectura.usach.cl

Organization: Let's Encrypt

Issued To: arquitectura.usach.cl

Supported SSL Versions: TLSv1.2, TLSv1.3

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

80.170.176.85

webdirect.vegasytems.de

www.vegasytems.de

Vegasytems Core

Germany, Paderborn

end-product

SSL Certificate

Issued By: es

Common Name: es

Organization: Let's Encrypt

Issued To: webdirect.vegasytems.de

Supported SSL Versions: TLSv1.2, TLSv1.3

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: "58e3a7e-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: AAAAB3NzaC1yc2EAAAADAQABAAQDAI153y15btfmNoBwC1Dn7Hh8BS5wrr7ZmVd0f7

On voir 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

World map showing distribution of results by country.

Countries

United States1,501,713

Germany713,319

China366,410

Singapore277,257

Japan220,784

Ports

801,726,661

221,668,493

4431,301,521

9100118,124

222243,267

MORE...

Organization

DigitalOcean, LLC796,421

Amazon Technologies Inc.219,124

Netflix Online GmbH208,209

Google LLC184,526

Alipay Computing Co., Ltd123,266

MORE...

Vulnerabilities

CVE-2024-238972,176

PHPAN209

Log4j2123

CVE-2021-4398886

Heartbleed21

MORE...

Products

nginx3,438,740

OpenSSH1,762,769

Proxmox/ve Node Exporter120,974

Grafana/lorenz/Securecat4,503

Jenkins4,507

MORE...

Tags

end-product3,444,992

cloud2,367,062

self-signed39,530

proxy10,094

cdm17,078

MORE...

Operating Systems

Ubuntu5,227,077

Ubuntu 20.04.6 LTS (Focal Fossa) Lin...6,054

Ubuntu 22.04.4 LTS Jammy Jellyfish ...4,198

Ubuntu 20.04.6 LTS (Focal Fossa) Lin...4,325

Ubuntu 22.04.4 LTS Jammy Jellyfish ...4,042

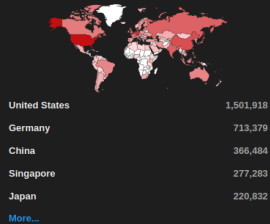
MORE...

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










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

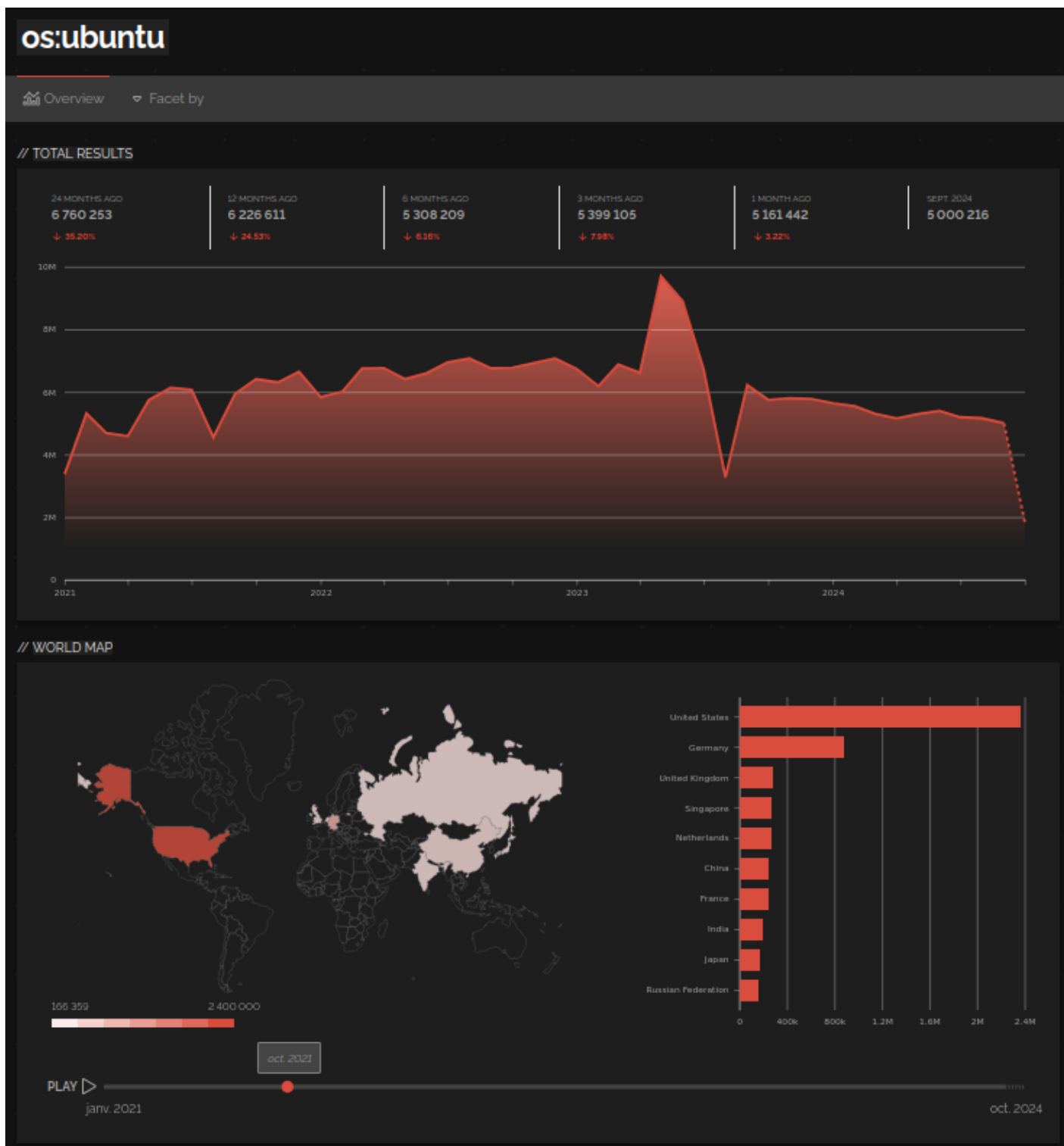
TOP ORGANIZATIONS

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](#)

<b>69.167.49.68</b>  <a href="#">ipinfo.io/ip/69.167.49.68</a>  United States, Orem	SSH-2, 8-OpenSSH_7.6p1_Ubuntu-4ubuntu8.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAQDZBYW7ZJ+oD6JUSY1+9EU0Ht6gTn/ZawJjbra5pTsup98oyIFhgT5Q5oe9RFPqkgtrub2N3DRvGh.lqjIrn1NKTG6slzYFARdtCz6zRy189W0uequf/nj3Rb6ypsb/Bj5k14yLzXBU1kDwedDqk+Dw75uwSh7t2FVLAnrda3/G8Ky6thGd2n/7AwM761FGz8QjE08...	2024-10-08T07:53:37.27580
<b>97.107.133.136</b>  <a href="#">ipinfo.io/ip/97.107.133.136</a>  United States, Cedar Knolls 	SSH-2, 8-OpenSSH_7.6p1_Ubuntu-4ubuntu8.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAQDu/vJse3kaJZkg3Kj7VGIzy6H8ancdI3Q0/KT96WlJsup17fx/XD06BvSAvgJvcMvTE+KVVUESuWAZvJM0R680X/ZUtbVoh1Q1N7NunctkyG+eugzYDfp0UhlC71a1fQ3Mj7M0up0FtskIht187vtpPgJdPDcct0UJA1evdXR6Z0BXW0ag5+AtQ+qq3021nEzrkfFKG...	2024-10-08T07:53:35.585771
<b>103.139.175.30</b>  <a href="#">ipinfo.io/ip/103.139.175.30</a>  Indonesia, Jakarta	SSH-2, 8-OpenSSH_7.6p1_Ubuntu-4ubuntu8.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAQDQ5D91ntfTj8Bhmh7TVGdpCnUyU/cdGjHmH100EECIgysHnsSP0wakL9LHQcX8u0b6SgSazAG1lyA8tbo453pR4cHt064TF+4tFvG9ekxJHgC+Sp/GJLT9kcp0lag40jjs2Vypjtnq8IsD1XNMP0wXUqfIn3mD0KCIswNpPj7TDgPy3f4jy7C13xd8gsG6F...	2024-10-08T07:53:35.111220
<b>54.36.182.218</b>  <a href="#">ipinfo.io/ip/54.36.182.218</a>  France, Lille	SSH-2, 8-OpenSSH_7.2p2_Ubuntu-4ubuntu2.8 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAQDDIDApC1R/x85FKzsupIrjZw00Q05t21MA+TB5K1z2N6B7z3G2wmiL20WPKs00W0AutC8hJPKgK2wZKXC1LLMP5CnwW7Q29R0Uy+X1L1Mj56M5151qz4...	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/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