Operational Technology (OT) Cybersecurity Assessment

The Dragos Operational Technology (OT) Cybersecurity Assessment provides specific, prioritized guidance to reduce risk and mature your organization's OT cyber defense. Our services evaluate your network and OT security posture, focusing on protection, detection, and response capabilities.

Through documentation reviews and staff interviews, Dragos provides tactical and strategic recommendations to enhance the security of critical industrial control systems (ICS). While each review is tailored to the context of your organization, the process includes key modules designed to identify security gaps and deliver actionable insights.

Strengthen Security Foundation

Through comprehensive evaluation of network architecture, policies, and critical assets, organizations can build a more robust and resilient cybersecurity defense system

Prioritize Critical Asset Protection

By identifying and analyzing crown jewels and their vulnerabilities, organizations can focus resources on protecting what matters most to their operations.

Enhance Threat Response Capabilities

Strategic analysis of data sources and network topology enables organizations to improve their ability to detect and respond to cybersecurity threats.

NETWORK DATA COLLECTION WITH THE DRAGOS PLATFORM

Dragos Architecture Reviews leverage the Dragos Platform for analysis of network telemetry:

- Automates capture and analysis of network traffic that feeds service delivery.
- Allows for weeks of data collection for more complete asset inventories and vulnerability analysis.
- Provides risk-prioritized vulnerabilities, with "now, next, never" guidance.
- Delivers high fidelity evaluation and detailed forensics of any existing compromise or threat in the environment.

Four Assessment Options: Choose According to Cybersecurity Program Maturity

Each component of the OT Cybersecurity Assessment has a specific objective that contributes to the overall understanding of your current state and the advancement of your protective controls. Your OT cybersecurity maturity should guide your choice, with more mature organizations choosing the OT Cybersecurity Assessment (OTCA) option, shown in the table below. You should conduct assessments periodically to evaluate and chart maturity progress.

Objective	Description	Compromise Assessment (CA)	Architecture Review (AR)	Cybersecurity Architecture Design Review (CADR)	OT Cybersecurity Assessment (OTCA)
Program Review	Evaluates cybersecurity policies, roles, and plans to find gaps and improve governance and documentation across the organization.				✓
Collection Management Framework	Maps what security data is collected, stored, and accessed, and defines retention to support full visibility and monitoring.				✓
Crown Jewel Analysis	Identifies and prioritizes critical assets to focus protection on systems whose failure would cause severe operational impact.				✓
Standards & Regulations Review	Checks how well security controls align with standards like TSA pipeline regulations, NIST, ISO, or NERC CIP to assess compliance.			✓	
Sensor Placement	Plans optimal locations for security sensors to ensure full network visibility and detection coverage.		✓	✓	✓
Topology Review	Assesses network design to find security gaps, focusing on segmentation, traffic flow, and architectural risks.		✓	✓	✓
Indicators of Compromise Sweep	Searches for evidence of attacks or suspicious activity by scanning or known threat patterns in system and network data.	✓	✓	✓	✓
Threat Discovery	Uses proactive analysis to detect hidden threats that bypass existing defenses, identifying unknown risks.	✓	✓	✓	✓
Asset Vulnerability Assessment	Identifies weaknesses in systems and devices, ranks risks, and highlights what could be exploited by attackers.	✓	✓	✓	✓
Asset Inventory	Catalogs hardware and software, mapping relationships and documenting each item's role and configuration.	✓	✓	✓	✓

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**.