



Community Defense Program

Enhancing Resilience to Cyber Threats Facing Small Utilities

Dawn Cappelli, Director OT-CERT
Gus Serino, OT-CERT/I&C Secure, Inc.

Risk to the Under Resourced

- Recent cyber attacks demonstrate the risk
 - Cyber Av3ngers impacted water utilities with Israel-made OT devices
 - 22 companies in Danish energy infrastructure compromised via free/low-cost firewalls used by small organizations
 - Colorado co-op impacted by ransomware
- Small water, electric, and gas utilities often lack the resources to instrument OT cyber security

Importance of Community



DRAGO

Safeguarding Civilization

The Most Effective OT Security Tech Platform

Visibility into OT assets, vulnerabilities, traffic, and threats to reduce OT risk.

A Community-Focused Mission

Skills, communications, & resources to strengthen the collective defense

Expert OT Intelligence & Service Resources

OT expert analysts, threat hunters, & responders to help you win the fight.

Dragos Community Defense Program (CDP)

Free OT cybersecurity software technology

Dragos Platform & other key resources such as Dragos Academy

For small water, electric, and natural gas providers

<\$100 million revenues

To help reduce risk of cyber events

- Inventory assets
- Detect & hunt threats
- Manage vulnerabilities
- Respond to incidents

Register at:

[Dragos.com/community-defense-program](https://dragos.com/community-defense-program)

Email us at:

CDPinfo@dragos.com

Dragos CDP: What's Included

Dragos Platform

- ICS/OT visibility & network monitoring (assets, threats, vulns)
- Includes Sensors and SiteStore, virtual models

Neighborhood Keeper

Anonymized community threat visibility amongst Platform users

Threat Hunting Services

CDP participant telemetry analyzed by OT expert threat hunters

OT-CERT Membership

Toolkits, guides, & members-only working sessions to improve cyber capability

Dragos Academy

On-demand training for OT security and Dragos Platform use

Software Updates & KnowledgePacks

Latest functionality, threat detections, & vulnerabilities

Dragos CDP: Application Process & Requirements

- Completion of the CDP application
 - [Dragos.com/community-defense-program](https://dragos.com/community-defense-program)
 - Dragos will review application to confirm eligibility and ability to deploy
- Confirmation of basic network infrastructure
 - Need to support SPAN or a tap (our technology is passive monitoring)
- Virtual infrastructure for Dragos Platform Sensors
 - Or ability to purchase hardware to meet the software specifications
 - Hardware purchase options will be available from Dragos in the future
- Completion of contracts detailing terms and conditions & authorization to deploy

Community: Dragos OT-CERT



OT-CERT
OPERATIONAL TECHNOLOGY
CYBER EMERGENCY READINESS TEAM

**1,600
members**

**60
countries**

OT-CERT is the Operational Technology – Cyber Emergency Readiness Team dedicated to addressing the OT resource gaps that exist in industrial infrastructure.

CDP & OT-CERT – A Community Working Together

1. Participants build the virtual infrastructure and install Dragos Platform
2. CDP-specific training program
 - Short training videos can be watched and referenced on-demand
 - OT-CERT series of interactive jump-start sessions
3. OT-CERT monthly working sessions to build a CDP community
4. OT-CERT resources help CDP participants to build a foundational OT cybersecurity program

A Call to Action: Protecting Small Utilities is ALL our jobs

Qualifying Organizations

Apply now. [Dragos.com/community-defense-program](https://dragos.com/community-defense-program) Or request more info cdpinfo@dragos.com

Organizations that don't qualify, and want to improve cyber security

Contact [info@dragos](mailto:info@dragos.com) to help chart your journey and join OT-CERT at [Dragos.com/ot-cert/registration](https://dragos.com/ot-cert/registration)

ISACs, other community & government organizations

Help get the word out. Send this link to qualifying organizations [Dragos.com/community-defense-program](https://dragos.com/community-defense-program)

The background of the image is a dark, semi-transparent view of an industrial plant or refinery. It features various structures like distillation columns, storage tanks, and piping. Overlaid on this is a network of glowing green lines and nodes, suggesting a digital or cybernetic theme. In the center, there is a black rectangular box with a thin green border. Inside this box, the text "OT-CERT Update" is written in a light green, sans-serif font.

OT-CERT Update

Cybersecurity Hardening

Checklist

ICS/OT Security Hardening Checklist		DRAGOS
Date	Revision #	Revision History
	1.0	August 2023 - Create initial draft
Process Owner:		
Author/Editor:		

1. Remove Nonessential Components
<ul style="list-style-type: none"><input type="checkbox"/> Audit system(s) to identify and remove any services, applications, protocols, drivers, and other nonessential components.<input type="checkbox"/> Disable nonessential components that cannot be removed.<input type="checkbox"/> Disable insecure communication protocols not required for business purposes.<input type="checkbox"/> Remove the following as applicable, where technically feasible.<ul style="list-style-type: none"><input type="checkbox"/> Email services<input type="checkbox"/> File sharing services<input type="checkbox"/> Network management tools<input type="checkbox"/> Printer sharing services<input type="checkbox"/> Disable debug mode.<input type="checkbox"/> Ensure all configuration settings are documented.

2. Restrict Remote Access
<ul style="list-style-type: none"><input type="checkbox"/> Engineering and OT teams must evaluate what systems are necessary to leverage remote access.<input type="checkbox"/> Remote access, including process control, should be limited as much as possible.<input type="checkbox"/> Remote access requirements should be determined, including IP address, communication types, and what processes can be monitored. All others should be disabled by default.<input type="checkbox"/> User-initiated access should require multi-factor authentication.<input type="checkbox"/> All remote access communication should be logged and monitored.<input type="checkbox"/> Document the remote access mechanism, required configuration, and use case.<input type="checkbox"/> Ensure remote access needs are periodically reviewed.

3. Change Default Passwords
<ul style="list-style-type: none"><input type="checkbox"/> Change all default passwords for devices and applications.<input type="checkbox"/> Passwords must meet organizational password requirements, where technically feasible.<input type="checkbox"/> Change local default root/administrator username and password per application.<input type="checkbox"/> Change local default root/administrator username and password on console/maintenance ports.<input type="checkbox"/> Devices that can't meet organizational password requirements must be configured to the maximum password strength.

4. Access Controls/Principle of Least Privilege
<ul style="list-style-type: none"><input type="checkbox"/> Devices must be configured with individual user's accounts, where technically feasible.



Remove Nonessential Components



Restrict Remote Access



Change Default Passwords



Least Privilege



Vulnerability Management... and more

ICS/OT Secure Remote Access

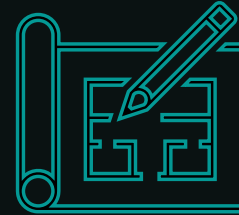
3 Part Series



- Part 1: Overview of Guiding Principals & Practices

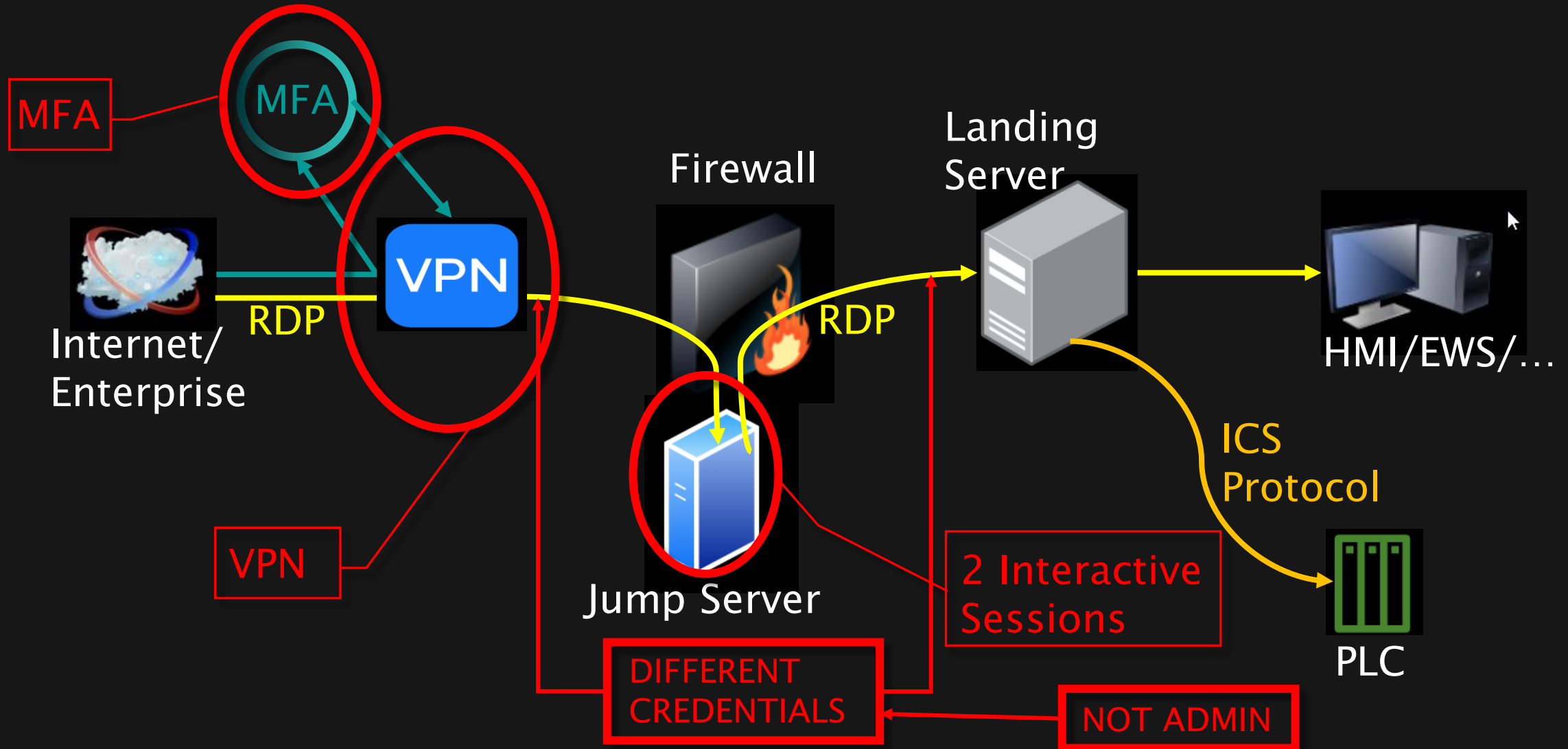


- Part 2: Video Discussion on Technical Aspects of VPN Configuration



- Part 3: Jump Server Configuration Details

Secure Remote Access - De Facto Standard



Secure Remote Access

Part 1: Getting Started Guide



Secure Existing Remote Access



Risk Based Approach



Guiding Principals of SRA



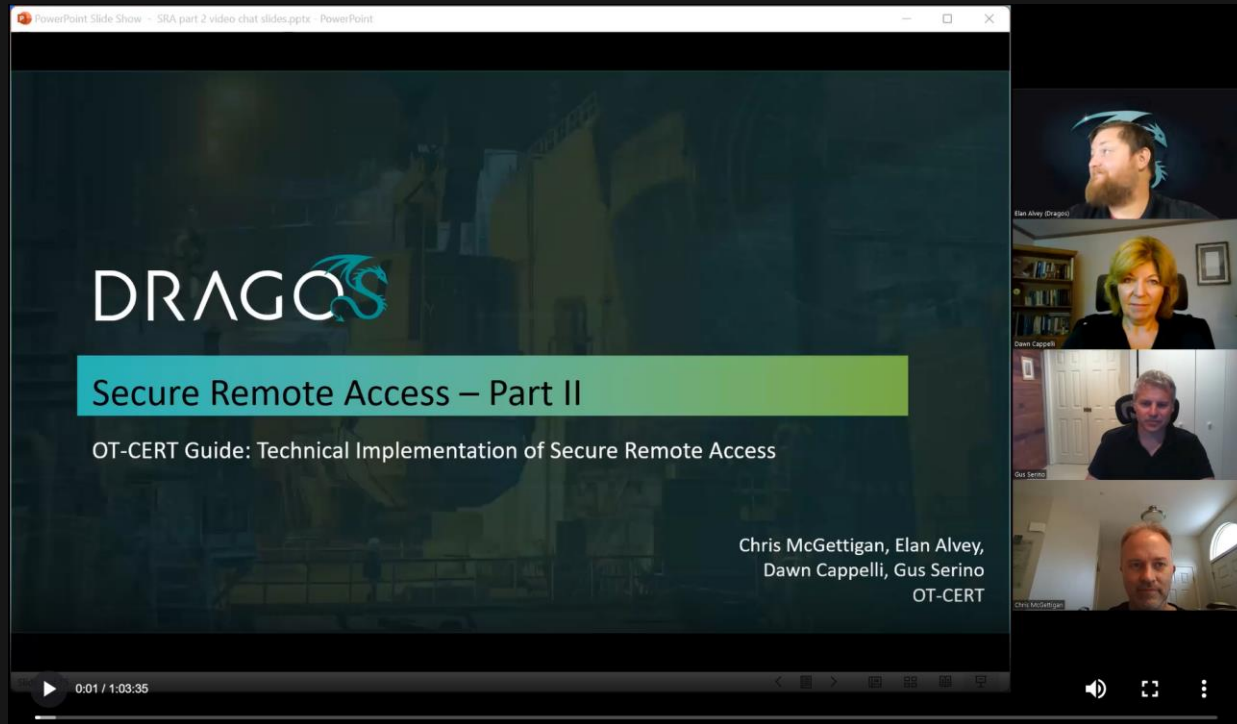
Detecting a Compromise



Procurement Language

Secure Remote Access

Part 2: VPN/Firewall Configuration



The screenshot shows a video player window. The main content is a presentation slide with the DRAGOS logo at the top. Below the logo, the text reads "Secure Remote Access – Part II" and "OT-CERT Guide: Technical Implementation of Secure Remote Access". At the bottom right of the slide, the names "Chris McGettigan, Elan Alvey, Dawn Cappelli, Gus Serino" and "OT-CERT" are listed. To the right of the slide is a video call interface with four participants: Elan Alvey (Dragon), Dawn Cappelli, Gus Serino, and Chris McGettigan. The video player controls at the bottom show a play button, a progress bar at 0:01 / 1:03:35, and volume and full-screen icons.



“Minimum” Security Baseline



VPN Configuration



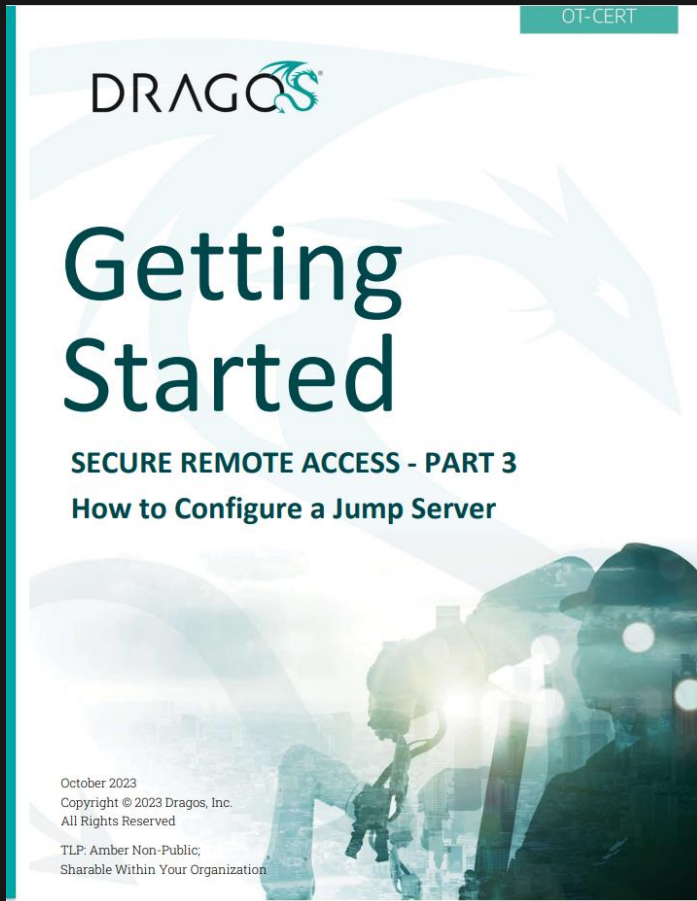
Firewall Rules



Maintenance

Secure Remote Access

Part 3: Jump Server Configuration



Jump Server Design



Cybersecurity Hardening



Detailed Technical Guidance

Windows Command Prompt

Ping 8.8.8.8

```
Command Prompt
Microsoft Windows [Version 10.0.22621.963]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ExampleUser>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=22ms TTL=55
Reply from 8.8.8.8: bytes=32 time=25ms TTL=55
Reply from 8.8.8.8: bytes=32 time=27ms TTL=55
Reply from 8.8.8.8: bytes=32 time=24ms TTL=55

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 27ms, Average = 24ms

C:\Users\ExampleUser>
```

Netstat -nao > Netstat_info.txt

```
Command Prompt - netstat -
TCP 127.0.0.1:9089 0.0.0.0:0 LISTENING 14280
TCP 127.0.0.1:28385 0.0.0.0:0 LISTENING 4
TCP 127.0.0.1:28390 0.0.0.0:0 LISTENING 4
TCP 127.0.0.1:63227 127.0.0.1:63228 ESTABLISHED 4472
TCP 127.0.0.1:63228 127.0.0.1:63227 ESTABLISHED 4472
TCP 172.16.0.36:139 0.0.0.0:0 LISTENING 4
TCP 172.16.0.36:49408 52.159.127.243:443 ESTABLISHED 4076
TCP 172.16.0.36:49742 40.74.108.123:443 ESTABLISHED 10180
TCP 172.16.0.36:50395 72.21.91.29:80 CLOSE_WAIT 7536
TCP 172.16.0.36:50399 13.107.246.36:443 CLOSE_WAIT 7536
TCP 172.16.0.36:63223 170.114.52.2:443 CLOSE_WAIT 9892
TCP 172.16.0.36:63224 170.114.52.2:443 CLOSE_WAIT 9892
TCP 172.16.0.36:63225 13.249.181.243:443 CLOSE_WAIT 9892
TCP 172.16.0.36:63230 13.249.181.243:443 CLOSE_WAIT 9892
TCP 172.16.0.36:63235 206.247.77.208:443 ESTABLISHED 4472
TCP 172.16.0.36:63336 204.79.197.200:443 TIME_WAIT 0
TCP 172.16.0.36:63337 204.79.197.200:443 TIME_WAIT 0
TCP 172.16.0.36:63338 13.59.123.141:443 ESTABLISHED 4472
TCP 172.16.0.36:63339 204.79.197.200:443 ESTABLISHED 11900
TCP 172.16.0.36:63340 20.140.147.200:443 ESTABLISHED 11900
TCP 172.16.0.36:63341 72.21.91.29:80 ESTABLISHED 11900
TCP 172.16.0.36:63342 13.107.3.254:443 ESTABLISHED 11900
TCP 172.16.0.36:63343 72.21.81.200:443 ESTABLISHED 11900
TCP 172.16.0.36:63344 172.64.142.36:80 ESTABLISHED 8884
TCP 172.16.0.36:63345 172.64.142.36:443 ESTABLISHED 8884
TCP 172.16.0.36:63346 204.79.197.222:443 ESTABLISHED 11900
TCP 172.16.0.36:63347 20.189.173.1:443 ESTABLISHED 12380
TCP 172.16.0.36:63348 52.113.196.254:443 ESTABLISHED 11900
TCP 172.16.0.36:63349 13.107.237.36:443 ESTABLISHED 11900
TCP 172.16.0.36:63350 13.107.18.254:443 ESTABLISHED 11900
```

Monitor External Exposure

Shodan Maps Images Monitor Developer More...

SHODAN Explore Pricing Search... Login

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

[SIGN UP NOW](#)

// EXPLORE THE PLATFORM

- Beyond the Web**
Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.
- Monitor Network Exposure**
Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.
- Internet Intelligence**
Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.

More than 3 million registered users across the world are using Shodan, including:

[Dragos.com/ot-cert](https://dragos.com/ot-cert)



Sign Up Today & Get Access

Register today for access to free resources to help you no matter where you are in your cybersecurity journey.

[REGISTER](#)



QUESTIONS AND ANSWERS

Contact us at ot-cert@dragos.com