BASIC SCADA SHODAN DORK

1.SCADA system product: XYZ SCADA
2.SCADA system by port: port:502 XYZ
3.SCADA system by protocol: XYZ Modbus
4.SCADA system by specific keyword: XYZ HMI
5.SCADA system with a specific OS: XYZ "Windows XP"
6.SCADA system with a specific manufacturer: XYZ "Siemens PLC"
7.SCADA system with a specific software: XYZ "Wonderware"
8.SCADA system with a specific device type: XYZ "RTU"
9.SCADA system with a specific service: XYZ "DNP3"
10.SCADA system with a specific city: XYZ city:"New York"
11.SCADA system with a specific country: XYZ country:"US"
12.SCADA system using a specific product version: XYZ "FactoryTalk View SE"
13.SCADA system with a specific IP range: net:192.168.1.0/24 XYZ
14.SCADA system with a specific hostname: hostname:scada.XYZ.com
15.SCADA system with default credentials: XYZ "default password"
16.SCADA system with known vulnerabilities: XYZ vuln:CVE-2020-12345
17.SCADA system with a specific organization: org:"XYZ"
18.SCADA system with a specific ICS protocol: XYZ "IEC 61850"
19.SCADA system with a specific web server: XYZ "Apache"
20.SCADA system with a specific hardware: XYZ "Schneider Electric"
21.SCADA system with exposed VNC: XYZ port:5900
22.SCADA system with exposed RDP: XYZ port:3389
23.SCADA system with exposed OPC UA: XYZ port:4840
24.SCADA system with exposed Profinet: XYZ port:34962
25.SCADA system with exposed EtherNet/IP: XYZ port:44818

https://www.scadaexposure.com/library/scada-googledorks-121227101926-phpapp01.pdf
https://www.hackers-arise.com/post/2016/06/30/hacking-scada-finding-scada-systems-using-shodan
https://www.linkedin.com/pulse/how-search-icsscada-systems-using-shodan-muhammad-mesbah/

https://www.linkedin.com/in/joas-antonio-dos-santos