DRAGOS

SOLUTION BRIEF

Operational Technology (OT) Cybersecurity Assessment

OT Cybersecurity Assessment

The Dragos OT Cybersecurity Assessment provides organizations with specific, prioritized guidance to mature their Operational Technology (OT) cyber defense by evaluating network architecture, critical asset protection, and threat detection and response capabilities. Delivered through documentation reviews, staff interviews, and data collection via the Dragos Platform, each assessment is tailored to the organization's maturity level and operational context.

With four assessment options ranging from Compromise Assessment to the full OT Cybersecurity Assessment, organizations receive actionable, tactical and strategic recommendations that identify security gaps, surface hidden threats, and strengthen defenses without disrupting operations. The outcome is a clear understanding of current security posture and a concrete roadmap to build greater resilience across the xOT environment.

The Challenge

Gaps You Can't See

Most OT security programs have gaps they can't see. Without a structured evaluation by specialists who understand xOT environments, organizations struggle to know which assets are truly critical, where their architecture leaves them exposed, and whether their detection and response capabilities would hold up under a real attack. Generic IT-focused assessments miss what makes OT different: the operational constraints, the process dependencies, and the consequences of getting it wrong.

THE SOLUTION

The Dragos OT Cybersecurity Assessment Solution

THE PROBLEM	HOW THE ASSESSMENT SOLVES IT
✕ **Unknown Weaknesses in Architecture and Policy** Network design, governance documents, and controls have never been evaluated together against OT threats.	✓ **Strengthen the Security Foundation** Evaluation of network architecture, policies, and critical assets shows where the defense holds and where it doesn't.
✕ **Protection Spread Evenly Across Unequal Assets** Resources go everywhere, so the systems that matter most get no more defense than the ones that don't.	✓ **Prioritize Critical Asset Protection** Crown jewel analysis identifies the assets whose failure carries the greatest operational impact, so resources concentrate where they count.
✕ **Blind Spots for Detection and Response** Data sources, sensor coverage, and topology have never been assessed for whether an attack would be detected.	✓ **Improve Threat Detection and Response** Analysis of data sources, sensor placement, and network topology shows what your team can detect today, what it would miss, and where there are areas for improvement.

Four Assessment Options: Choose According to Cybersecurity Program Maturity

Assessment Services

Each component of the OT Cybersecurity Assessment has a specific objective that contributes to the overall understanding of your current state. Your OT cybersecurity maturity should guide your choice, with more mature organizations choosing the OT Cybersecurity Assessment (OTCA) option, shown below.

Objective	Description	Compromise Assessment (CA)	Architecture Review (AR)	Cybersecurity Architecture Design Review (CADR)	OT Cybersecurity Assessment (OTA)
Program Review	Evaluates cybersecurity policies, roles, and plans to find gaps and improve governance and documentation.				✓
Collection Management Framework	Maps what security data is collected, stored, and accessed, and defines retention.				✓
Crown Jewel Analysis	Identifies and prioritizes critical assets to focus protection on systems whose failure would cause severe impact.				✓
Standards & Regulations Review	Checks how well security controls align with standards like TSA pipeline regulations, NIST, ISO, or NERC CIP.			✓	
Sensor Placement	Also known as a Continuous Monitoring Strategy. Plans optimal sensor locations for full visibility and 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 for known threat patterns.	✓	✓	✓	✓
Threat Discovery	Uses proactive analysis to detect hidden threats that bypass existing defenses.	✓	✓	✓	✓
Asset Vulnerability Assessment	Identifies weaknesses in systems and devices, ranks risks, and highlights what could be exploited.	✓	✓	✓	✓
Asset Inventory	Catalogs hardware and software, mapping relationships and documenting each item's role.	✓	✓	✓	✓

What Our Customers Are Saying

“The Dragos OT Cybersecurity Assessment gave us exactly what we needed — a clear picture of our security gaps and a prioritized roadmap to address them. The crown jewel analysis alone transformed how we allocate our security resources. We now focus on protecting what truly matters to our operations rather than trying to secure everything equally.”

- VP of Operations, Global Chemical Manufacturer

WHY DRAGOS

Why Dragos OT Cybersecurity Assessment?

01

OT Expertise

Assessments are performed by practitioners with over a decade of frontline OT incident response experience who understand operational constraints and process dependencies.

02

Threat-Informed, Not Checklist-Driven

Findings are evaluated against the real adversary behaviors Dragos tracks, including 26+ named OT threat groups.

03

Platform-Powered Data Collection

The Dragos Platform automates capture and analysis of network telemetry, producing complete asset inventories and behavioral baselines.

04

Minimal Operational Burden

Delivered through documentation reviews, data collection, and typically no more than two days of client interviews, without disrupting operations.

05

Prioritized By Operational Impact

Vulnerability findings carry “Now, Next, Never” guidance. Dragos research shows only 3-6% of OT vulnerabilities require immediate action.

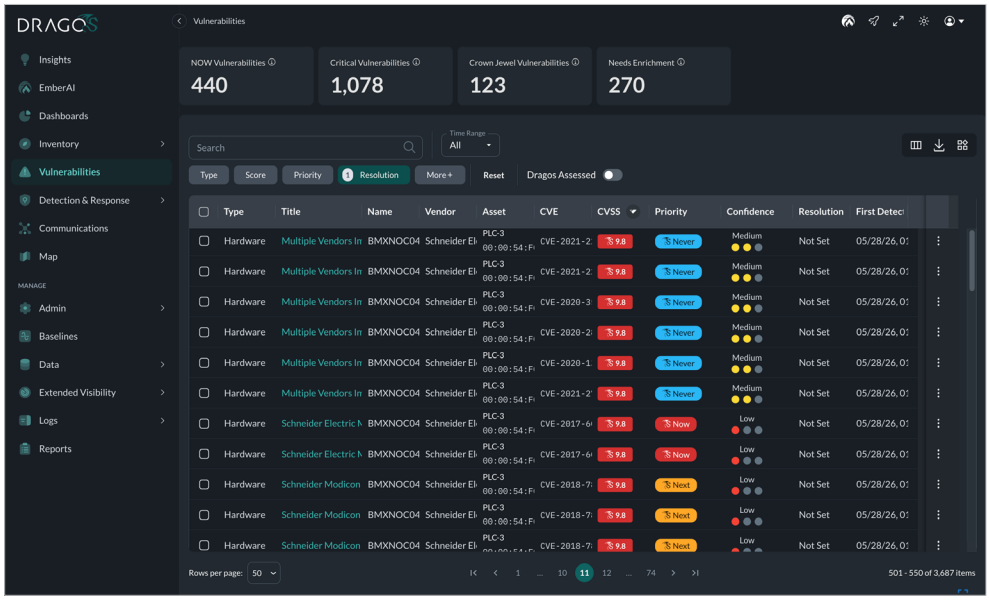
06

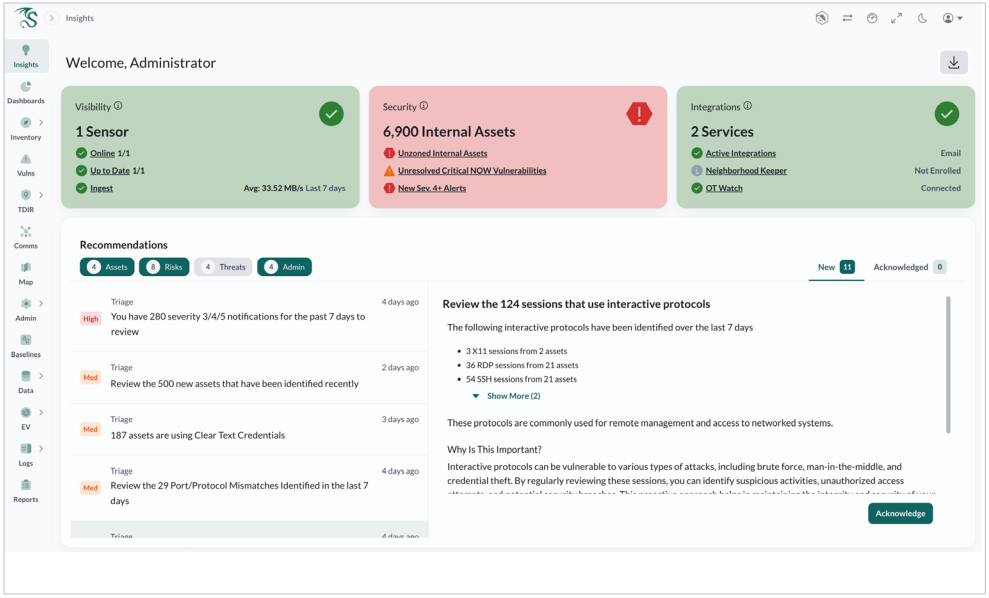
Recommendations You Can Act On

Findings include multiple remediation options, scoped to your maturity level, industry, and operational constraints.

Platform-Enhanced Visibility

The Dragos Platform automates network traffic capture and analysis, enabling weeks of continuous data collection for more complete asset discovery. It delivers risk-prioritized vulnerabilities with “Now, Next, Never” guidance and high-fidelity evaluation of any existing compromise.





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