Shodan QuickStart Guide for ICS/OT

shodan.io

What is SHODAN?

Shodan is a publicly available search engine which scans the entire Internet for a limited number of services, does its best to determine what those services are, indexes that data and makes it searchable.

You can find it at shodan.io.

IP Addresses & Ports

Single IP Address – Searching for single IP
Example: **133.232.95.171**

Subnet – Search across an IP subnet range
Example: **net:133.232.95.0/24**

Port – Find instances of active services on a port
Example: **port:502**

Service by Name – Search for instances of specific services with text string detected
Example: **modbus**

Service by Name on a Specific Port
Example: **modbus port:502**

Service by Name Not on a Specific Port
Example: **modbus -port:502**

Hostname – Search for string in hostname
Example: **hostname:"siemens.com"**

Autonomous System Number (ASN)
Example: **ASN:AS4782**

Physical Location

Country – Search by country code
Example: **country:US**

City – Search by city name
Example: **city:Chicago**

Region – Search by region name (outside US)
Example **region:IDF**

State – Search by state code abbreviation (in US)
Example: **state:IL**

Zip Code – Search by postal ZIP code
Example: **postal:60601**

Geo – Search by GPS coordinates
Example: **geo:41.85003,-87.65005**

Geo by Range – GPS search within Range by Km
Example: **geo:41.85003,-87.65005,2**

ICS/OT Search Terms - General

Search for general terms and similar:

- SCADA
- ICS
- IIoT
- OT

ICS/OT Search Terms – Manufacturers

Search for manufacturers and similar:

- Siemens
- Omron
- Bosch
- Schneider / Schneider Electric
- Rockwell / Rockwell Automation
- Mitsubishi / Mitsubishi Electric

ICS/OT Search Terms – Device Types

Search for device types and similar:

- PLC
- HMI
- DCS
- Controller
- Field I/O
- Serial Converter

ICS/OT Search Terms – PLC Brands

Search for device types and similar:

- Modicon (by Schneider Electric)
- Allen Bradley (by Rockwell Automation)
- Simatic (from Siemens)
- Sysmac (from Omron)
- Rexroth (from Bosch)

ICS/OT Search Terms – Model Types

Search by model type and similar:

- S7-300
- 1766-L32BWA
- V570-57-T20

Shodan Images Features

Shodan offers a feature where it records screen shots for certain services that can be reviewed to find systems of interest including PLCs and HMIs.

images.shodan.io

For Premium Account Access

There are a number of useful operators that require premium accounts (Enterprise, Academic, etc)

Tag – Search based on Shodan tagged assets
Example: **tag:ics** or **tag:database**

Special thanks to John Matherly and the Shodan team!

linkedin.com/in/mikeholcomb