Dragos OT Cyber Services

Dragos offers an extensive portfolio of operational technology (OT) based proactive assessments and incident response services. We help organizations identify vulnerabilities, test security controls, improve response readiness, and mitigate threats. With expert-led architecture reviews, penetration testing, tabletop exercises, and incident response services, Dragos helps to strengthen your organization's OT security, ensuring operational resilience and regulatory compliance.

EXPERT SERVICES BACKED BY THE DRAGOS PLATFORM

Dragos Services engagements use the Dragos Platform to capture, document, and organize data. The Platform:

- Passively monitors network traffic with Layer 7 OT/ICS-aware protocol analysis.
- Identifies assets, networks, and communications.
- Documents vulnerabilities and threats to form the starting point for advanced analysis by our consultants.

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.

Services Summary & Key Deliverables

Deliverable	Description	Key Deliverables
Rapid Response Retainer	Provides 24/7 access to OT cybersecurity experts for rapid incident response. Pre-clear contractual and documentation hurdles that delay engagement. Includes an onboarding workshop, flexible retainer hours, and priority response times. Helps organizations quickly mitigate cyber threats and leverage unused hours for proactive security improvements. Dragos Platform customers get priority response times for IR resources.	Pre-cleared work authorization in case of an incident; Onboarding workshop including how to declare an incident, overview of customer OT environment, review of essential customer IRP; any required GRC or safety training for customer systems (at customer expense)
OT Incident Response Services	Provides rapid response for industrial cyber incidents, offering remote and onsite support. Includes forensic investigation, containment, eradication, and recovery guidance.	Incident timeline, forensic investigation report, attack analysis, containment and eradication strategies, recovery recommendations, executive debriefs.
IRP Workshop	A structured session to review, develop, or refine an Incident Response Plan (IRP). Uses the PICERL framework to ensure organizations are prepared for OT security incidents. Includes customized scenario playbooks and a roadmap for improving response capabilities.	Incident Response Plan framework, scenario-based playbook guidance, response maturity assessment, best practice recommendations, final summary report.

Services Summary & Key Deliverables (continued)

Deliverable	Description	Key Deliverables
Architecture Review Suite	Evaluate your OT security posture by analyzing network architecture, security controls, and regulatory compliance. These assessments identify vulnerabilities, misconfigurations, and security gaps while providing prioritized recommendations to strengthen detection, protection, & response capabilities. Compromise Assessment (CA), Architecture Review (AR), Cybersecurity Architecture Design Review (CADR), and OT Cybersecurity Assessment (OTCA).	Comprehensive network architecture review, asset inventory assessment, risk-prioritized vulnerabilities, topology review, compliance gap analysis, strategic and tactical security recommendations.
Network Vulnerability Assessment	A security evaluation that identifies vulnerabilities in OT networks without active exploitation. Reviews configurations, detects weaknesses, and provides prioritized remediation steps to improve security posture and minimize attack surfaces.	Vulnerability findings report, prioritized remediation recommendations, attack path analysis, asset securityreview, security posture improvement plan.
Network Penetration Test	Simulates real-world cyber attacks on OT environments to evaluate security controls and identify exploitable vulnerabilities. Uses advanced techniques to demonstrate attack paths and assess network resilience, helping organizations strengthen defenses against sophisticated threats.	Penetration test findings report, attack timeline, validated vulnerabilities, risk prioritization, security control effectiveness evaluation, mitigation recommendations.
Threat Baseline	A collaborative workshop to identify credible OT cyber threats scenarios based on real-world incidents. Helps organizations prioritize cybersecurity investments, refine detection strategies, and develop a structured response plan for potential attacks.	Threat briefing pack, prioritized risk scenarios, detection and response strategy recommendations, detailed report with action items.
Tabletop Exercises	Simulated cybersecurity drills tailored to test an organization's OT incident response capabilities. Available in standard and custom formats, these exercises enhance communication, coordination, and preparedness against cyber threats like ransomware, insider threats, and supply chain attacks.	Facilitator handbook, master scenario events list, exercise agenda, participant manual, post-exercise after-action report.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East. Learn more about our technology, services, and threat intelligence offerings: **request a demo** or **contact us**.