DRAGOS

WHITEPAPER

The Vital Role of xOT-Native Network Visibility and Security Monitoring

The Dragos Platform: Built for Extended Operational Technology (xOT) Environments.

Table of Contents

Executive Summary

The extended operational technology (xOT) environments that power civilization's critical infrastructure face a fundamental shift in the threat landscape. Adversaries are no longer content to gain access and wait. They are actively mapping control loops, studying how industrial processes work, and building the capability for operational disruption.

The Dragos 2026 OT Cybersecurity Year in Review documents this shift. Protecting these environments demands OT-native technology. IT security tools do not understand xOT protocols, cannot safely operate in OT networks, and were not designed for environments where the wrong action can stop a turbine or take a substation offline.

This paper explains why xOT-native network visibility and security monitoring is foundational, how the Dragos Platform addresses these demands in alignment with the SANS 5 Critical Controls for ICS Cybersecurity, and what it takes to move from simply having visibility tools to detecting and responding to threats.

26+

Named OT-specific threat groups tracked by Dragos Intelligence

119

Ransomware groups targeting industrial organizations in 2025 — up 49% YoY

3,300+

Industrial organizations impacted by ransomware in 2025

Key Finding

IT security practices do not translate to OT. Legacy technology, proprietary protocols, and 100% uptime requirements demand purpose-built, OT-native approaches — not IT tools adapted for operational environments.

The 2026 xOT Threat Landscape

The Dragos Intelligence Fabric, built from over a decade of OT-specific telemetry, adversary research, and incident response, reveals a consistent and urgent pattern: threat groups are gaining access to industrial environments and positioning for operational impact, but most organizations lack the visibility to detect it.

From Reconnaissance to Operational Disruption

The 2026 Year in Review documents a structural shift: coordinated threat groups are advancing from isolated device targeting to mapping entire industrial control systems.

- KAMACITE systematically mapped control loops across critical infrastructure throughout 2025.
- ELECTRUM targeted distributed energy systems with deliberate attempts to affect operational assets.
- Three new threat groups emerged during the year.

The absence of immediate disruption is no longer a sign of safety. Reconnaissance and establishing a beachhead often precede action by months. Living off the land (LOTL) techniques make these adversaries particularly difficult to detect — they blend malicious activity with normal xOT operations using native protocols and legitimate engineering workflows. Only OT-native behavioral analytics mapped to confirmed adversary TTPs can reliably distinguish an attacker from an engineer.

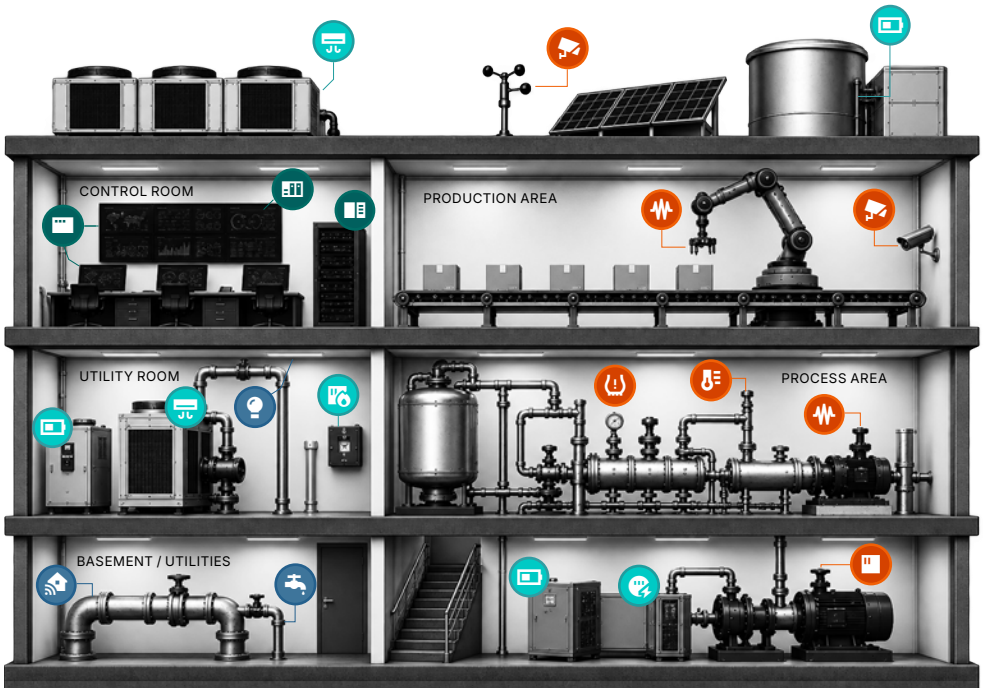
The xOT Visibility Crisis

Across incident response cases, assessments, and platform deployments, a single failure pattern repeats: organizations discover they have been compromised only after something in a physical process behaves abnormally. By then, adversaries have already achieved reconnaissance, lateral movement, and in many cases control loop mapping.

The root cause is a visibility gap. Most OT networks have limited visibility and poor situational awareness. Legacy equipment operates with architectures that were never designed with security monitoring in mind. Even organizations with security tools in place frequently have those tools deployed only at the IT/OT boundary — missing everything happening south of the firewall where the most critical assets operate.

Manufacturing Plant - OT, BMS, IoT & IIoT Devices

Connected Operations.
Smarter Decisions.
Safer Facilities.



IoT DEVICES

- Smart Thermostat
- Smart Lighting
- Leak Detection Sensor

BMS DEVICES

- BMS Controller
- HVAC Controller
- Fire Alarm Panel
- Lighting Control
- Energy Meter

OT DEVICES

- Programmable Logic Controller
- Human Machine Interface
- Distributed Control System

IIoT DEVICES

- Vibration Sensor
- Temperature Sensor
- Predictive Maintenance Sensor
- Flow Sensor
- Security Camera

2026 YIR Finding

Threat groups are gaining access to industrial environments and positioning for operational impact, but in most cases, compromise becomes visible only after something in the process behaves abnormally. Many organizations lack the visibility to detect reconnaissance, lateral movement, and control loop mapping before adversaries achieve their objectives.

Unique Challenges in Monitoring OT Environments

01

OT Protocols Are Fundamentally Different from IT

IT networks rely on widely understood protocols such as HTTP/S, DNS, and RPC. OT environments run hundreds of vendor-specific application protocols: Modbus, BACnet, OPC-UA, CIP, CodeSys, and dozens of proprietary variants. These protocols carry the actual machine commands that run industrial equipment. Security tools that do not understand them create the visibility gaps adversaries actively exploit.

Understanding these protocols is not optional. The system commands embedded in xOT protocol traffic are exactly what attackers use to manipulate equipment. Without protocol-native visibility, defenders cannot tell the difference between normal engineering activity and an attacker preparing for operational disruption.

02

The Extended OT (xOT) Environment

The attack surface extends beyond traditional OT. Modern operational environments include IT infrastructure, IoT devices, edge systems, and IIoT sensors — any system whose failure influences a physical process or drives a high-impact operational outcome. Dragos defines this as the extended OT (xOT) environment.

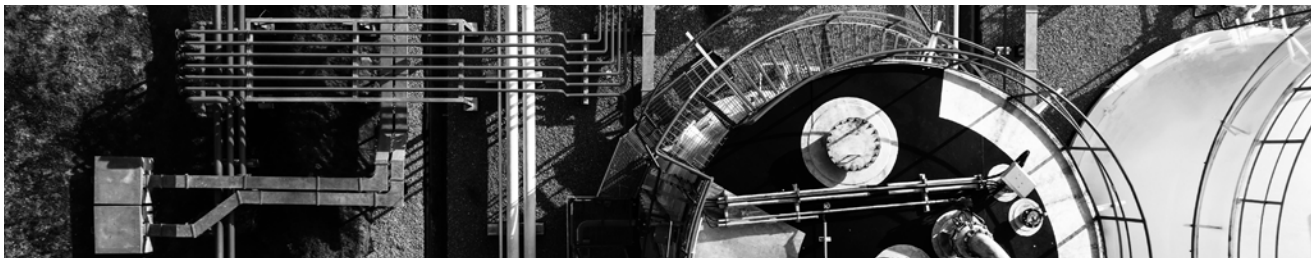
xOT is not a device category — it is defined by operational influence. A building HVAC system that maintains manufacturing conditions is part of the xOT environment. A cloud analytics platform collecting historical data is not. This distinction matters for security: defenders must protect systems based on operational dependency, not device classification.

03

The OT Availability Imperative

OT environments must operate continuously. When systems are down, electricity does not flow, oil is not refined, goods are not manufactured. The goal is 100% uptime with carefully planned maintenance windows — a standard that directly conflicts with how IT security typically responds to vulnerabilities and incidents.

Any monitoring approach that adds unexpected network traffic, queries devices aggressively, or requires system restarts is incompatible with xOT operations. Security tools must be purpose-built for OT, and capable of providing operational alternatives to immediate patching when vulnerabilities are found.



The SANS 5 Critical Controls for ICS Cybersecurity

SANS developed a strategic, OT-specific framework widely adopted by regulators across the world. Dragos finds these five controls to be an invaluable distillation of what effective xOT security requires. The Dragos Platform and Expert Services address all five controls.

ICS Incident Response Plan
Have an operations-informed incident response plan with a focus on system integrity and recovery capabilities during an attack.

Defensible Architecture
Design architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, and process-communication enforcement.

xOT Visibility & Monitoring
Enable continuous network security monitoring of the xOT environment using protocol-aware toolsets and system of systems interaction analysis capabilities.

Secure Remote Access
Identify all remote access points and allowed destination environments and implement on-demand access and multi-factor authentication (MFA) where possible.

Risk-Based Vulnerability Management
Understand the cyber digital controls in place and device operating conditions to make risk-based vulnerability management decisions regarding your OT environment.

The Regulatory Mandate for xOT Network Monitoring

xOT network visibility is no longer solely a security best practice — it is increasingly a regulatory requirement. Organizations operating critical infrastructure face a growing body of mandates that explicitly require continuous monitoring, asset inventory, incident response capability, and demonstrable security controls. Failure to meet these requirements carries financial penalties, operational restrictions, and reputational consequences.

FRAMEWORK	OT MONITORING REQUIREMENT
NERC CIP	Mandates continuous electronic security perimeter monitoring, incident response plans, and vulnerability management for bulk electric system assets.
NIS2 (EU)	Requires essential entities — energy, water, manufacturing, transport — to implement continuous network monitoring, incident detection, and reporting obligations.
TSA Pipeline Directives	Mandates continuous OT network monitoring, incident response plans, and architecture reviews for critical pipeline operators.
IEC 62443	Defines security levels and zones for industrial automation systems, requiring ongoing monitoring, anomaly detection, and network segmentation validation.
NIST SP 800-82	Guidance for securing ICS environments, including requirements for asset inventory, continuous monitoring, and risk-based vulnerability management.

The Dragos Platform is built to support compliance with these frameworks. Continuous passive monitoring satisfies regulatory requirements for network evidence retention. Asset inventory satisfies NERC CIP and NIS2 requirements for critical asset documentation. Vulnerability management with OT-corrected scoring supports NIST SP 800-82 and IEC 62443 requirements. Beyond satisfying checkboxes, OT-native monitoring transforms compliance from a burden into a security outcome.

The Dragos Intelligence Fabric

Every capability in the Dragos Platform is powered by the Dragos Intelligence Fabric — the living knowledge engine behind Dragos. It is the codification of over a decade of OT-specific telemetry, asset and protocol research, adversary research, vulnerability data, and frontline practitioner expertise into a continuously updating loop that gives defenders the right context to act fast and get it right.

Five Interconnected Elements

01
Data

Over 5 petabytes of daily xOT telemetry, plus more than a decade of adversary research and incident response drawn exclusively from operational environments. The largest xOT/ICS security dataset in the industry.

02
People

Adversary hunters, intelligence analysts, incident responders, and assessment experts, all operating against a shared, continuously updated adversary model informed by what they observe in the field.

03
Partnerships

Relationships with government agencies and intelligence communities that surface early signals and validate findings beyond what any single organization can observe.

04
Systems

The Dragos Platform, OT Watch Complete, and Neighborhood Keeper feed telemetry back in, stress-testing assumptions at scale and triggering updates when something diverges.

05
AI

Dragos EmberAI, built on this unmatched dataset, helps analysts surface and act on new insights faster.

NEIGHBORHOOD KEEPER

Shares anonymized telemetry across participants, surfacing validated xOT threats in peer environments through Trusted Insight Alerts for earlier, higher-confidence detection.

Value of xOT-Native Monitoring: Seven Core Principles

01

Do No Harm — Non-Invasive Monitoring

IT discovery tools can be aggressive — pinging devices, flooding segments with traffic. OT environments are sensitive to any unexpected network behavior. The Dragos Platform operates in an xOT-safe mode, never making tradeoffs between operational resilience and security.

02

Complete Asset Visibility Across the xOT Environment

The Dragos Platform builds and continuously updates asset inventory across all device types — OT, IT, IoT, and IIoT — operating deep within the OT environment at Purdue Model Levels 1 through 3.5. Asset discovery uses three complementary methods:

- Passive monitoring across 600+ industrial protocols as the foundation.
- Active Collection for segmented or legacy environments where passive methods leave gaps.
- Data import from engineering configuration files that neither passive nor active collection can reach.

3–6%

"Now" — Requires immediate action. Address urgently.

~68%

"Next" — Network exploitable, no direct operational impact. Mitigate through monitoring, segmentation, MFA.

~29%

"Never" — No active exploitation path. Monitor for signs of exploitation only.

03

Deep Network Visibility — xOT Protocol Intelligence

xOT network traffic carries commands to change device settings, configure equipment, and control physical processes. The Platform performs Deep Packet Inspection (DPI) on hundreds of unique OT protocols, logging key activities, function codes, and system commands. This data supports investigation of both security events and operational issues — delivering value to operations teams and security teams alike.

04

Practical OT Vulnerability Management

CVSS scores were designed for IT and can be inaccurate in OT context. A vulnerability with a low IT-centric CVSS score can knock a factory floor offline. Conversely, a high CVSS finding in OT may be "insecure by design" with no real operational exposure. The Dragos Platform corrects for this with OT-enriched scoring and the "Now, Next, Never" prioritization framework.

05

Intelligence-Driven Threat Detection

Generic anomaly detection creates alert fatigue without context. Dragos addresses this with four detection methodologies, all continuously updated through Knowledge Packs delivered weekly:

- Modeling Detections — mathematical anomaly detection defining normal behavior and measuring deviations.
- Configuration Detections — monitor changes to device configurations against known-good architecture.
- Indicators of Compromise (IOCs) — match specific evidence of security incidents to known malicious infrastructure.
- Behavioral Threat Detections — codify adversary tradecraft (TTPs) to detect threats regardless of specific tools or infrastructure.

Layered above these four: Composite Detections correlate multiple atomic detections across time and data sources into a single analyst-ready narrative, surfacing coordinated campaigns and significantly reducing alert volume.

06

Process Insights and Root Cause Analysis

Cyber threats are not the only disruptor of industrial operations. Misconfigurations, network faults, equipment errors, and process anomalies all impact production. The Platform's detailed monitoring and forensic logging helps operations teams identify root causes of both security and operational problems without shutting systems down.

07

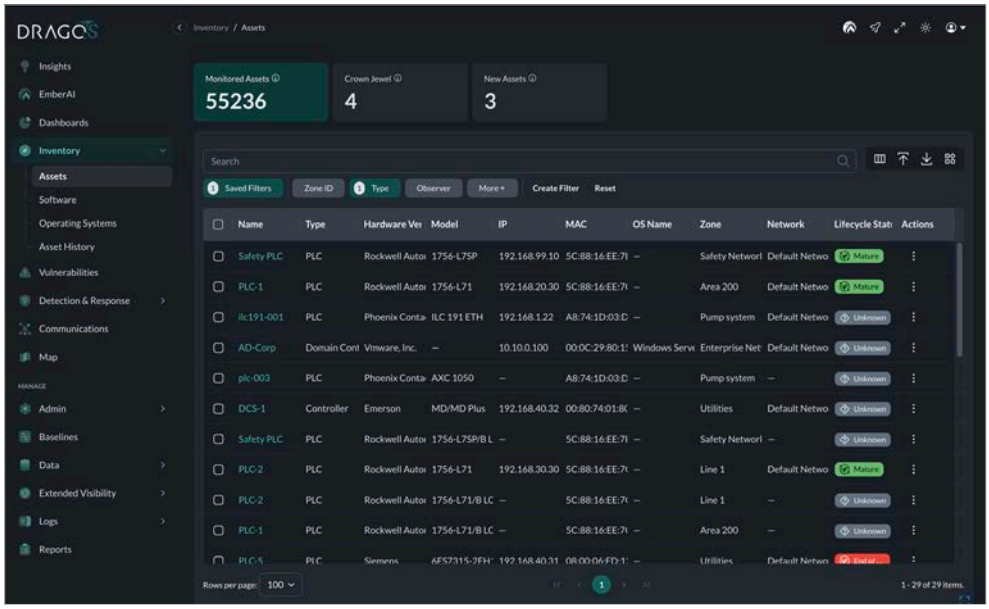
Integration with IT Security Operations

xOT security cannot operate in isolation. The Dragos Platform connects into existing security operations infrastructure: SIEMs like Splunk, Fortinet, and CrowdStrike; firewalls with asset inventory-driven policy creation; EDR via CrowdStrike for cross-boundary telemetry; and workflow platforms for full integration across vulnerability management and incident response.

Dragos Platform: Core Capabilities

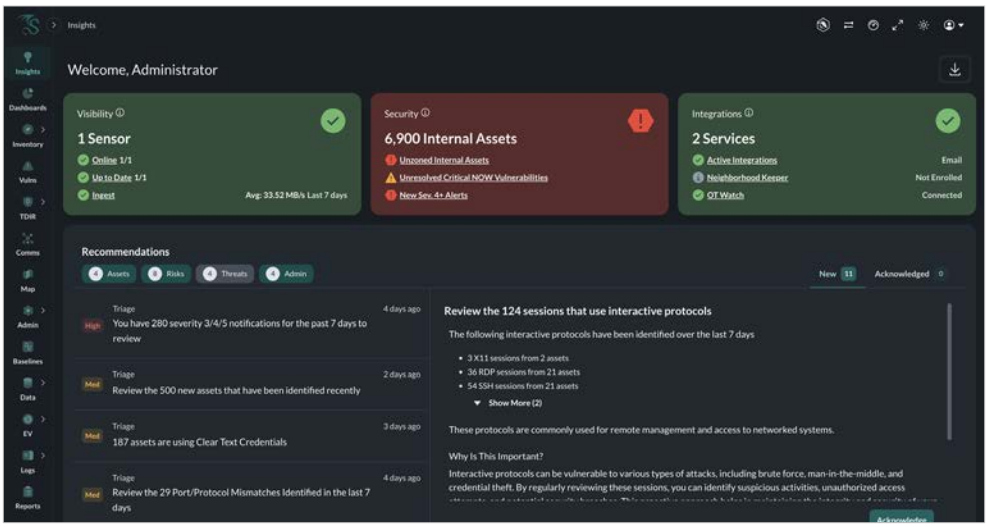
Asset Visibility and Inventory

The Platform automatically discovers and continuously updates inventory for all OT, IT, IoT, and IIoT devices. Device profiles include vendor, model, OS, firmware version, and deep context. A timeline analysis feature gives security teams a chronological view of network changes for investigation and change detection.



xOT Network Visibility and Monitoring

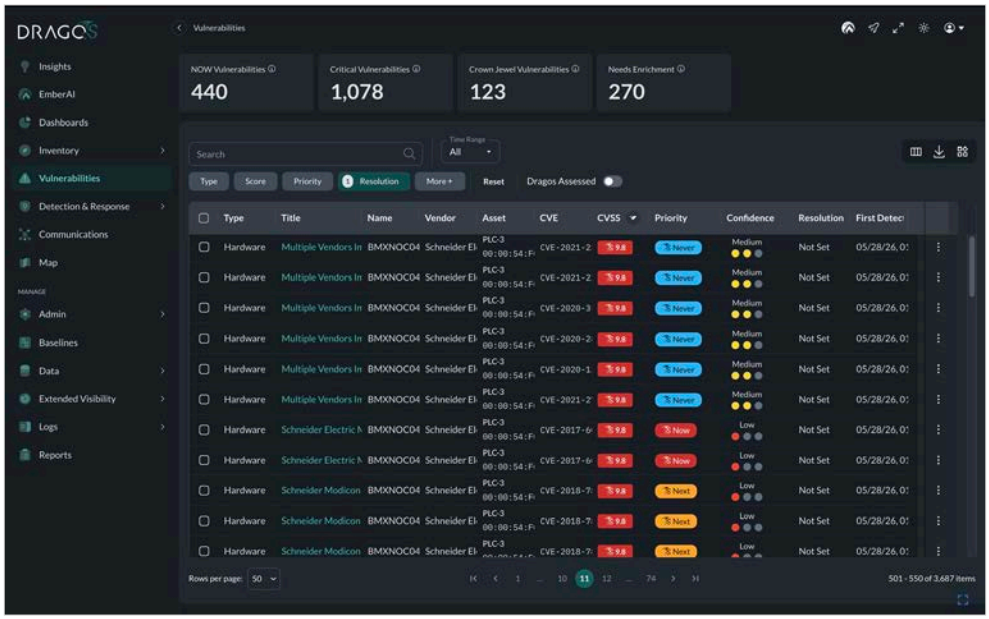
Comprehensive visibility means understanding how assets communicate and behave, not just what exists. The Platform monitors and logs OEM system commands, baselines communication patterns, and provides a correlation engine to detect combinations of anomalies. Custom rules, dashboards, and data export in common formats support both security investigations and operational diagnostics.



Dragos Platform: Core Capabilities

Segmentation Validation

Network diagrams show intended architecture. Dragos shows actual architecture — and the gaps between them. Segmentation Validation analyzes firewall, router, and switch configuration files to map real-world network topologies, identify cross-zone communication paths that should not exist, and detect segmentation drift over time.



OT Cyber Threat Intelligence and Knowledge Packs

Dragos fields the largest civilian threat intelligence operation focused on xOT. This intelligence ships to the Dragos Platform via Knowledge Packs — regular updates including new IOCs, CVEs, threat detections, and playbooks. Defenses evolve with the threat landscape automatically, without manual tuning.

Full finished threat intelligence is also available via Dragos WorldView — the only threat intelligence built exclusively for xOT — by subscription. WorldView gives IT security teams OT adversary context for SIEMs and TIPs, provides executives with strategic reporting, and gives advanced teams complete TTP mapping for threat hunting and IR readiness.

Dragos EmberAI

Dragos EmberAI is the AI specifically built for xOT. Built on the Dragos Intelligence Fabric, EmberAI activates over a decade of OT-specific telemetry, adversary research across 26+ tracked threat groups, vulnerability analysis, and frontline incident response expertise — making that intelligence immediately accessible to every analyst, regardless of their OT background.

Dragos Platform: Core Capabilities

EMBERAI CAPABILITY	DESCRIPTION
Intelligence-Driven Query Engine	Ask in plain English, get xOT-contextual answers grounded in the Dragos Intelligence Fabric.
Contextual Correlation	Connects assets, vulnerabilities, threat intelligence, and network activity into a unified real-time understanding.
Adversary-Informed Guidance	Detections mapped to known OT threat groups and real attack patterns from the Intelligence Fabric.
Workflow Acceleration	Alert triage, incident summaries, and reporting reduced from hours to minutes.
Continuous Learning	Evolves as new intelligence, telemetry, and field insights flow into the Intelligence Fabric.
Expert-Built OT Skills	Guided, repeatable workflows built and validated by Dragos analysts.

OT Watch Complete: 24/7 Managed Threat Hunting

Many organizations have deployed OT visibility tools but lack the people and expertise to use them effectively. OT Watch Complete is a 24/7 managed xOT threat management service where Dragos experts continuously monitor, hunt, triage, tune, and harden — so security teams get the outcomes of a mature OT security program without building one in-house.

OT Watch Complete delivers: proactive expert-led threat hunting informed by the Dragos Intelligence Fabric; SLA-backed alert triage with only validated findings escalated; continuous platform tuning as the environment evolves; vulnerability reporting with monthly executive summaries; and incident response support when events occur.

Investigation and Response

The Platform accelerates forensic investigations with embedded case management, expert-authored response playbooks, timeline analysis, and Query Focused Datasets. Pre-configured playbooks cover common ICS threat scenarios. Network capture files (PCAP) can be stored for post-event replay and forensic analysis, supporting post-incident reporting for regulators, insurers, and legal counsel.

EXPERT SERVICES

Completing the SANS Framework

OT-native technology addresses SANS Controls 3 and 5 directly — network visibility and monitoring, and risk-based vulnerability management. But Controls 1 and 2 — ICS Incident Response Plan and Defensible Architecture — demand human expertise, structured assessment, and organizational readiness that technology alone cannot deliver. Dragos Expert Services close this gap.

SERVICE	WHAT IT DELIVERS
xOT Cybersecurity Assessment	Expert-led evaluation of network architecture, critical asset protection, and threat detection and response capabilities. Four options from Compromise Assessment to full OT Cybersecurity Assessment.
Segmentation Validation	Continuous analysis of firewall and network device configurations to map actual vs. intended architecture and detect segmentation drift. Supports NERC CIP, IEC 62443, and TSA compliance.
Tabletop Exercises	Structured workshops grounded in actual adversary TTPs and industry-specific scenarios to evaluate and improve incident response plans. Directly addresses SANS Control 1.
Rapid Response Retainer	Pre-established 24/7 access to Dragos OT incident response experts. First contact within one hour; analysis underway within four. Pre-documented environments accelerate containment for Platform customers.
Red Team Services	Network Vulnerability Assessment, Penetration Testing, and Purple Team Exercises conducted by OT security experts using real ICS adversary TTPs — to identify hidden attack paths and validate that defenses actually work.
Dragos WorldView	The only finished threat intelligence built exclusively for xOT. Adversary research, corrected vulnerability analysis, IOCs, and strategic reporting — produced by the largest private ICS/OT threat intelligence team in the industry.

Incident Response Reality

While most organizations have an IT cyber incident response plan, few have plans for operational environments. Incidents impacting power plants, substations, pipelines, and manufacturing floors have unique requirements. SANS ICS Critical Control #1 exists for exactly this reason: proactively identify the people, systems, and resources needed before the worst day arrives.

Platform Deployment: xOT Visibility from the Ground Up

Where To Monitor

Dragos Sensors deploy at key aggregation points throughout the xOT network, from Level 1 (Basic Control) through Level 3 (Operations Systems) and at the IT/OT boundary (Level 3.5) of the Purdue Model. This ensures visibility into the most critical systems, not just the network edge. Sensors use network spans, port mirroring, or traffic aggregators to capture network traffic passively.

Passive First, Active When Needed

Passive monitoring is the foundation. When passive methods leave gaps, Safe Active Collection fills them with read-only queries designed specifically for xOT environments. SiteStores aggregate sensor data on-premises or in the cloud, and can be deployed virtually on approved hardware models via ESXi and HyperV.

Integration with IT Security Operations

The Platform connects into existing security infrastructure with no rip-and-replace required:

- SIEMs (Splunk, Fortinet, CrowdStrike) — xOT-enriched alerts and telemetry flow into existing security operations workflows.
- Firewalls — asset inventories drive policy creation; threat-triggered isolation capabilities contain active threats.
- EDR (CrowdStrike) — additional threat telemetry across the IT/OT boundary accelerates detection and response.
- ServiceNow — xOT asset discovery and vulnerability prioritization improve workflow decisions and overall efficiency.

Getting Started: A Practical Path Forward

Closing the xOT visibility gap does not require a complete program overhaul. Most organizations benefit from a structured, phased approach that builds visibility, validates defenses, and matures detection capability over time.

STEP	ACTION	DRAGOS CAPABILITY
Step 1	Understand your current posture	Compromise Assessment or Architecture Review surfaces existing threats, maps assets and architecture, and identifies the highest-priority gaps before technology deployment begins.
Step 2	Deploy foundational visibility	Dragos Sensors at key aggregation points begin building asset inventory and network baselines immediately. Multi-detection monitoring delivers value from day one.
Step 3	Activate intelligence-driven detection	Knowledge Packs keep detections current. EmberAI gives every analyst immediate access to OT-contextual intelligence. The Insights Hub connects alerts to action.
Step 4	Build readiness for response	Tabletop Exercise validates the incident response plan against real OT adversary scenarios. Rapid Response Retainer ensures expert support is pre-established and ready when needed.
Step 5	Sustain and mature	OT Watch Complete provides 24/7 coverage, ongoing platform tuning, and expert-led threat hunting — so the program keeps improving without requiring additional internal resource dedication.

Conclusion

Threat actors targeting OT environments are no longer running reconnaissance operations. They are actively mapping industrial control systems, learning physical processes, and building the capability for operational disruption. The 2026 Dragos OT Cybersecurity Year in Review documents this structural shift and the OT visibility crisis that leaves most organizations unable to detect it before something breaks.

The SANS 5 Critical Controls for ICS Cybersecurity provide a clear, actionable framework. The Dragos Platform implements Controls 3 and 5 directly with xOT-native network visibility and monitoring, and risk-based vulnerability management with “Now, Next, Never” prioritization. Dragos Expert Services address Controls 1 and 2 — defensible architecture and ICS incident response readiness. Together, they close the loop on what effective xOT security requires.

Regulatory mandates across NERC CIP, NIS2, TSA, IEC 62443, and NIST SP 800-82 are making continuous xOT network monitoring a compliance requirement. Dragos EmberAI makes the Dragos Intelligence Fabric accessible to every analyst, regardless of OT experience. Neighborhood Keeper turns the customer community into a collective defense network. Named a Leader in the 2026 Gartner Magic Quadrant for CPS Protection Platforms for the second consecutive year, the Dragos Platform is trusted by global organizations.

In OT, the cost of a delayed or incorrect decision is a disruption event that can directly impact society. OT-native security is not optional. It is how critical infrastructure stays safe.

About Dragos

Dragos is the world's leading OT cybersecurity firm headquartered in Washington DC, USA area with offices around the world. It provides the most effective OT cybersecurity technology for industrial and critical infrastructure to deliver on our global mission: safeguarding civilization. The Dragos Platform provides visibility and monitoring of OT environments for asset identification, vulnerability management, and threat detection with continuous insights generated by the industry's most experienced OT threat intelligence and services team. Dragos protects customers across the range of operational sectors, including electric, oil & gas, data centers, manufacturing, water, transportation, mining, and government.

Learn more: dragos.com