IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

GET YOUR S.O.S. How-to Guide
(STUFF OFF SEARCH*)

DEFEND TODAY, SECURE TOMORROW

As today's world has become more connected, many industrial control system (ICS) devices can now access the Internet and be found using full spectrum search engines. Many device owners intentionally enable remote access to their ICS devices for increased asset or system attribute visibility. But some owners may not realize that their devices are partially or fully exposed and can be found on the public internet. They are also unaware that this exposure can increase their attack surface, or the potential number of ways a cyber attacker can breach a device or network.

Fortunately, there are several tools to help owners identify internet-accessible devices – Internet of Things (IoT)/Industrial Internet of Things (IIoT).– and protect their assets from potential harm.

Here are some common, publicly-available tools* to help you Protect Your Assets and get your Stuff Off Search (S.O.S.):

Shodan	Censys	Thingful
Shodan is a web-based search platform for internet connected devices. Key features: • Identify Internet connected devices, Internet of Things/Industrial Internet of Things (IoT/IIoT), and industrial control systems (ICS). • Potential exploits. • Default passwords. • Integrations with vulnerability tools, logging aggregators and ticketing systems allow Shodan to be seamlessly integrated into an enterprise. https://www.shodan.io	Censys is a web-based risk management tool that helps identify publicly accessible assets —even if they can't be scanned by a vulnerability management tool. Key features: • Home network risk identifier (HNRI), allowing employers to anonymously monitor staff's home network infrastructure for vulnerabilities that may pose a risk to the company. • Exposed routers. • Default credentials. • Popular vectors for ransomware. https://www.censys.io	Thingful is a search engine for the Internet of Things (IoT). Key features: • Searchable index of public and private connected objects and sensors around the world. • Monitors IoT networks and infrastructures including energy, radiation, weather, and air quality devices. • Reports seismographs, iBeacons, vehicles, ships, aircraft and animal trackers. The tool assists with response by enabling end users to create watchlists and publications on public/private IoT resources. https://www.thingful.net

*Shodan, Censys, Thingful, and other full spectrum search engines. The United States Government does not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by the United States Government. The list of providers above is not intended to be exclusive.

POTENTIAL USE CASES TO CONSIDER

A key capability of these tools is identifying exposed assets to enable owners and operators of Industrial Control Systems (ICS), IoT, and IIoT devices to reduce their attack surface by enumerating and detailing any number of Internet-connected targets. By pulling back banners of Internet connected devices, end users can use any combination of search filters to narrow search results to specifically query for potentially vulnerable devices. Below are some common use case searches for reducing attack surface.

ASSESS PUBLIC ASSET RISK PROFILE

Each finding represents a distinct system, and each system may have many entries for services running on different ports. For each system, service, and port that is exposed, ask the following questions:

- Why does this system and service need to be running? Equipment often enables capabilities by default that are not necessary in normal operations.
- What is the business need requiring this system, service, and port to be exposed to the Internet? Administrative tools may be inadvertently configured to connect on an Internet-accessible interface.
- Can this system, service, or port reside behind a VPN? VPNs add strong authentication mechanisms and remove a direct link to potential adversaries.
- Can the service offer strong, multi-factor authentication? Contact your vendor to explore options.
- When was the last time this system or service was fully updated? There may be a valid business justification for why a system was not updated; otherwise, follow your change management process and update your systems on schedule.
- When was the last time this system or service was hardened? Contact your vendor for best practices and support.

FOR FURTHER INFORMATION

How-to Guide: Stuff Off Censys
How-to Guide: Stuff Off Shodan
How-to Guide: Stuff Off Thingful