DRAGOS

Small Utility, Big Target: Understanding and Defeating Cyber Threats

Dawn Cappelli
Director OT-CERT, Dragos Inc.
Former CISO, Rockwell Automation

My Background

Westinghouse
Software Engineer – nuclear power plants

Carnegie Mellon Software Engineering Institute CERT Program
Cybersecurity Research – insider threat / critical infrastructure protection

Rockwell Automation
Insider Risk Director -> Chief Information Security Officer

RETIRED!

Dragos
Director of OT-CERT

DRAGOS

Safeguarding Civilization

OT Security Technology Platform
Expertise integrated into software to reduce OT risk

A Community-Focused Mission
Building skills & communications to strengthen the collective defense

Expert OT Intelligence & Service Resources
OT expert analysts, threat hunters, & responders to help you win the fight.

8TH ANNUAL YEAR IN REVIEW

FROM THE 2025 OT/ICS CYBERSECURITY REPORT

Conflict-driven threat activity

Ukraine-Russia

Israel-Hamas

Israel / Iran / US

Mounting tension between China and Taiwan

- **Targeted operations** against **critical infrastructure**
- **Hacktivists** cause panic & negatively impact public perception of the resilience of critical services
- **Intelligence gathering & capability staging** activity

CURRENT THREAT LANDSCAPE

STATE-SPONSORED THREAT GROUPS

"HACKTIVIST" GROUPS

CYBERCRIMINALS

TWO NEW DRAGOS THREAT GROUPS

China

THREAT GROUP UPDATE: VOLTZITE

PERSISTENT ACCESS TO INDUSTRIAL ENTERPRISE NETWORKS

"[Chinese government-linked hackers have burrowed into U.S. critical infrastructure and are waiting] 'for just the right moment to deal a devastating blow.'"

"The CCP's dangerous actions—China's multi-pronged assault on our national and economic security—make it the defining threat of our generation."

- US FBI Director Christopher Wray

- Oil & Natural Gas
- Electric
- Telecom
- Water & Wastewater

Success Story: LELWD Beat Voltzite – Follow Their Lead!

LELWD vs VOLTZITE Case Study (Dragos Perspective)

1. Late 2023: U.S. water and electric utility implemented Dragos Platform and engaged Dragos industrial threat hunters

2. Dragos Platform and threat hunters discovered that early in 2023 VOLTZITE had compromised the utility and over the next **300+ days**:
   - exfiltrated details on operational processes, configurations of operational technology (OT) assets, geographic information system (GIS) data, SCADA system configurations, and lists of critical customers.
     - NOTE: Voltzite was not able to infiltrate the OT networks - historical or archival information stored on the file server was stolen
   - **VOLTZITE was focused on accessing and exfiltrating sensitive documents and data that are pivotal to critical operations of the electric utility.**

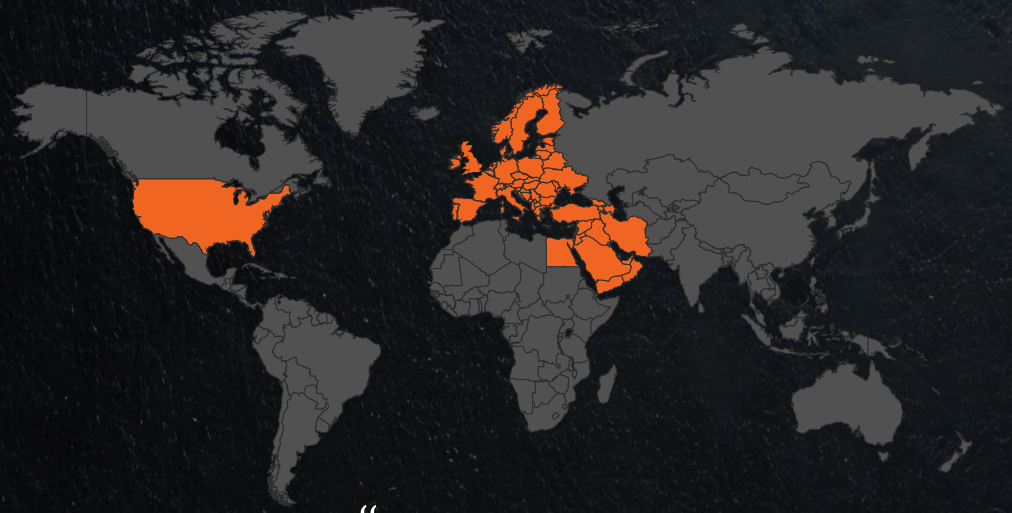
3. Dragos launched additional hunts across subscribed customers and Neighborhood Keeper and anonymously notified impacted parties.

Iran

DRAGOS

NEW THREAT GROUP: BAUXITE (associated with CyberAv3ngers)

ICS ACTIONS AGAINST EASY-TO-ACCESS TARGETS

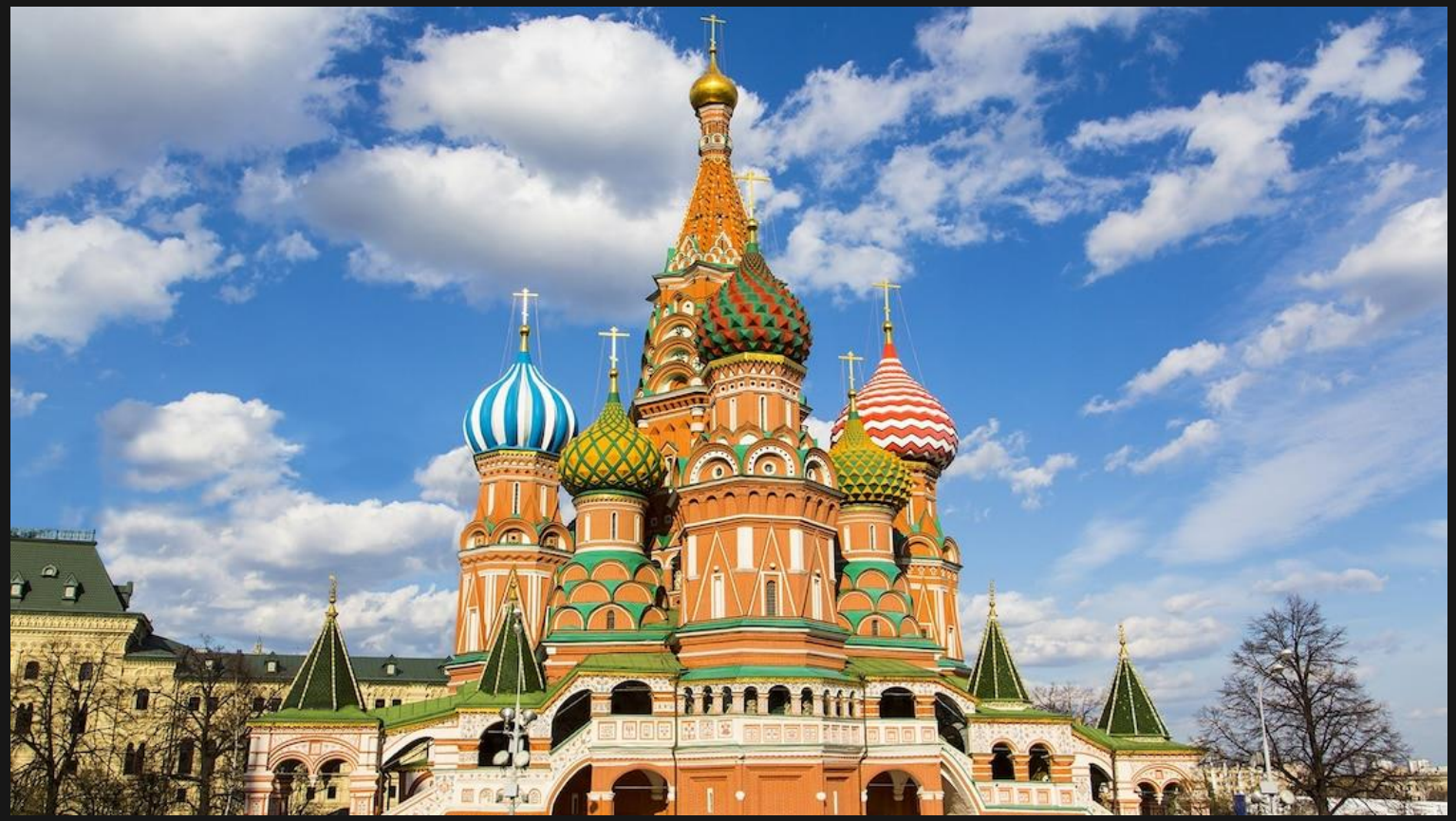


"Between November 2023 and January 2024, CyberAv3ngers targeted U.S.-based Unitronics PLC devices used in multiple critical infrastructure industries, including the WWS Sector, likely in four separate waves of cyberattacks. The actors compromised at least 75 devices, including at least 34 in the WWS Sector in the United States."

-- Cybersecurity & Infrastructure Security Agency

- Oil & Natural Gas
- Electric
- Water & Wastewater
- Food & Beverage
- Chemical Manufacturing

Russia



CyberArmyofRussia_Reborn

PRESS RELEASES

Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn

"In January 2024, CARR claimed responsibility for the overflow of water storage tanks in Abernathy and Muleshoe, Texas, posting video of the manipulation of human-machine interfaces at each facility on a public forum. The compromise of the industrial control systems resulted in the loss of tens of thousands of gallons of water.

Additionally, CARR compromised the supervisory control and data acquisition (SCADA) system of a U.S. energy company, giving them control over the alarms and pumps for tanks in that system."

More Hacktivist Attacks on US Utilities

WIRED

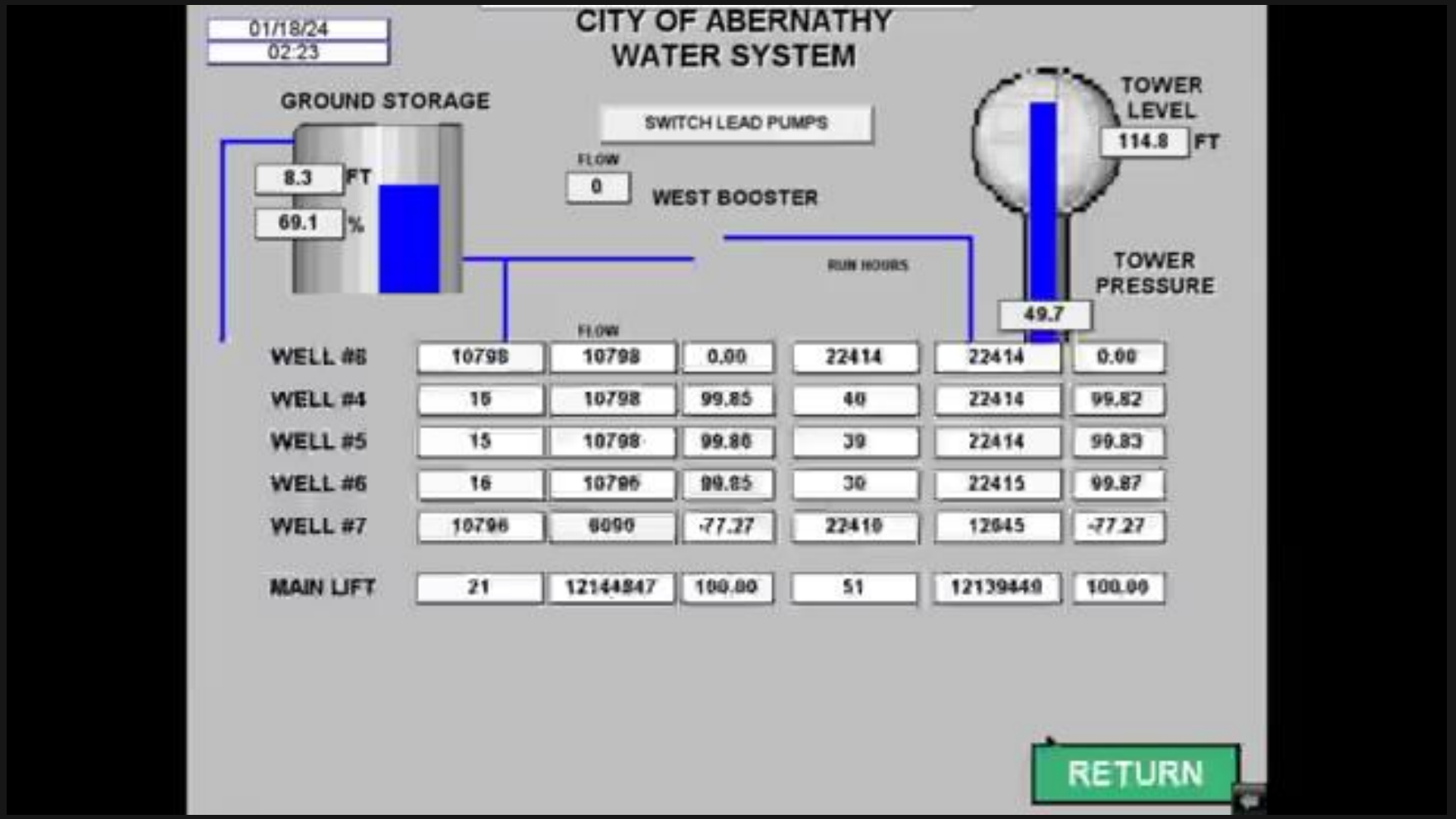
NEWSLETTERS SUBSCRIBE

BY ANDY GREENBERG SECURITY APR 17, 2024 6:00 AM

Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities

Cyber Army of Russia Reborn, a group with ties to the Kremlin's Sandworm unit, is crossing lines even that notorious cyberwarfare unit wouldn't dare to.

WIRED


01/18/24
02:23
CITY OF ABERNATHY
WATER SYSTEM
GROUND STORAGE
8.3 FT
69.1 %
SWITCH LEAD PUMPS
FLOW
0
WEST BOOSTER
TOWER
LEVEL
114.8 FT
TOWER
PRESSURE
49.7
RUN HOURS
FLOW
WELL #8 10798 10798 0.00 22414 22414 0.00
WELL #4 16 10798 99.85 40 22414 99.82
WELL #5 15 10798 99.86 39 22414 99.83
WELL #6 16 10796 99.85 30 22415 99.87
WELL #7 10796 8090 -77.27 22410 12645 -77.27
MAIN LIFT 21 12144847 100.00 51 12139449 100.00
RETURN

WIRED

DRAGOS

Ransomware

RANSOMWARE ATTACKS BY SECTOR

RANSOMWARE ATTACKS INCREASED BY 87% IN 2024

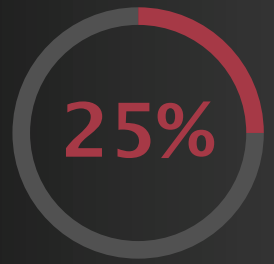
RANSOMWARE BY ICS SECTOR

BASED ON PUBLIC THREAT INTEL SOURCES

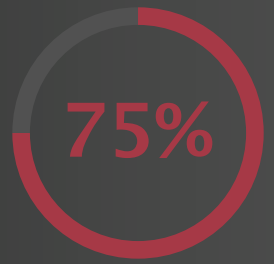
- 1171 Manufacturing
- 177 Industrial Control Systems
- 176 Transportation
- 44 Oil & Gas
- 41 Communications
- 30 Electric
- 20 Government
- 12 Water
- 11 Mining
- 7 Renewables
- 4 Data Centers

TOTAL: 1693 INCIDENTS

Ransomware Insights From Dragos Incident Response Cases



Involved full shutdown



Involved disruption to operations to some degree

WHAT CAN GO WRONG: RANSOMWARE

EXPLOITED UNPATCHED VPN WITH WEAK CREDENTIALS

GAIN ADMIN RIGHTS THROUGH MISCONFIGURED ACCESS

MOVED FROM IT TO OT DUE TO POOR SEGMENTATION

DEPLOY RANSOMWARE

ENCRYPT CRITICAL DATA, CAUSING DOWNTIME

HOW TO FIX IT

- Patch VPN vulnerabilities, enforce MFA
- Restrict admin privileges, monitor access
- Implement strict IT/OT segmentation
- Deploy OT-native threat & anomaly detection
- Conduct TTX, establish offline backups

Ransomware Insights From Dragos Incident Response Cases

Involved some element of a remote service, such as a VPN appliance or remote desktop protocol (RDP) server being leveraged by adversaries.

Numerous ransomware groups are leveraging low-barrier-of-entry intrusion tactics against industrial organizations and capitalizing on a lack of basic network and security hygiene practices.

Until these elements are addressed, ransomware groups will continue exploiting them.

NEW ICS MALWARE DISCOVERED

2010 — STUXNET

2013 — HAVEX

2015 — BLACKENERGY

2016 — CRASHOVERRIDE

Effective techniques with little knowledge of protocols used.

IEC101, IEC104, IEC61850/MMS, OPC-DA

2017 — TRISIS

Understanding of the protocols for reconnaissance and attack.

First malware designed for impacts to human safety.

TRISTATION, TCM, Triconex OS

2022 — PIPEDREAM / INDUSTROYER2

Cross-industry malware toolkit with capabilities for staging an end-to-end attack.

CODESYS, Modbus,

2024 — FUXNET / FROSTYGOOP

Unsophisticated malware causing significant impacts.

Modbus TCP

ICS Malware is…

1. Capable of ICS functions
2. Designed with malicious intent
3. Able to cause adverse effects in OT

FROSTYGOOP ICS MALWARE

What happened?

In January 2024, during sub-zero temperatures, a cyber attack disrupted the energy supply for central heating in more than 600 apartment buildings in Ukraine.

Dragos discovered FrostyGoop in April 2024.

FrostyGoop interacts directly with industrial control systems (ICS) using Modbus TCP over port 502.

9th
known ICS malware

1st
known Modbus ICS malware that causes effects on ICS devices

46,000
Internet-exposed ICS devices communicating over Modbus TCP

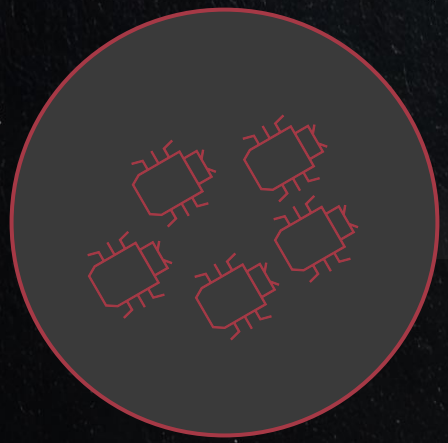
Modbus is used worldwide across industries.

CHERNOVITE'S PIPEDREAM (2022)

Evolution of ICS/OT malware

FIRST scalable, cross-industry OT attack framework (7TH overall ICS/OT specific)
Discovered before it was employed for destructive purposes.

5



ICS PROTOCOLS ABUSED

FINS, MODBUS, CODESYS, OPC UA, Schneider Electric NetManage

100s

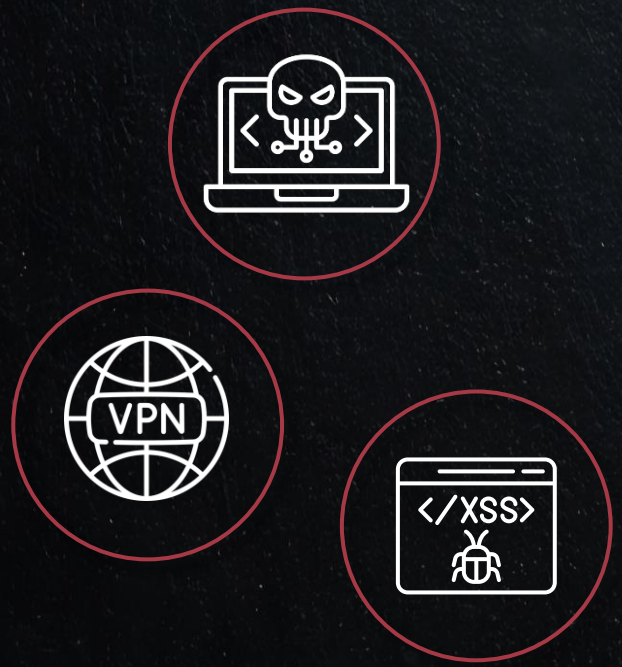
VENDORS IMPACTED

1000s

DEVICES POTENTIALLY IMPACTED

CAPABLE OF DISRUPTIVE & DESTRUCTIVE ICS CYBER ATTACKS

TACTICS, TOOLS, & PROCEDURES



New ICS Malware
is increasingly emerging; lack of visibility in OT conceals the full scope of attacks

Internet-accessible OT devices
key attack path, highlighting need for simple changes to create more defensible architectures

Remote Access
adversaries routinely exploit VPNs, SSH, default credentials, & third-party remote access.

Lateral Spread After Compromise
adversaries use LOTL techniques, native tools, ICS protocols to evade detection.

What can you do??

Free resources available NOW from Dragos

WHY?

Dragos Mission: Safeguarding Civilization

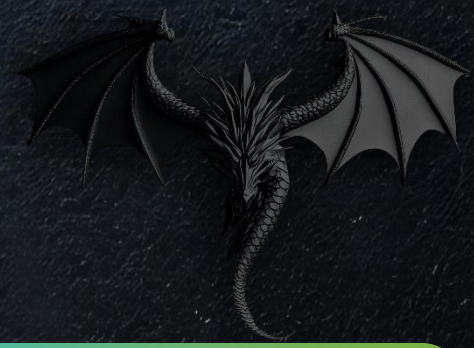
Utilities at Risk: Under Resourced Water, Electric, & Gas

Dragos Community Defense Program

ALL Under Resourced Organizations with OT Environments

Dragos OT-CERT

Dragos Community Defense Program (CDP)



Free OT cybersecurity software technology

Dragos Platform & other key resources

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

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 OT-CERT*

Industrial cybersecurity resources for the OT community

*Operational Technology – Cyber Emergency Readiness Team

FREE CYBERSECURITY RESOURCES

Free content is available for OT asset owners and operators, to help you build and maintain an effective OT cybersecurity program.

OPEN TO GLOBAL ICS/OT COMMUNITY

Content is oriented toward Small and Medium Businesses (SMBs) and resource-challenged organizations with OT environments that lack in-house expertise.

NEW CONTENT

Members have access to a growing library of resources such as toolkits, guides, how-to videos, templates, best practice blogs, tabletop exercises and more, available from the OT-CERT portal.

WORKING SESSIONS

Monthly virtual sessions are offered in 2 convenient time zones for members to get to know each other, ask questions, get advice, and share their successes and challenges.

VULNERABILITY DISCLOSURES

We take a coordinated approach to the disclosure of vulnerabilities, working with vendors to better protect our customers and the ICS/OT community.

Some OT-CERT Resources available now

OT Cybersecurity Fundamentals Self-Assessment

<u>Toolkits:</u>
Asset Management
Collection Management Framework
Host-Based Logging
Incident Response Plan
OT Backups
Secure Remote Access / MFA
Network Segmentation
Default Passwords and Internet-Exposed Devices
System Hardening
Firewall Configurations
Change Management / Detection

Self-Service OT Ransomware Tabletop Toolkit

ICS/OT Cybersecurity Introductory Training, Guides, and Videos

OT-CERT Working Sessions

Best Practices Blog Series

Securing Leadership Support for OT Cybersecurity

Don’t Wait! Get Started Now!

75 free resources

~2,675 members

64 countries

OT-CERT is the Operational Technology — Cyber Emergency Readiness Team

Dedicated to addressing the OT resource gaps that exist in industrial infrastructure.

Best Practices for Cybersecurity in OT

THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

01 ICS Incident Response Plan

02 Defensible Architecture

03 ICS Network Monitoring Visibility

04 Secure Remote Access

05 Risk-based Vulnerability Management


Defense is
Doable
And Together
We Can
Safeguard
Civilization