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

How-to Guide:
Stuff Off Censys.io

DEFEND TODAY,
SECURE TOMORROW

As people and organizations have become more reliant on the Internet, visibility of many different types of assets on the public Internet has become more common. But the interconnectedness and data sharing that mark today's world also increase the chances a system or device can face a cyberattack – and many times, organizations are unaware of this increased exposure. The ability to query for Internet-connected assets is vital to managing attack surface, and Censys.io can support those efforts.

WHAT IS CENSYS.IO[1]

Censys.io (www.censys.io) is a web-based search platform for assessing attack surface for Internet connected devices. The tool can be used not only to identify Internet connected assets and Internet of Things/Industrial Internet of Things (IoT/IIoT), but Internet-connected industrial control systems and platforms. Leveraging ingestion formats supported by WebUI, API, Raw Data, Google BigQuery, Censys.io provides maximum extensibility into any size cyber security ecosystem. Integrations with leading vulnerability tools and platforms, logging aggregators and other scanning systems allow Censys.io to be seamlessly integrated into an enterprise.

POTENTIAL USE CASES FOR CENSYS.IO

A key capability of Censys.io is its use as an attack surface reduction tool, with the ability to recognize any number of Internet connected targets, including ICS and IIoT. With the ability to assess and index IP addresses, parse TLS certificates, and track domains, Censys.io provides a 360-degree depiction of an organization's Internet attack surface. Censys.io has also been positioned as a platform capable of providing visibility into an organization's Internet remote workforce.

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.

USEFUL CENSYS SEARCHES

Useful Censys Searches (Non-ICS Specific)
[[IPv4]] location.country_code: US and protocols: ("23/telnet" or "21/ftp" or “80/http”)
Identifies any host in the US, with telnet, ftp, or http Internet facing
[IPv4] location.country_code: CN and protocols: ("445/smb" or "3389/rdp")

[1] 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.

Identifies any host in China, with protocols smb or rdp Internet facing.
[IPv4] 22.0.0.0/8 or 12.12.12.0/24
Finds all hosts in the subnet ranges 22.0.0.0/8 and 12.12.12.0/24
[Websites] 80.http.get.headers.server: Apache and protocols: "80/http"
Finds all [Websites] running an Apache web server with protocol http Internet facing
[Websites] 80.http.get.headers.server: Microsoft and protocols: ("80/http" or "1433/mssql")
Finds all [Websites] running Microsoft IIS with protocols http or 1433 Internet Facing
Useful Censys Searches (ICS Specific)
[IPv4] location.country_code: US and tags: scada
Finds all hosts within the US with a banner tag of scada
[IPv4] location.city: Shanghai and tags: ("modbus" or "scada")
Finds all hosts within Shanghai with banner tags of modbus or scada
[IPv4] location.city Houston and protocols: ("502/modbus" or "20000/dnp3")
Finds all hosts in Houston with protocols modus or dnp3 Internet facing
[IPv4] ("Schneider Electric" or "Siemens")
Searches for all hosts with vendor product name of Schneider Electric or Siemens

MORE INFORMATION

Censys.io is an extremely powerful tool with searching capabilities that are extensive. There are several licensing options that are available depending on the type of usage required, as well as the specific use cases that need to be addressed. For more information about Censys.io or to get further searching guidance, visit https://www.censys.io.