



# 2025 OT Cybersecurity Action Guide

G L O B A L

CONTENTS

Introduction.....3

Key Findings: By The Numbers..... 4

Global OT Threat Trends ..... 6

    Geopolitical Cyber Operations Intensify Against Industrial Targets..... 6

    Convergence of State-Sponsored Threat Groups, Ransomware, and Hacktivists..... 6

    Ransomware Groups Shift to OT-Specific Attack Vectors..... 6

    Living-Off-the-Land (LOTL) Techniques Enable Persistent ICS Attacks ..... 6

    Exploitation of Vulnerabilities in Internet-Exposed OT Devices ..... 7

    Security Postures Must Evolve to Meet Growing Threats ..... 7

Adversaries Targeting Operational Technology (OT)..... 8

    New Dragos Threat Groups..... 8

    Dragos Threat Group Updates..... 9

The Deployment of ICS Malware ..... 10

The Ransomware Threat Landscape.....11

Your 2025 Action Guide: Mapping to 5 Critical Controls for ICS Cybersecurity ..... 12

    Define An ICS Incident Response Plan.....12

    Build a Defensible Architecture..... 14

    Establish OT Visibility & Network Monitoring .....17

    Secure Remote Access..... 19

    Take a Risk-Based Approach to Vulnerability Management .....21

Ready to Dive Deeper? ..... 23

# Introduction

Operational technology (OT) cybersecurity has never been more critical. Last year, attacks on industrial control systems (ICS) were driven by state-sponsored adversaries, ransomware groups, and hacktivists seeking to destabilize and disrupt industrial infrastructure. From destructive wiper malware attacks on energy and telecom networks to ransomware crippling manufacturing and water treatment facilities, adversaries are evolving their tactics faster than defenders can react.

The 2025 OT Cybersecurity Action Guide transforms the latest findings from Dragos's 2025 OT/ICS Cybersecurity Report, our 8th annual Year in Review, into immediate, actionable steps organizations can take to detect, mitigate, and prevent cyber threats targeting industrial operations. Whether responding to a ransomware attack exploiting remote access, assessing vulnerability risks to your most critical assets, or building an OT-specific threat monitoring program, this guide provides simplified guidance to strengthen defenses and enhance operational resilience.

By following the SANS Institute's 5 Critical Controls for ICS Cybersecurity, organizations can map real-world attack scenarios to their environment, test and refine defenses, and close visibility gaps before adversaries can exploit them. Defense is doable no matter where you are in your OT cybersecurity journey.

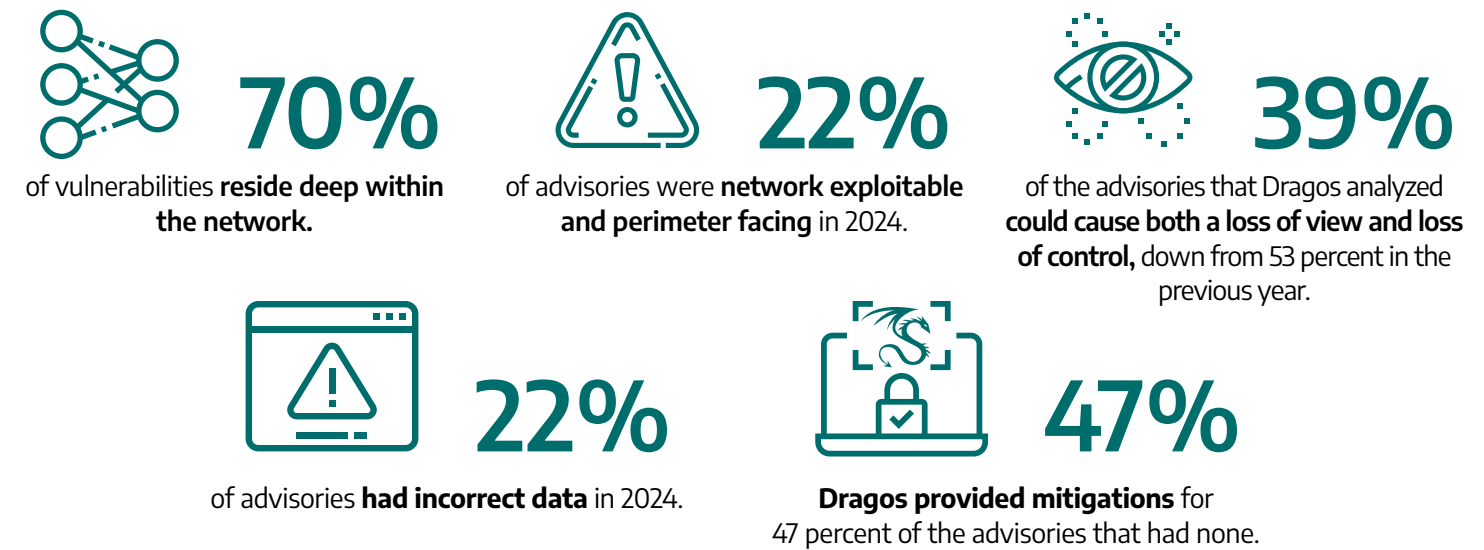


# Key Findings: By The Numbers

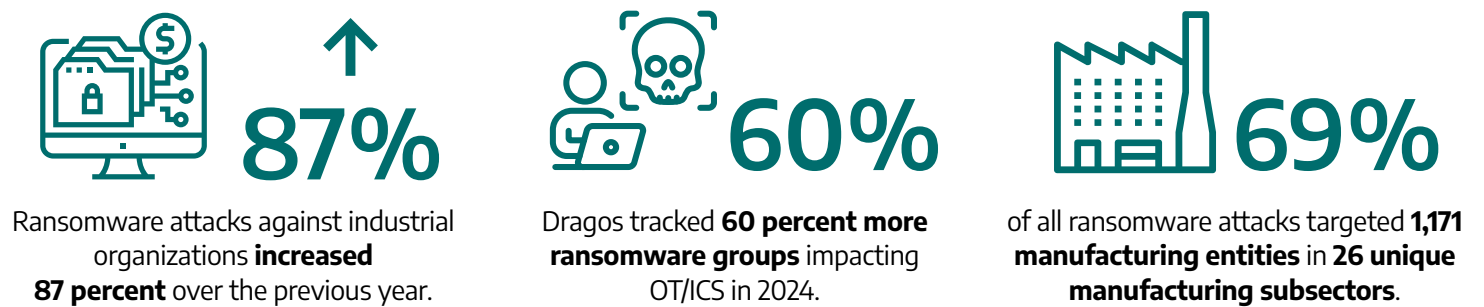
Dragos tracks 23 THREAT GROUPS, 9 of which were active in 2024.



## Key Vulnerabilities Findings



## Key Ransomware Findings



OT Protocols Used

Modbus	FINS	Meter-bus
CIP	OPC/UA	S7comm
	CODESYS	

IT Protocols Used

SSH	RDP	VNC
HTTP	HTTPS	PPTP
IMAP	WebDAV (over HTTPS)	

Industries Targeted



Electric



Oil & Gas



Defense Industrial  
Base



Manufacturing



Telecommunications



Maritime



Water & Wastewater



Food & Beverage



Chemical Manufacturing



Mining

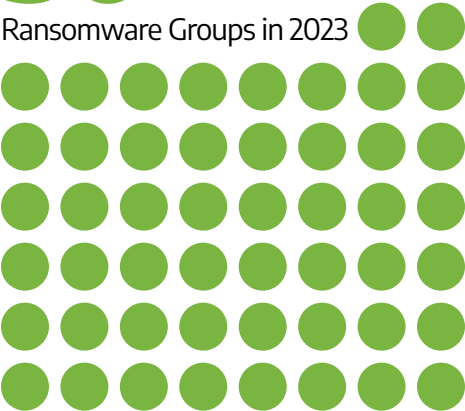


Transportation & Logistics

Ransomware Groups

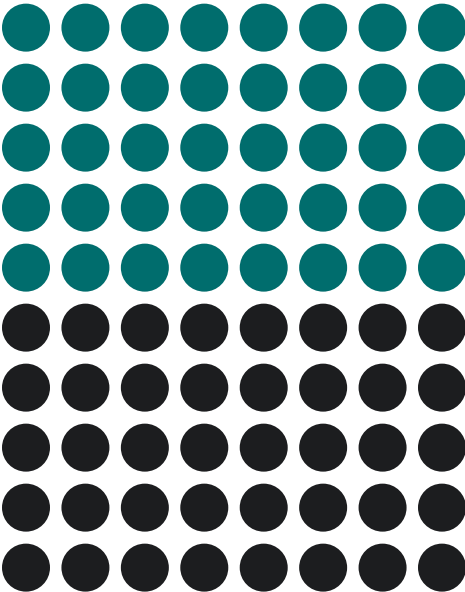
50

Ransomware Groups in 2023



80

Ransomware Groups in 2024



50%  
target  
Manufacturing



# Global OT Threat Trends

## Geopolitical Cyber Operations Intensify Against Industrial Targets

The industrial threat landscape continues to evolve, with geopolitically driven cyber operations increasingly targeting critical industrial infrastructure. State-sponsored threat groups prioritize energy, telecommunications, and water systems as strategic targets, with groups like ELECTRUM maintaining their focus on ICS-specific cyber operations. The Kyivstar telecom attack in December 2023 and the discovery of the AcidPour wiper in early 2024 highlight the continued expansion of disruptive operations against industrial control systems, reinforcing the need for real-time OT network monitoring to detect adversary footholds before they escalate to destructive attacks. In addition to targeting VPN and firewall vulnerabilities for long-term access, VOLTZITE has been linked to espionage campaigns against critical infrastructure in multiple regions, focusing on pre-positioning within ICS networks for potential future operations. Without OT-native network visibility, defenders cannot detect these threats in time to mitigate impact.

## Convergence of State-Sponsored Threat Groups, Ransomware, and Hacktivists

A concerning trend is the convergence of hacktivists, cyber criminals, and state-sponsored adversaries, creating a blurred, more unpredictable threat landscape. The emergence of the Fuxnet ICS malware deployed by the pro-Ukraine hacktivist group and the unrelated BAUXITE threat group demonstrates that ICS-specific threats are no longer exclusive to highly sophisticated threat groups – any motivated group with the right tools can now disrupt industrial operations. Moreover, the revelation of shared intelligence, infrastructure, and victims across specific

state-sponsored threat groups and hacktivist groups demonstrates these associations are not merely theoretical. Meanwhile, several hacktivist groups actively used ransomware as a component of their cyber operations, a concerning new evolution for critical sectors that are viewed as strategic targets. As the OT threat ecosystem broadens, industrial organizations must prioritize network visibility and real-time threat detection to counter threats that increasingly bypass traditional IT security tools.

## Ransomware Groups Shift to OT-Specific Attack Vectors

Ransomware remains one of the most disruptive threats to industrial operations, with an 87 percent increase in attacks on OT environments in 2024. Ransomware groups targeting industrial organizations account for 60 percent of all tracked ransomware operations. The targeting of remote access mechanisms has made industrial networks particularly vulnerable. Unpatched remote access gateways in OT networks enable ransomware groups to deploy payloads that encrypt engineering workstations, HMIs, and industrial databases. Without OT-native threat detection, these attacks go unnoticed until they directly impact operational uptime and safety.

## Living-Off-the-Land (LOTL) Techniques Enable Persistent ICS Attacks

Adversaries increasingly employ living off the land (LOTL), using built-in ICS protocols and administrative tools to evade detection. Instead of relying on custom exploits or malware, adversaries manipulate native ICS commands, making it difficult for traditional security tools to identify malicious behavior. Groups like BAUXITE, known for SSH-based persistence in industrial networks, and KAMACITE, which

has leveraged PowerShell to maintain energy network access, exemplify this behavior. Adversaries with disruptive intent leveraged ICS protocols throughout the past year, including Modbus TCP and DNP3. Ransomware groups also took advantage of native administrative tools to conceal malicious activities and remain undetected for extended periods of time. Only monitoring with deep ICS protocol awareness can distinguish between legitimate engineering activity and adversary abuse or built-in functionalities.

## Exploitation of Vulnerabilities in Internet-Exposed OT Devices

Exploiting vulnerabilities in internet-exposed OT devices remains a pressing concern. 100 percent of BAUXITE's observed targets were internet-accessible, indicating that adversaries prioritize weakly defended, remotely accessible entry points. Organizations that continue operating unpatched or exposed industrial assets without compensating controls leave critical infrastructure vulnerable to scanning, credential theft, and remote exploitation. Network segmentation and attack surface reduction are crucial, but they must be complemented by active monitoring of ICS traffic to identify early stage-reconnaissance and unauthorized access attempts.

## Security Postures Must Evolve to Meet Growing Threats


Despite the aggressiveness of OT threats in 2024, many industrial organizations cannot still see what is happening on their OT networks. The 45 percent of industrial organizations that still do not have complete visibility into their OT environments cannot detect malware infections, unauthorized access, or ICS protocol abuse. They cannot assess the full scope of an attack, making it near impossible to contain and mitigate it. IT security tools are not enough – without OT-native network monitoring and ICS-aware threat detection, defenders will continue playing catch-up against adversaries who have already adapted their techniques to bypass traditional security solutions. As cyber threats to industrial operations accelerate, real-time network monitoring, proactive threat hunting, and deep visibility into OT environments must become foundational security priorities. These must be complemented with an ICS-specific incident response plan, defensible architecture, secure remote access, and a risk-based approach to securing vulnerabilities for assets within and adjacent to OT networks.




# Adversaries Targeting Operational Technology (OT)


Driven by geopolitical conflicts, adversaries across the spectrum are actively compromising OT networks, collecting intelligence, and pre-positioning for disruptive action. Dragos tracks 23 threat groups targeting industrial organizations, nine of which were active, with two new threat groups detailed in this year's [OT Cybersecurity Year in Review](#) report.

## New Dragos Threat Groups



BAUXITE






**Industries:** Oil & Gas, Electric, Water & Wastewater, Chemical Manufacturing, Food & Beverage Manufacturing


**Geographic Focus:** Global, focus on the United States, Europe, and the Middle East


**Attack Vectors:** Internet-facing devices and services, specifically virtual private networks (VPNs), firewalls, and programmable logic controllers (PLCs)

BAUXITE targeted industrial control systems (ICS) through brute-force SSH attacks, default PLC credentials, and malware like IOControl, leading to persistent backdoors, ladder logic manipulation, and potential firmware wiping.



GRAPHITE





**Industries:** Oil & Gas, Defense Industrial Bases, Government, Logistics

**Geographic Focus:** Eastern Europe, Middle East

**Attack Vectors:** Spear-phishing emails with malicious attachments

GRAPHITE leveraged exploits in Microsoft Outlook (CVE-2023-23397) and WinRAR (CVE-2023-38831) for spear-phishing and credential theft, deploying backdoors like HEADLACE and MASEPIE while using IMAP drafts for covert exfiltration.





## Dragos Threat Group Updates



### VOLTZITE



**Industries:** Energy, Telecom, Water Infrastructure

**Geographic Focus:** North America, Asia-Pacific

**Attack Vectors:** Exploited VPNs and firewalls

VOLTZITE focused on espionage and ICS reconnaissance, exploiting internet-facing devices, small office/home office (SOHO) routers, and living-off-the-land (LOTL) techniques to establish persistent botnets and map industrial networks.



### KAMACITE



**Industries:** Energy, Oil & Gas

**Geographic Focus:** Ukraine, expanding into Europe

**Attack Vectors:** Exploited VPNs and remote access vulnerabilities

KAMACITE specializes in persistent access and espionage, using Kapeka malware to infiltrate Ukraine's energy and telecom networks, later expanding into European oil & gas. It continues deploying DarkCrystal RAT for surveillance while leveraging LummaStealer in spear-phishing campaigns targeting major technology providers. KAMACITE intrusions enable ELECTRUM ICS attacks.



### ELECTRUM



**Industries:** Energy, Telecom

**Geographic Focus:** Ukraine, Poland

**Attack Vectors:** VPNs, routers, ICS-aware malware

ELECTRUM continues targeting energy and telecom infrastructure, leveraging ICS-aware malware and disruptive cyber operations. The group disrupted telecommunications and critical infrastructure in Ukraine, with potential spillover into energy systems. The group has also deployed the Acid Pour wiper malware, designed to manipulate and disrupt industrial control systems, reinforcing its capabilities in destructive ICS-targeted cyber operations.



# The Deployment of ICS Malware

Unlike general-purpose IT malware, ICS malware is purpose-built to impact industrial control systems, making it an immediate operational risk to industrial and critical infrastructure. In 2024, Fuxnet and FrostyGoop, the eighth- and ninth-known ICS malware families, respectively, were discovered.

**Fuxnet is the eighth known ICS malware, designed to disrupt OT sensor operations.** First observed in April 2024, the pro-Ukrainian hacktivist Blackjack allegedly used it to target Moskollektor, a Russian organization managing Moscow's municipal infrastructure. The attack aimed to

interfere with critical monitoring networks, though its full capabilities are still under validation.

**FrostyGoop is the first malware to use Modbus TCP protocol for disruptive effects and the ninth known ICS malware** overall, which was discovered in early 2024. It directly interacts with industrial control systems via Modbus TCP over port 502, making it a highly targeted threat to OT environments. In January 2024, an attack using FrostyGoop disrupted the energy supply for central heating in 600+ apartment buildings in Ukraine, highlighting the increasing risk of ICS malware targeting critical infrastructure.

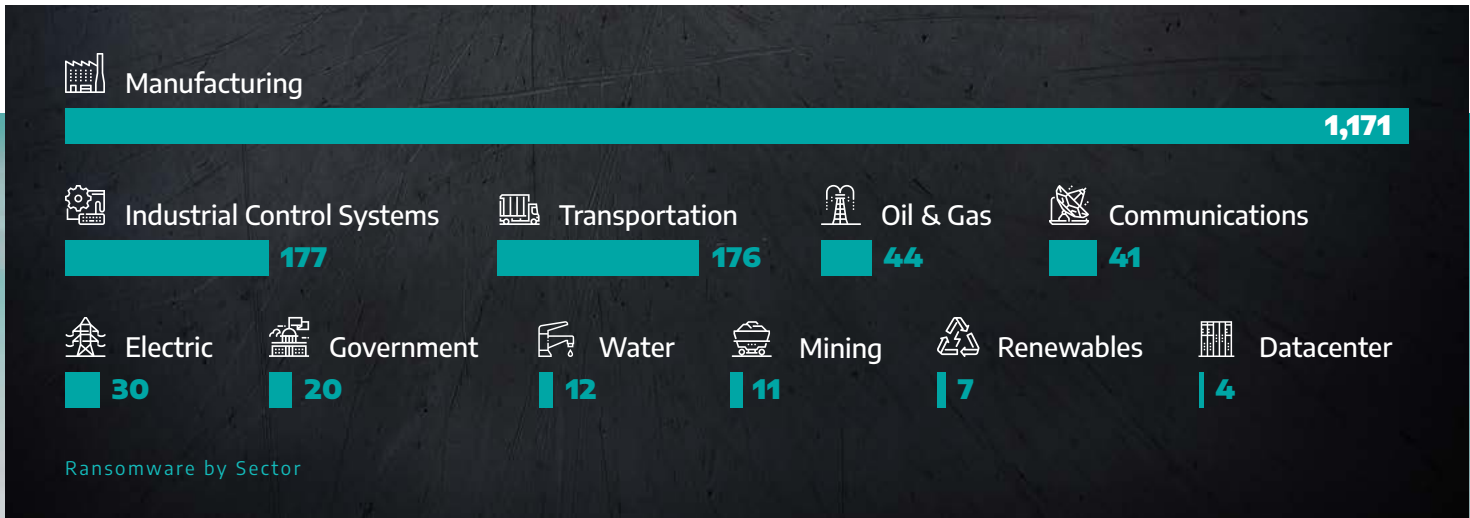
# The Ransomware Threat Landscape

In 2024, Dragos observed 1,693 industrial organizations with sensitive data and information posted onto various ransomware groups’ dedicated leak sites (DLS). This represents an 87 percent increase over the previous year.

Manufacturing remains the top target for ransomware attacks against industrial organizations; more than 50 percent of all observed ransomware victims were in the manufacturing sector, representing 1,171 attacks.

Ransomware groups know that even brief disruptions can cause significant financial and logistical fallout, putting safety at risk and making manufacturers more likely to pay. Other industrial sectors, including energy, transportation, and industrial control system vendors, also remain high on the list as ransomware groups refine their tactics to maximize pressure and impact.

With these threats showing no sign of slowing, organizations must prioritize resilience, proactive defenses, and incident response readiness.



# Your 2025 Action Guide: Mapping to 5 Critical Controls for ICS Cybersecurity

Adversaries continuously evolve their tactics. Critical cybersecurity controls can be optimized and informed by the emerging threat intelligence and strategic insights provided in the 2025 Dragos OT/ICS Cybersecurity Report.

Effective implementation of the SANS Institute's 5 Critical Controls for ICS Cybersecurity remains the best defense against adversaries targeting OT. Organizations with strong incident response capabilities, defensible architectures, secure remote access protocols, and robust network monitoring are far better positioned to reduce the risk of a successful attack on the enterprise OT even in this increasingly complex threat environment.



## Define An ICS Incident Response Plan

Ransomware compromises accounted for most cases that Dragos responded to, with 25 percent resulting in a complete shutdown of an OT site and 75 percent resulting in at least some disruption to operations. Twenty percent of all incidents involved remote access exploitation, including VPN exploits, remote access applications, and remote desktop protocol (RDP) from the enterprise IT network.

An ICS incident response plan aims to detect, contain, and recover from cyber incidents without disrupting industrial operations or safety. The plan must be actionable, tested, and integrated across security, engineering, and operations teams to ensure a coordinated and effective response.

**Refer to the Dragos 2025 OT/ICS Cybersecurity Report to build intelligence-driven threat scenarios, such as the one for a ransomware attack via remote services in the example below. Use the report as an entry point to develop, test, and refine incident response plans.**



## Scenario: Ransomware Attack via Remote Services

The following scenario highlights the complexity of ransomware attacks in OT environments, where IT intrusions can quickly escalate into operational disruptions. Effective incident response requires rapid detection and containment and a deep understanding of OT threats, adversary tactics, and system interdependencies.



A ransomware group exploits unpatched VPN appliances (CVE-2020-3259 and CVE-2023-20269) to gain unauthorized access to the OT network. They use stolen credentials and brute-force techniques to access remote services. Once inside, they disable security tools, move laterally across IT and OT environments, and encrypt critical OT files, including HMI configurations, engineering workstation data, and operational databases. Facility operations are disrupted. The ransomware group demands a \$5 million ransom in cryptocurrency and threatens to leak sensitive information.

#### **Inject 1: IT security detects unauthorized VPN access using stolen credentials.**

- ☒ Investigate VPN logs
- ☒ Disable compromised accounts
- ☒ Initiate containment measures

#### **Inject 2: Endpoint protection logs show attempts to disable security tools on IT and OT systems.**

- ☒ Review security tool logs
- ☒ Investigate RDP usage
- ☒ Monitor on critical OT systems

#### **Inject 3: Lateral movement detected between IT and OT networks.**

- ☒ Check firewall logs
- ☒ Isolate engineering workstations and remote desktop servers
- ☒ Initiate threat hunting operations

#### **Inject 4: OT operators report locked files and ransom notes appearing on HMI and engineering workstations.**

- ☒ Quarantine all affected workstations and HMIs
- ☒ Validate PLC integrity
- ☒ Assess backup integrity
- ☒ Engage legal, law enforcement, and threat intelligence partners

#### **Inject 5: OT operations experience downtime, with safety risks escalating.**

- ☒ Assess physical and process safety systems
- ☒ Conduct forensic analysis
- ☒ Review and enhance VPN security

## How Dragos Can Help

Dragos equips organizations with the technology, threat intelligence, and expertise to detect, respond, and recover from cyber incidents in OT environments.

- The Dragos Platform provides deep visibility, continuous monitoring, and advanced threat detections to identify and contain threats before they disrupt operations.
- Dragos Professional Services provide expert-led investigation, containment, and recovery to minimize downtime and operational impact. Professional Services further strengthen security postures through

proactive assessments, tabletop exercises (TTX), and tailored defense strategies.

- OT Watch, Dragos's threat hunting service, ensures expert monitoring and rapid response.
- At the same time, WorldView Threat Intelligence delivers actionable insights into adversary tactics, including ransomware impacting industrial organizations, to keep defenders ahead of emerging threats.

This integrated approach to the threat lifecycle helps organizations respond effectively to cyber attacks impacting operational technology and industrial control systems.

<sup>1</sup><https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a>



## Build a Defensible Architecture

Dragos assessed that organizations that did not employ network segmentation experienced longer recovery times from a cyber event, more involved incident response efforts, more severe production downtime, and increased remediation costs.

Building a defensible architecture will reduce the attack surface, limit adversary movement, and ensure only authorized users and systems can interact with OT environments. This protects both business continuity and system integrity.

**Use the Dragos 2025 OT/ICS Cybersecurity Report to understand how adversaries infiltrate industrial organizations. The example below illustrates the techniques and capabilities used in BAUXITE attacks. Use this and other examples in the report to strengthen the defensibility of your OT architecture based on active threats.**



### STEP 1

Map Your Attack Surface Using Real-World Threat Trends



### STEP 2

Implement Security Controls to Block High-Risk Entry Points



### STEP 3

Analyze Access & Segmentation Policies



### STEP 4

Conduct Threat-Informed Defensibility Testing

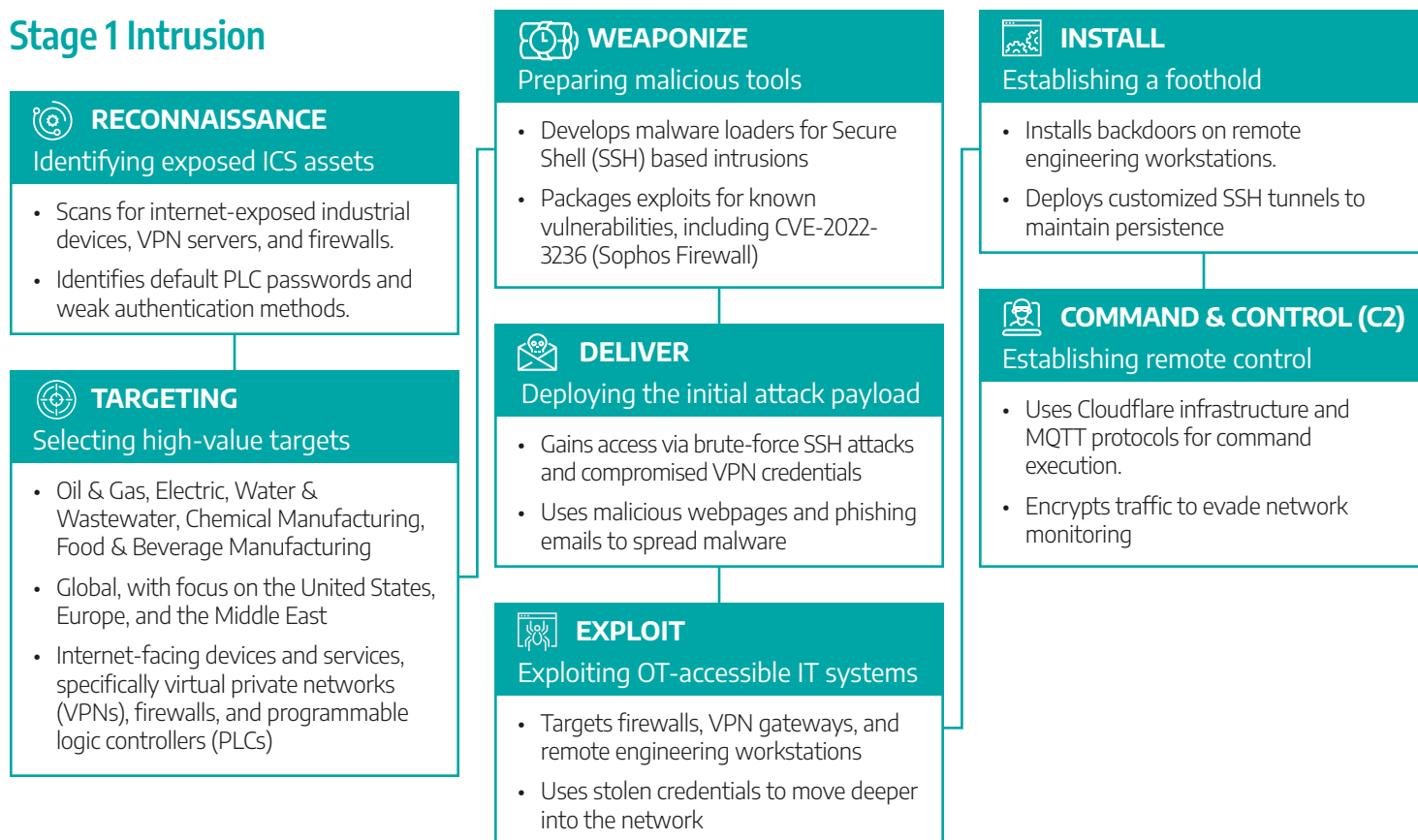




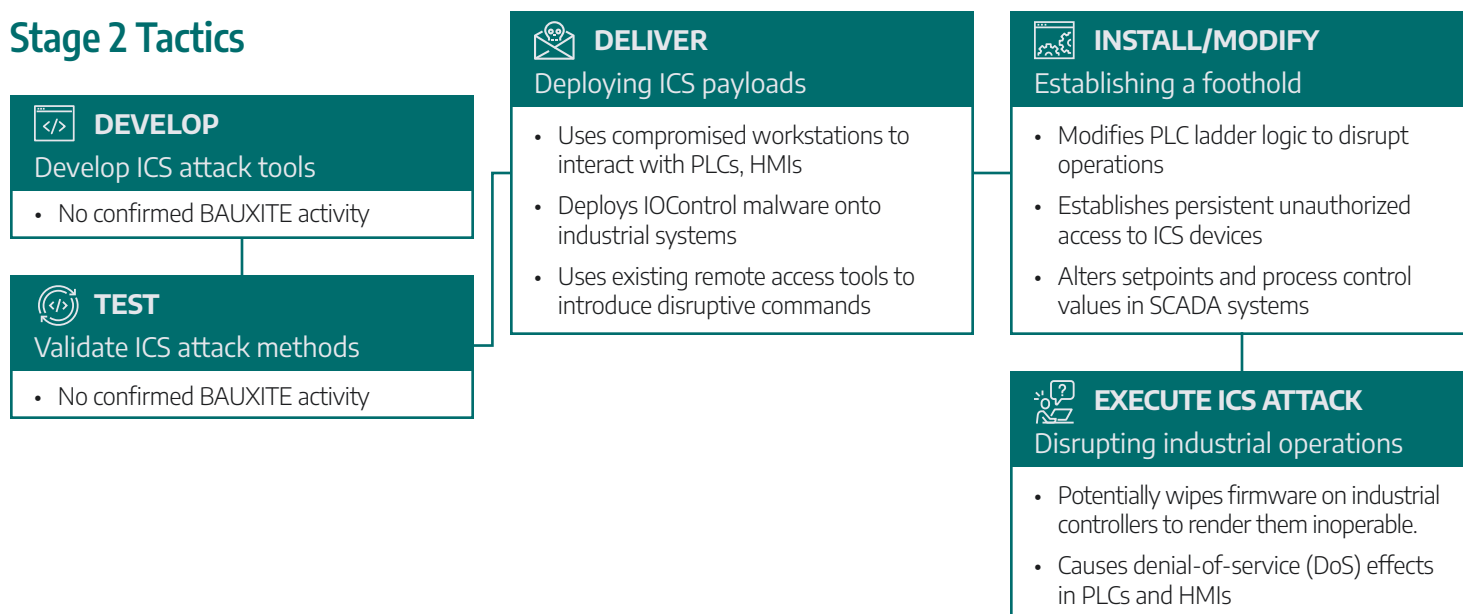
## ICS Cyber Kill Chain: BAUXITE

The BAUXITE ICS Cyber Kill Chain demonstrates how adversaries exploit weak points in OT environments, from initial intrusion to full-scale operational disruption. Understanding these tactics is crucial for strengthening defenses, limiting attack opportunities, and ensuring critical systems remain secure against evolving threats.

### Stage 1 Intrusion



### Stage 2 Tactics



### Defending Against BAUXITE – A Checklist

The following checklist defines what your organisation can do to defend against the BAUXITE threat group.

- ☑ Disable internet exposure of OT devices
- ☑ Enforce firewall rules for SSH and VPN connections.
- ☑ Replace default credentials on PLCs, HMIs, and firewalls.
- ☑ Implement multi-factor authentication (MFA) for all remote access.
- ☑ Monitor for unauthorised remote access (SSH, VPN, RDP).
- ☑ Deploy network monitoring and threat detection for ICS protocols.
- ☑ Implement strict access controls to protect critical OT assets.
- ☑ Conduct red team exercises to test detection of BAUXITE tactics.
- ☑ Develop playbooks for ICS threat hunting and response.
- ☑ Evaluate firewall policies along with access paths to and through OT.

## How Dragos Can Help

A strong defensible architecture is key to reducing attack surfaces and limiting adversary movement in OT. Dragos helps organisations achieve this by providing deep visibility into assets and network behaviors, ensuring threats are detected before they escalate.

- Dragos Platform enables organisations to monitor continuously for misconfigurations, unauthorised access attempts, and high-risk behaviors associated with known threat groups like BAUXITE.
- OT Watch continuously hunts for threats to detect deviations and emerging tactics.
- At the same time, WorldView Threat Intelligence provides proactive insights ensuring defenses stay

ahead of the threat landscape.

- Through Professional Services, Dragos helps organisations implement best practices, conduct tabletop exercises (TTX), and assess architecture resilience against real-world adversary techniques.
- NP-View automates analysis of firewall policies, access paths, and network topology maps to visualize and build more secure networks.

By integrating Dragos solutions, customers gain a hardened OT environment that minimises vulnerabilities, limits lateral movement, and detects when unauthorised users and systems interact with critical infrastructure – ultimately protecting business continuity and system integrity.







## Establish OT Visibility & Network Monitoring

45 percent of the organizations that Dragos assessed lack complete visibility and monitoring for their OT networks. This means many industrial organizations still do not know if they have been compromised or the full scope of cyber attacks impacting their industrial control systems.

Early threat detection can prevent minor security issues from becoming major operational disruptions. This requires continuous situational awareness of all assets, communications, anomalies, and threat behaviors within the OT environment.

**The Dragos 2025 OT/ICS Cybersecurity Report provides critical threat intelligence on how adversaries evade detection in OT environments using living-off-the-land techniques, dual-use tools, and ICS protocol abuse.**

Establishing and continuously validating baseline behaviors and emerging adversary techniques is essential



**STEP 1**  
Establish a Baseline and Document Threat Behaviors



**STEP 2**  
Conduct Threat Hunts for Emerging Threats & Deviations



**STEP 3**  
Validate Threat Detection Against Known Behaviors

for detecting suspicious activity in OT environments. However, hunting for threats and developing effective detections require deep expertise across industrial protocols, adversary tradecraft, malware analysis, and operational technology environments – skills that are not common. By comparing real-time network traffic against known-good operations, defenders with the right expertise can identify unauthorized access, protocol misuse, and adversary techniques like those seen in FrostyGoop malware and BAUXITE threat group attacks.

## Detecting FrostyGoop ICS Malware

FrostyGoop ICS malware interacts directly with industrial controllers over port 502. Understanding baseline data and analyzing threat behaviors associated with FrostyGoop informs the hunt for and the detection of this threat.

Baselines: What Normal Looks Like	Detection: Suspicious Threat Behaviors
Routine communication interactions between HMIs, PLCs, and engineering workstations.	Unauthorized Modbus TCP write commands modifying register values outside expected ranges.
Limited read/write register operations and absence of diagnostic or loopback commands.	Unexpected function codes, such as Force Listen Only Mode, Loopback, and Control Coil commands.
Authorized engineering or SCADA systems IP addresses issuing Modbus TCP requests.	Unusual IP addresses issuing Modbus TCP requests to PLCs on port 502, originating from IT or external sources.
Command execution is limited to approved devices without unauthorized system changes.	High-frequency scanning and reconnaissance behavior looking for responsive industrial device, originating from IT or external sources.

Detecting BAUXITE

BAUXITE exploits weaknesses in remote access security, weak authentication, and IT-OT segmentation.

Baselines: What Normal Looks Like	Detection: Suspicious Threat Behaviors
Routine remote access interactions limited to authorized personnel.	Access attempts via brute-force attacks, stolen or default credentials, exploiting unpatched vulnerabilities.
Predictable ICS protocol traffic between known assets, with no IT-OT communications.	Unauthorized SMB, RDP, and RPC traffic was detected between the IT and OT networks, indicating lateral movement.
Authorized engineering workstations issue legitimate control commands to PLCs and HMIs with expected function codes.	Unauthorized firmware modifications, ladder logic changes, and attempts to execute scripts on engineering workstations.
Command execution is limited to approved devices with no unauthorized system changes.	Adversaries disable logging, remove forensic artifacts, and establish C2 channels.

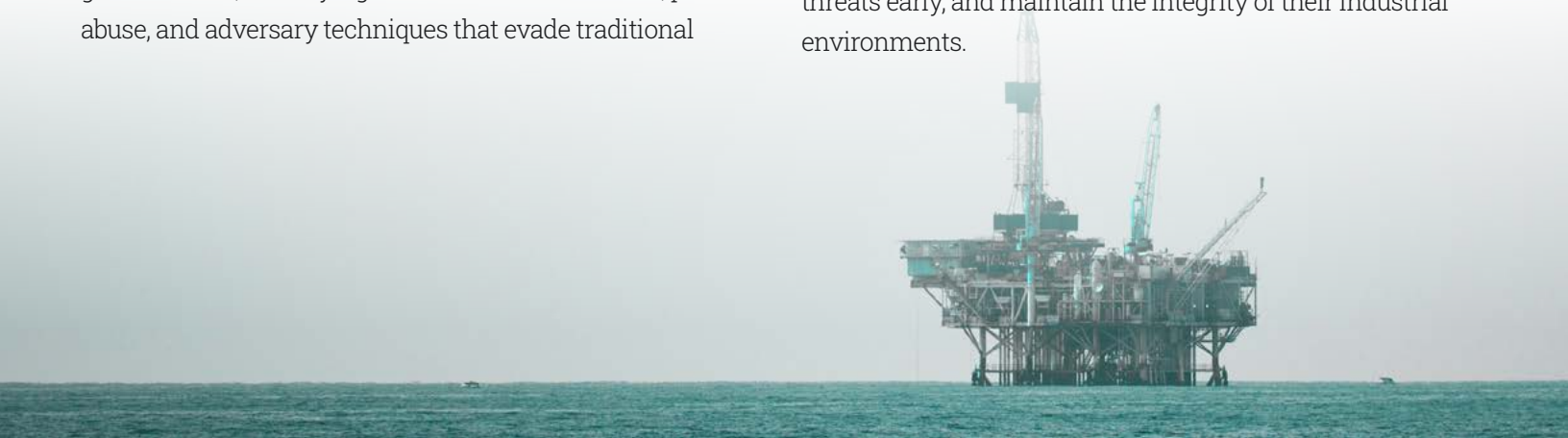
How Dragos Can Help

Adequate OT security starts with complete visibility into assets, communications, and network behaviors.

The Dragos Platform provides deep situational awareness by passively monitoring OT networks, identifying assets, mapping communication flows, and detecting deviations from normal operations. With deep packet inspection (DPI) and ICS protocol awareness, the platform analyzes traffic at a granular level, identifying unauthorized commands, protocol abuse, and adversary techniques that evade traditional

security tools. It also captures and maintains a baseline of normal OT network behavior, enabling the detection of configuration changes, unexpected system modifications, and emerging threats.

OT Watch provides expert-led threat hunting, ensuring real-time visibility and rapid containment of adversary activity. With threat detection and hunting informed by real-world adversary tactics from WorldView Threat Intelligence, Dragos helps organizations eliminate blind spots, detect threats early, and maintain the integrity of their industrial environments.





## Secure Remote Access

65 percent of organizations Dragos assessed had insecure remote access conditions related to configurations, unpatched systems, and poor network architecture tied to remote access appliances and applications.

Any persistent remote connection is a potential entry point. State-sponsored threat groups, hackers, and ransomware groups routinely exploited vulnerabilities and misconfigurations in remote access points.

Secure remote access allows trusted users and vendors to connect to OT environments without creating persistent vulnerabilities. Remote access should be tightly controlled, logged, and used only when necessary.



**STEP 1**  
Reduce External  
Connections from High-  
Risk Exposure Points



**STEP 2**  
Implement Access  
Restrictions on Targeted  
Points of Entry



**STEP 3**  
Deploy Real-Time  
Access & Network  
Monitoring

**The Dragos 2025 OT/ICS Cybersecurity Report shares insights on vulnerabilities that are actively exploited by adversaries and need to be addressed now. The examples below highlight some of the high-risk vulnerabilities exploited in 2024 based on the “Now, Next, Never” vulnerability management framework and would have been identified as vulnerabilities your organizations should address immediately or “Now.”**



## Access Control & Monitoring: VOLZITE Threat Group

The VOLTZITE threat group demonstrates how adversaries exploit remote access weaknesses to infiltrate OT environments, bypass authentication controls, and pivot between IT and OT networks. Understanding these tactics is essential for strengthening defenses, limiting unauthorized access, and detecting malicious activity before it disrupts operations.

Control Area	Secure Configuration	VOLTZITE Techniques	Actions
<b>Remote Access Points</b>	Remote connections restricted to pre-approved users; VPNs hardened with MFA.	Exploitation of unpatched VPN vulnerabilities and compromised RDP sessions to gain initial access.	Enforce strict patching cycles for remote access points, restrict VPN/RDP access to known IPs, and monitor failed login attempts.
<b>User Authentication &amp; Privileges</b>	Unique accounts per user, least privilege access model, and admin-only RDP access.	Use of stolen credentials to bypass authentication controls and establish persistence.	Implement MFA and detect anomalous access patterns via behavioral analytics.
<b>Network Segmentation &amp; Isolation</b>	IT-OT segmentation is enforced, jump servers are required for access to critical OT systems, and there are no direct internet-facing ICS assets.	Adversaries pivot from IT to OT using misconfigured jump servers or exposed remote access tunnels.	Monitor east-west traffic, restrict IT-OT cross-traffic.
<b>Real-Time Session Monitoring</b>	Remote access sessions logged, recorded, and continuously monitored for anomalies.	Live session hijacking, use of LOTL techniques to disguise malicious commands in regular admin traffic.	Deploy anomaly detection to flag suspicious command execution.
<b>Access Logging &amp; Alerting</b>	Centralized logging (SIEM) for all remote access events, real-time alerting on privilege escalation.	Attackers disable logging mechanisms or inject false authentication records.	Enforce logs and deploy real-time checks on authentication systems.

## How Dragos Can Help

We help organizations detect and respond to threats that exploit secure remote access into OT environments.

The Dragos Platform continuously monitors for unauthorized connections, abnormal authentication attempts, and adversary techniques such as VPN exploitation, brute-force attacks, and session hijacking. With

deep packet inspection and ICS protocol awareness, Dragos identifies threats that evade traditional IT security tools.

OT Watch enhances this visibility with expert-led threat hunting, ensuring rapid detection and containment of remote access compromises. By integrating advanced threat intelligence from WorldView, organizations can stay ahead of emerging attack methods, reducing the risk of adversaries using remote access as a foothold into industrial systems.



## Take a Risk-Based Approach to Vulnerability Management

Adversaries actively track OEM vulnerability disclosures and rapidly exploit newly exposed OT weaknesses. Security teams must prioritize vulnerabilities that adversaries are actively exploiting and use compensating controls where patching isn't an option.

Patching OT systems is not as simple as updating IT endpoints. Many critical ICS assets cannot be taken offline without disrupting production. This makes the traditional “patch everything” approaches impractical.

Risk-based vulnerability management allows organizations to focus on the vulnerabilities that matter, rather than applying patches indiscriminately. Where patching isn't feasible, apply alternative mitigations like network segmentation, firewall rules, and access restrictions.

**STEP 1**  
Implement “Now, Next, Never” Vulnerability Prioritization


**STEP 2**  
Integrate Vulnerability Management with Threat Intelligence

**STEP 3**  
Test Your Resilience with Vulnerability Assessments



**The Dragos 2025 OT/ICS Cybersecurity Report shares our risk-based approach to vulnerability management, helping defenders move beyond infeasible patching lifecycles. The vulnerabilities described in the report are actively exploited, meaning that mitigation efforts should be prioritized.**

### Actively Exploited Vulnerabilities

The “Now, Next, Never” Framework help organizations prioritize vulnerabilities based on real-world risks rather than traditional patching used in IT. This approach ensures that security teams focus on vulnerabilities that matter most while maintaining system stability.

Priority	CVEs & Risks	Mitigation Actions
 NOW (Requires immediate mitigation due to active exploitation)	CVE-2020-3259, CVE-2023-20269 (VPN appliances targeted by VOLTZITE for initial access)	<ul style="list-style-type: none"><li>• Apply available patches immediately.</li><li>• Implement MFA for remote access.</li><li>• Monitor VPN for unauthorized attempts.</li></ul>
	CVE-2023-23397 (Microsoft Outlook UNC Path Injection, used in GRAPHITE campaigns)	<ul style="list-style-type: none"><li>• Block outbound SMB traffic.</li><li>• Apply Microsoft’s official patch.</li><li>• Conduct phishing awareness training.</li></ul>
	CVE-2022-3236, CVE-2022-1040 (Sophos Firewall exploits leveraged by BAUXITE)	<ul style="list-style-type: none"><li>• Apply patches and update firewall configurations.</li><li>• Restrict admin privileges to trusted sources.</li><li>• Monitor for unauthorized configuration changes.</li></ul>

## Actively Exploited Vulnerabilities (continued)

Priority	CVEs & Risks	Mitigation Actions
 NEXT (May become weaponized soon, requires proactive defenses)	SOHO router vulnerabilities exploited by VOLTZITE for persistent access	<ul style="list-style-type: none"> <li>• Segment OT and IT networks to prevent lateral movement.</li> <li>• Disable unnecessary services on routers.</li> <li>• Monitor for unusual outbound traffic.</li> </ul>
	Weak SSH credentials in industrial devices (BAUXITE's Unitronics PLC attack, default pass: 1111)	<ul style="list-style-type: none"> <li>• Require complex passwords and disable default credentials.</li> <li>• Implement rate-limiting for SSH login attempts.</li> <li>• Monitor failed login attempts for brute-force attacks.</li> </ul>
 NEVER (Minimal risk to OT or infeasible attack paths)	Vulnerabilities in non-internet-exposed devices with no known exploits	<ul style="list-style-type: none"> <li>• Deprioritize patching unless operationally required.</li> <li>• Focus resources on threats with confirmed exploitation.</li> </ul>

## How Dragos Can Help

Effective vulnerability management in OT environments requires more than just patching – it demands threat-driven prioritization, expertise in impacts on OT, and continuous asset visibility.

- The Dragos Platform helps organizations identify high-risk vulnerabilities in OT assets, map them to real-world adversary behaviors, and detect early signs of exploitation. Using the Now, Next, Never approach, customers can identify and mitigate high-risk vulnerabilities with ease.

- With WorldView Threat Intelligence, defenders gain insights into which vulnerabilities adversaries are actively targeting, enabling smarter risk-based vulnerability management strategies.
- OT Watch provides expert-driven monitoring to detect exploitation attempts in real-time.
- Dragos Professional Services help organizations assess and harden their environments against known attack vectors.

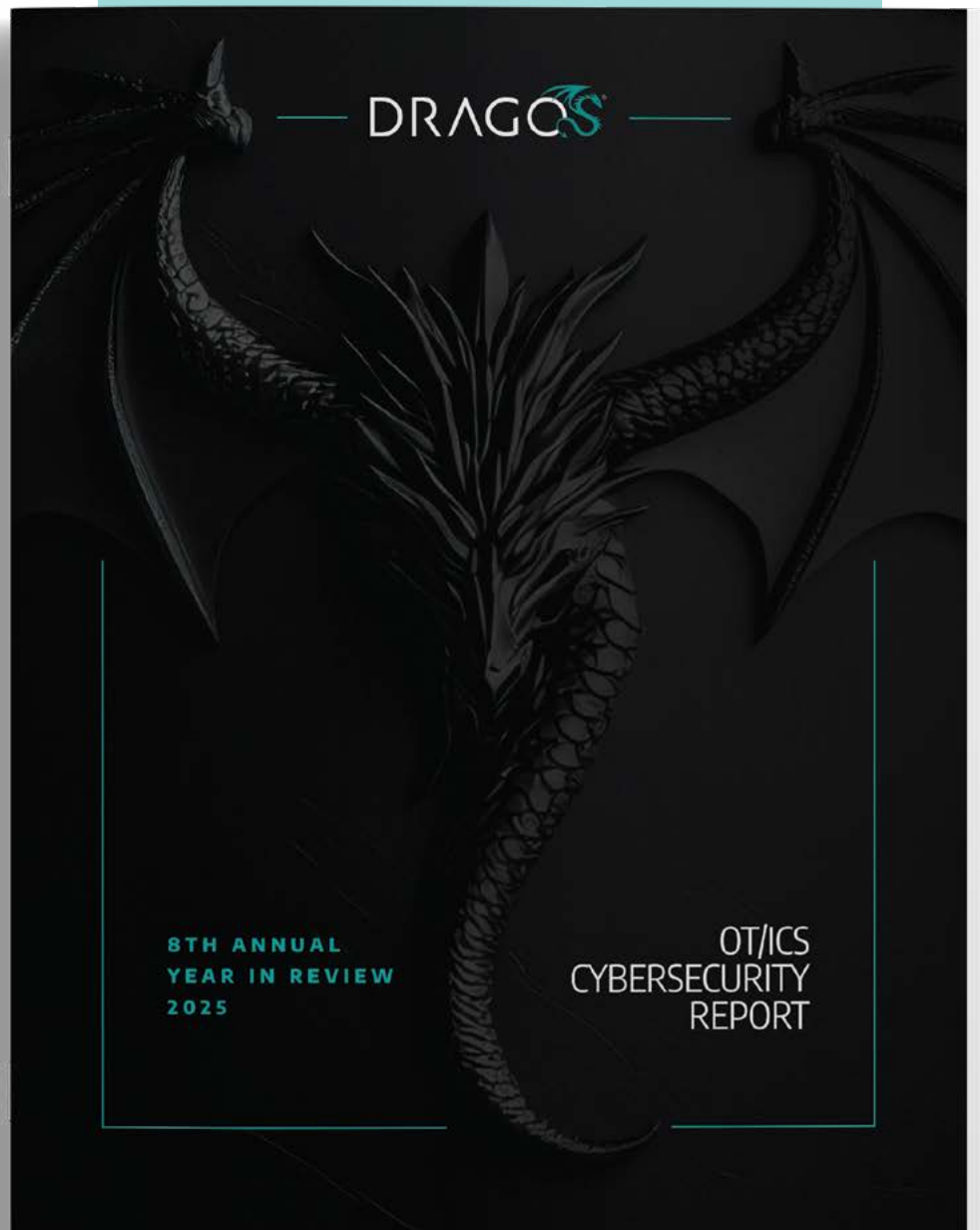
This proactive approach to vulnerabilities reduces risk, minimizes operational disruption, and strengthens resilience against evolving threats.

# Ready to Dive Deeper?

The insights we've covered in this action guide offer a glimpse of the technical depth and real-world threat intelligence available in the Dragos 2025 OT/ICS Cybersecurity Report. This report is built from frontline incident response, adversary tracking, and deep OT threat intelligence, delivering actionable guidance to help industrial defenders strengthen their security posture.

OT cyber threats are evolving – and defenders need real intelligence, not just theoretical guidance. Whether you are securing power grids, oil and gas rigs, manufacturing plants, or transportation systems, this report equips your team with the technical details, threat hunting best practices, and mitigation strategies needed to stay ahead of adversaries.

Take your OT cybersecurity strategy to the next level of defense and resilience. Download the full 2025 OT/ICS Cybersecurity Report at: [dragos.com/ot-cybersecurity-year-in-review](https://dragos.com/ot-cybersecurity-year-in-review).





Dragos is an industrial (OT/ICS) cybersecurity company on a mission to safeguard civilization.

Dragos is privately held and headquartered in the Washington, D.C. area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

[Request a Demo](#)

[Contact Us](#)