Shodan: The Search Engine for Connected Devices

Every public IP. Every open port. Every banner. What's exposed about you — and the entire internet.

All	24/7	Free	Banners
PUBLIC IPV4 / IPV6	CONTINUOUS SCANNING	TIER AVAILABLE	+ TECH FINGERPRINTS

What Shodan indexes

CORE

Open ports + services

Every responding port. Service banners. Software versions.

TLS certificates

Cert details. Helps find hostnames + related infrastructure.

HTTP titles + bodies

Page titles, headers, response codes, HTML samples.

Tech fingerprints

Framework, CMS, web server, DB version inferred from banners.

Useful search filters

`org:"Your Company Inc"` — everything attributed to your org

`net:198.51.100.0/24` — IP CIDR range

`hostname:example.com` — by reverse-DNS

`port:5432 country:US` — open Postgres in the US (don't!)

`product:"nginx"` — by software

`http.favicon.hash:-123456789` — find every host with same favicon

`vuln:CVE-2024-XXXX` — vulnerable hosts (paid tier)

DEFENDER USE

Self-search your org weekly. Find shadow IT before attackers do. The favicon-hash trick reveals corporate apps exposed on unexpected IPs.

LEGAL FLOOR

Searching Shodan = legal. Accessing systems you find = not legal without authorization. Shodan tells you what exists; it does not authorize you to use it.

DEFENSIVE RECIPES

1. **Inventory open ports**
   Every IP block you own
2. **CVE match by banner**
   Detect outdated software at the edge
3. **Cert transparency cross-ref**
   Find subdomains via crt.sh + Shodan
4. **Favicon-hash pivot**
   Locate corporate apps on rogue IPs
5. **Alert on changes**
   Shodan Monitor

PLANS

1. **Free**
   Limited searches, basic filters
2. **Membership ($69 once)**
   Most useful tier for one-time learners
3. **Small Business +**
   Continuous monitoring + vuln data

Full guide: **djenterprises.ai/blog/osint-shodan**