DRAGOS

SOLUTION BRIEF

Dragos OT Cyber Services

Strengthen your OT security posture with an extensive portfolio of proactive assessments and incident response services.

Dragos OT Cyber Services

Strengthen your OT security posture with an extensive portfolio of proactive assessments and incident response services.

Overview

Dragos offers an extensive portfolio of operational technology (OT) proactive assessments and incident response services, delivered by OT security experts and powered by the Dragos Intelligence Fabric. We help organizations identify vulnerabilities and other potential security issues, test security controls, improve response readiness, and mitigate threats. With expert-led architecture reviews, penetration testing, tabletop exercises, and incident response services, Dragos strengthens your organization's OT security posture and supports operational resilience and regulatory compliance.

THE CHALLENGE

You Can't Defend Without Full Situational Awareness

Adversaries targeting OT environments understand ICS protocols, physical processes, and the specific weaknesses of operational networks — and they're accelerating attacks with AI, automating reconnaissance and compressing the time between discovery and exploitation. Point solutions handled by separate vendors produce findings that can't be deduplicated, contextualized, prioritized, or acted on together. Most organizations don't know which gap to close first, whether their defenses would hold under a real attack, or whether their team would recognize it in progress.

The Dragos Solution

- **Rapid Response Retainer**
- **OT Incident Response Services**
- **IRP Workshop**
- **Architecture Review Suite**
- **Network Vulnerability Assessment**
- **Network Penetration Test**
- **Purple Team Exercise**
- **Tabletop Exercises**

THE SOLUTION

Services Details

Service	The Problem It Solves	Description & Key Deliverables
Rapid Response Retainer	Contracting and environment discovery consume the opening days of an incident while the adversary keeps moving.	24/7 access to OT cybersecurity experts with contractual and documentation hurdles cleared in advance. Includes an onboarding workshop, flexible retainer hours usable for proactive services, and priority response times for Dragos Platform customers. Four tiers: Essential (80 hours), Standard (160), Enhanced (240), and Custom (320+). Deliverables: pre-cleared work authorization, onboarding workshop covering incident declaration, your xOT environment, and essential IRP review, plus any required GRC or safety training for customer systems (at customer expense).
OT Incident Response Services	Responders without OT experience recommend containment steps that can halt production or create safety risks.	Rapid remote and onsite response for OT cyber incidents, including forensic investigation and containment, eradication, and recovery guidance. Deliverables: incident timeline, forensic investigation report, attack analysis, containment and eradication strategies, recovery recommendations, executive debriefs.
IRP Workshop	Response plans written for IT, or never written at all, fail when an OT incident demands different priorities.	A structured session to review, develop, or refine an Incident Response Plan (IRP) using the PICERL framework, with customized scenario playbooks and a roadmap for improving response capabilities. Deliverables: IRP framework, scenario-based playbook guidance, response maturity assessment, best practice recommendations, final summary report.
Architecture Review Suite	Architecture, controls, and compliance posture have never been evaluated together against OT threats.	Evaluations of OT security posture across network architecture, security controls, and regulatory alignment, at four levels matched to program maturity: Compromise Assessment (CA), Architecture Review (AR), Cybersecurity Architecture Design Review (CADR), and OT Cybersecurity Assessment (OTCA). Deliverables: network architecture review, asset inventory assessment, riskprioritized vulnerabilities, topology review, compliance gap analysis, strategic and tactical recommendations.
Network Vulnerability Assessment	Generic IT scanners can't evaluate OT devices safely, so teams work from an incomplete picture of exposure.	A security evaluation that identifies vulnerabilities in OT networks without active exploitation. Reviews configurations, detects weaknesses, and provides prioritized remediation steps. Deliverables: vulnerability findings report, prioritized remediation recommendations, asset security review, security posture improvement plan.
Network Penetration Test	Controls look right on paper but have never faced a real adversary pursuing your perations.	An objective-based test in which OT penetration testers pursue the destinations a real adversary would, such as pivoting from the enterprise network to the OT DMZ and into the process control network, with findings framed against the ICS Cyber Kill Chain. Deliverables: findings report, attack timeline, validated vulnerabilities, risk prioritization, security control effectiveness evaluation, mitigation recommendations.
Purple Team Exercise	Detection tools are deployed, but analysts have never hunted a live adversary in their own environment.	A collaborative exercise in which a Dragos penetration tester executes roughly 30-35 adversary techniques while a Dragos incident responder coaches your team through hunting each one with your own tools. Each technique is scored Detected, Partially Detected, or Not Detected and mapped to MITRE ATT&CK. Deliverables: detection capability report with per-technique results and improvement recommendations.
Tabletop Exercises	Coordination breakdowns, unclear authorities, and missing playbooks stay invisible until a real incident exposes them.	Simulated cybersecurity drills tailored to test OT incident response capabilities, available in Standard, Custom, and Executive formats, covering threats like ransomware, unauthorized operator actions, and supply chain attacks. Deliverables: facilitator handbook, master scenario events list, exercise agenda, participant manual, and an After-Action Report with performance ratings for each core response capability.

> The comprehensive OTCA assessment was a game-changer for our mature security program. The threat discovery and IOC sweep components found suspicious activities our existing tools missed. Having all ten assessment modules gave our board complete confidence in our security investments and helped justify additional resources for critical improvements."
>
> *- CISO, Electric Utility Company*

Expert Services Backed By The Dragos Platform

Dragos Platform automates network telemetry collection and analysis for complete asset visibility, behavioral baselines, forensic fidelity, and priority incident response. Available across assessments, threat hunting, and IR engagements.

Dragos Service Engagements have options for physical, virtual, and cloud-delivered Platform components. Any physical hardware deployed is new and can be converted to sale for ongoing monitoring and security.

01

Monitor Traffic

Monitor network traffic with Layer 5 OT/ICS-aware protocol analysis.

02

Identify Assets

Identify assets, networks, and communications.

03

Assess Findings

Document vulnerabilities, threats, and security findings for advanced analysis by our consultants.

Why Dragos OT Cyber Services

01

Dragos OT Expertise

24/7 access to practitioners with frontline OT incident response experience and direct knowledge of 26+ named OT threat groups. Dragos understands operational constraints, process dependencies, and how to respond without breaking the operation.

02

Minimal Operational Burden

Assessments conducted through documentation review, automated data collection, and focused client interviews. Vulnerability assessments identify weaknesses without active exploitation; penetration tests pursue real attack objectives while Platform-powered telemetry collectionstrengthens visibility over weeks, not days.

Why Dragos OT Cyber Services

03

Threat-Informed, Not Checklist-Driven

Findings evaluated against real adversary behaviors Dragos tracks, framed against the ICS Cyber Kill Chain and MITRE ATT&CK. Severity reflects actual threats to your industry, not generic scoring frameworks.

04

Prioritized By Operational Impact

Protection focuses on assets whose failure creates greatest operational risk. Vulnerability findings guided by “Now, Next, Never” triage as research shows only 3-6% require immediate action. Penetration tests pursue destinations real adversaries would target.

05

Platform-Powered Intelligence

Dragos Platform automates network telemetry collection and analysis for complete asset visibility, behavioral baselines, forensic fidelity, and priority incident response. Available across assessments, threat hunting, and IR engagements.

06

Recommendations You Can Act On

Findings include multiple remediation pathways tailored to your maturity level, industry, and operational constraints. Services range from vulnerability assessment and architecture reviews to incident response readiness (IRP workshops, tabletop exercises) and detection validation (purple team exercises).

About Dragos

Dragos delivers xOT cybersecurity for industrial and critical infrastructure, backed by a decade of frontline incident response experience. The Dragos Platform provides asset visibility, continuous monitoring, vulnerability management, and real-time threat detection, all powered by industry-leading intelligence. Dragos protects OT environments globally, including electric, oil and gas, manufacturing, water, and transportation.

Dragos is privately held and headquartered in Hanover, Maryland, operating globally across North America, EMEA, and APAC. Learn more about our technology, services, and threat intelligence offerings: request a demo or contact us.

Learn more: dragos.com