Electric Sector Cybersecurity

INTELLIGENCE-DRIVEN CYBER DEFENSE STRATEGY 2025

From board members to practitioners, there should be alignment on your cybersecurity needs. Only measuring cybersecurity controls against frameworks, regulations, or risk scores ultimately hinders this alignment.

Move beyond compliance frameworks to threat-focused cybersecurity that addresses real adversary behaviors and protects what matters most.

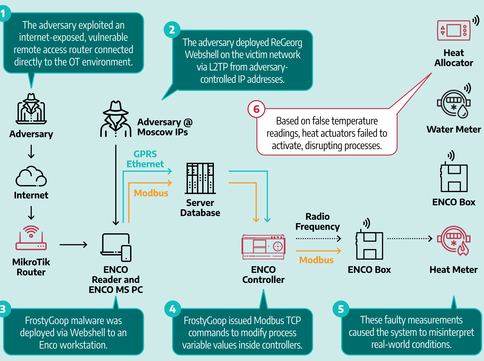
- STEP 1 — Identify Intelligence-Driven Threat Scenarios
- STEP 2 — Deploy Critical Security Controls
- STEP 3 — Prioritize Industrial Sites
- STEP 4 — Gain Security Investment Alignment

Step 1: Identify Intelligence-Driven Threat Scenarios

Identifying industry-specific threat scenarios can enable an organization to understand the adversaries targeting network protocols and systems in operational technology (OT) environments.

FrostyGoop ICS Malware Example

FrostyGoop ICS malware can target devices communicating over Modbus TCP to manipulate control, modify parameters, and send unauthorized command messages. Modbus TCP is a standard ICS protocol used across all industrial sectors worldwide. The malware was used in a disruptive cyber attack on a district energy company in Ukraine, shutting down heating for two days to approximately 100,000 customers during sub-zero temperatures.



Step 2: Deploy Critical Security Controls

What security measures are most critical against the threat?

Applying SANS 5 Critical Controls for World-Class OT Cybersecurity can mitigate threats like FrostyGoop. Each control addresses specific aspects of cybersecurity readiness and resilience.

1 — Incident Response for ICS

Have OT-specific plans that enable rapid isolation of devices, detection of unauthorized Modbus commands, and safe restoration of operations. Train teams for ICS-targeted attacks.

2 — Defensible Architecture

Segment networks to limit exposure—no direct internet access to controllers. Use industrial DMZs and strict IT-to-OT access controls to contain threats.

3 — ICS Network Visibility & Monitoring

Monitor Modbus TCP traffic continuously. Use protocol-aware tools to detect anomalies on port 502 and catch threats early.

4 — Secure Remote Access

Enforce MFA, log all access, and restrict remote entry to only what's needed. Regularly audit and control VPN and user privileges.

5 — Risk-Based Vulnerability Management

Prioritize fixes for network-exploitable vulnerabilities. Where patching isn't possible, apply compensating controls like monitoring and access restrictions.

Step 3: Prioritize Industrial Sites

Where are you most at risk from the threat?

- Map exposed sites with direct or indirect access from business networks.
- Identify facilities using remote access or shared engineering workstations.
- Focus on high-consequence environments.

Step 4: Gain Security Investment Alignment

What should you do and why now?

- Justify investments with real threat scenarios and known adversary activity.
- Use threat intelligence to show business risk, not just technical risk.
- Align controls to adversary behavior, not just compliance frameworks.

GLOBAL CYBERSECURITY REGULATION DRIVERS

NERC CIP | NIS2 | AESCSF | OTCC | CCOP

ADDITIONAL ELECTRIC SECTOR THREAT SCENARIOS

Vz VOLTZITE

METHOD: Living-off-the-land techniques

TARGET: U.S. electric utilities via exposed firewalls/VPNs

IMPACT: Steals engineering files, disrupts operator visibility

ATTACK PATH

- Vulnerable remote access devices
- Leverage native tools
- File theft
- Persistent access

Ka KAMACITE

METHOD: Phishing and credential theft

TARGET: Electric sector (initial access role)

IMPACT: Establishes foothold, supports follow-on OT compromise

ATTACK PATH

- Phishing
- Remote access
- Lateral movement with native/commodity tools
- Handoff to ELECTRUM

El ELECTRUM

METHOD: Custom ICS malware (e.g., Industroyer2)

TARGET: Ukraine electric grid

IMPACT: Grid disruption via industrial protocol manipulation

ATTACK PATH

- Deploy ICS malware
- Issue remote breaker commands via IEC-101/104
- Disrupt Operations
- Use wiper to hinder recovery

Want Deep Insights Into These Threats?

Explore detailed threat group profiles, real-world attack scenarios, and electric sector risk trends in the 2025 Dragos OT/ICS Cybersecurity Report, our 8th Annual Year in Review.

DOWNLOAD REPORT

Dragos delivers complete industrial cybersecurity for electric utilities, from real-time OT detection to in-depth threat intelligence and expert-led threat hunting and response services. Let's work together to reduce risk, stop adversaries, and safeguard operations across your OT network. Dragos.com.

DRAGOS