Oil & Gas 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.

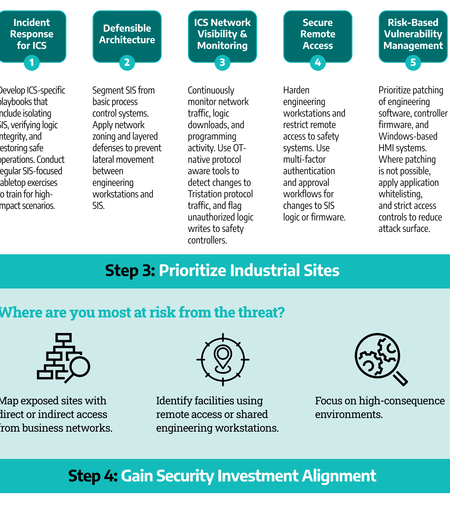
- STEP 1 — Identify Intelligence-Driven Threat Scenarios
- STEP 2 — Deploy Critical Security Controls
- STEP 3 — Prioritize Industrial Sites
- STEP 4 — Gain Security Investment Alignment

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.

TRISIS ICS Malware Example

TRISIS marked the first direct targeting and compromise of safety system features, having been deployed against a petrochemical plant SIS in Saudi Arabia in 2017. The threat group XENOTIME, responsible for TRISIS, has been identified in multiple Middle Eastern facilities. The attackers aimed to disable safety features, but a minor coding error caused the attack to fail, triggering safety shutdowns and halting plant operations.



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 TRISIS. Each control addresses specific aspects of cybersecurity readiness and resilience.

1 Incident Response for ICS

Develop ICS-specific playbooks that include isolating SIS, verifying logic integrity, and restoring safe operations. Conduct regular SIS-focused tabletop exercises to train for high-impact scenarios.

2 Defensible Architecture

Segment SIS from basic process control systems. Apply network zoning and layered defenses to prevent lateral movement between engineering workstations and SIS.

3 ICS Network Visibility & Monitoring

Continuously monitor network traffic, logic downloads, and programming activity. Use OT-native protocol aware tools to detect changes to Tristation protocol traffic, and flag unauthorized logic writes to safety controllers.

4 Secure Remote Access

Harden engineering workstations and restrict remote access to safety systems. Use multi-factor authentication and approval workflows for changes to SIS logic or firmware.

5 Risk-Based Vulnerability Management

Prioritize patching of engineering software, controller firmware, and Windows-based HMI systems. Where patching is not possible, apply application whitelisting, and strict access controls to reduce attack surface.

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 OIL & GAS SECTOR THREAT SCENARIOS

Bx BAUXITE

METHOD: Exploitation of vulnerable internet-facing firewall

TARGET: Opportunistic, compromised oil rig sites

IMPACT: Potential reconnaissance; pathway for future OT disruption

ATTACK PATH

- Internet-facing firewall appliances
- Vulnerability exploited
- Pathway to actions on objectives

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

Gr GRAPHITE

METHOD: Spearphishing and malicious documents to deliver malware

TARGET: Downstream and midstream oil & gas entities

IMPACT: Credential harvesting

ATTACK PATH

- Phishing email delivers malicious documents
- Downloads malware enabling backdoor
- Harvests credentials
- Gains access to files tied to OT systems

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