DRAGOS

SOLUTION BRIEF

Network Vulnerability Assessment, Penetration Testing & Purple Team Exercises

Red Team Services

Network Vulnerability Assessment, Penetration Testing & Purple Team Exercises

Security evaluation and validation for xOT environments — delivered by OT security experts, powered by the Dragos Intelligence Fabric.

OVERVIEW

Validate Your OT Security Posture The Way An Adversary Would

Dragos Red Team Services provide security evaluation and validation for xOT environments through three complementary offerings: Network Vulnerability Assessment, Network Penetration Testing, and Purple Team Exercises. Conducted by OT security experts with deep knowledge of real-world ICS adversary tactics and powered by the Dragos Intelligence Fabric, each engagement is designed to identify hidden attack paths, validate existing security controls, and build detection capabilities without disrupting critical operations.

Organizations receive practical, risk-prioritized recommendations tailored to their operational constraints, whether the goal is establishing a vulnerability baseline, proving control effectiveness under active attack, or training internal teams to recognize and respond to adversary behavior. The result is a stronger, more defensible OT security posture grounded in the realities of OT threat landscapes.

THE CHALLENGE

You Can't Defend Without Full Situational Awareness

Adversaries targeting xOT environments understand ICS protocols, physical processes, and the specific weaknesses of operational networks. Now, those same adversaries are accelerating attacks with AI by automating reconnaissance, compressing the time between discovery and exploitation, and adapting tactics in real-time in ways that traditional defenses can't keep pace with. Most organizations don't know which paths those adversaries would take, whether existing controls would stop them, or whether their team would recognize the attack in progress.

Key Benefits Across All Red Team Services

Identify Weaknesses: Get visibility into exploitable attack paths, systemic vulnerabilities, and detection gaps across your OT networks.

Build a Defensible Network: Validate existing controls, identify missing safeguards, and improve your team's ability to detect and respond to OT cyber threats.

OT-Native Expertise: Responders bring over a decade of OT-specific incident response experience, informed by the Dragos Intelligence Fabric, and understand the operational consequences of every containment decision.

Prioritize Remediation Steps: Receive practical, risk-prioritized recommendations aligned with your operational constraints, focused on what matters most for your critical processes.

OT Threat Intelligence Integration: Testing uses the Dragos Intelligence Fabric, combining 10+ years of adversary research and OT telemetry to reflect real-world ICS TTPs and industry-specific threats—not generic attack scenarios.

THE SOLUTION

The Dragos Red Team Services

THE CHALLENGE	HOW RED TEAM SERVICES SOLVE IT
× **Unknown Entry Points** Devices, applications, and network interfaces quietly expose critical ICS processes and xOT assets.	✓ **Hidden Attack TTPs & Identification** We discover and map exposures in the context of the attack sequences a real adversary would use.
× **Unproven Controls** Defenses look right on paperbut have never faced a real attack scenario.	✓ **Control and Segmentation Validation** We test whether existing defenses actually prevent the attack techniques observed against xOT environments.
× **Untested Detection** Your team has tools in place but limited experience recognizing live adversary behavior.	✓ **Recognize and Respond to Adversary Behavior** in your own environment with collaborative exercises and team training.
× **Findings Without Direction** Long vulnerability lists don't account for what your operations can absorb.	✓ **Prioritized Remediation** Risk-based recommendations balance security improvements with operational requirements.

What Our Customers Are Saying

"The Dragos Red Team identified critical vulnerabilities we didn't know existed in our OT environment. Their approach was thorough yet respectful of our operational constraints. The prioritized recommendations helped us focus our limited resources on the changes that would have the biggest impact on our security posture."

- Security Manager, Global Manufacturing Company

SERVICE OFFERINGS

Choosing The Right Service For Your Needs

Three complementary engagements, each mapped to a different stage of OT security maturity.

01

Network Vulnerability Assessment

PRIMARY FOCUS
Identify vulnerabilities without exploitation

BEST FOR
Organizations that need broad vulnerability discovery and prioritization

KEY DELIVERABLE
Risk-prioritized vulnerability report with a remediation roadmap

02

Network Penetration Testing

PRIMARY FOCUS
Validate controls through active exploitation exercises

BEST FOR
Organizations that want to prove security control effectiveness against attacks

KEY DELIVERABLE
Attack timeline with successful/failed exploitation paths

03

Purple Team Exercise

PRIMARY FOCUS
Build detection and response capabilities

BEST FOR
Organizations that need to improve threat detection & response to adversary behaviors

KEY DELIVERABLE
Detection capability assessment with improvement recommendations

SERVICE 01

Network Vulnerability Assessment

Network Vulnerability Assessments identify vulnerabilities in xOT environments through systematic information gathering and configuration review, without exploitation. Our red team experts use specialized tools and the Dragos Platform to catalog vulnerabilities and other potential findings across domains, hosts, networks, and devices, providing a complete view of your security posture.

Key Features

- ✓ Passive and active vulnerability identification methods
- ✓ Configuration review with privileged access to key systems
- ✓ Attack path analysis to frame vulnerabilities in context
- ✓ Collaborative white box approach for full coverage
- ✓ Limited to 50 unique devices per engagement

What You Receive

- ✓ Vulnerability discovery, attack simulation, and detection training to validate industrial security controls
- ✓ Actionable recommendations tailored to your environment and circumstances
- ✓ Attack path analysis showing possible attack sequences
- ✓ Detailed technical evidence and remediation guidance
- ✓ Summary table for quick remediation planning

What You Receive With The Dragos Platform In Your Environment

- ✓ **Automate capture and analysis of network traffic**
- ✓ **Enable weeks of data collection for complete asset inventories**
- ✓ **Provide risk-prioritized vulnerabilities with "Now, Next, Never" guidance**
- ✓ **Deliver high-fidelity evaluation of any existing compromise or threat**

SERVICE 02

Network Penetration Testing

Network Penetration Testing (NPT) actively attempts to exploit vulnerabilities to validate security controls in your xOT environment. Dragos NPTs are objective-based: rather than cataloging every vulnerability, testers pursue the destinations a real adversary would, such as pivoting from the enterprise network into the OT DMZ, and from the DMZ into the process control network, with findings framed against the ICS Cyber Kill Chain. Engagements run from an assumed-breach position using a collaborative white box approach, so every vulnerability identified is a link in a real attack path and breaking that link measurably disrupts adversary capability.

Key Features

- ✓ ICS-expert testers — specialists in industrial control system exploitation
- ✓ Real attack pathway mapping documenting how adversaries reach critical assets
- ✓ Comprehensive assessment of networks, VPNs, servers, passwords, and design flaws
- ✓ Proof of concept demonstrating which defenses work and which fail

What You Receive

- ✓ Detailed attack timeline showing successful attack paths
- ✓ Priority recommendations for protecting critical OT assets
- ✓ Failed control identification and remediation steps
- ✓ Risk-severity prioritized findings, Critical to Informational

How It Works

IT/OT Boundary Penetration Test

- Begins from assumed breach position on corporate network
- Tests ability to breach the IT/OT perimeter
- Validates OT perimeter security and exposure to corporate systems

DMZ/OT Boundary Penetration Test

- Starts from OT DMZ asset or network position
- Focuses on DMZ security controls and adjacent firewalls
- Evaluates exposure of underlying OT systems

OT System Test

- Begins within the xOT environment
- Assesses internal OT security controls
- Tests privilege escalation and lateral movement; mandatory white box methodology

SERVICE 03

Purple Team Exercise

Purple Team Exercises are collaborative, hands-on engagements that assess and improve your organization's ability to detect and respond to real-world adversary behaviors. Dragos Penetration Testing executes planned attack techniques on site while a Dragos incident responder coaches your team through hunting each action with your own tools. A typical engagement covers roughly 30–35 adversary techniques over a week of testing, with each technique scored as Detected, Partially Detected, or Not Detected and mapped to MITRE ATT&CK.

Key Features

- ✓ Suitable for organizations at all maturity levels
- ✓ Uses your existing security tools (SIEM, EDR, Dragos Platform)
- ✓ Safe, controlled execution with no operational impact
- ✓ Industry-specific scenarios reflecting relevant threats

What You Receive

- ✓ **Practical experience.** Hands-on training using your own tools to recognize threat activity.
- ✓ **Optimized monitoring.** Recommendations to tune existing infrastructure for better threat detection.
- ✓ **Documented results.** A complete report with pertechnique detection results and prioritized improvements.
- ✓ **Stronger capabilities.** Improved ability to detect and respond to actual OT cyber threats.

How It Works

01 Tailored Threat Scenario

We propose an industry-specific threat scenario based on the latest Dragos threat intelligence.

→

02 Parallel Execution

The Red Team executes attack steps while the Blue Team guides your security analysts through threat hunting.

→

03 Real-Time Learning

Your team uses existing security tools to detect and analyze each action.

→

04 Capability Assessment

We evaluate detection capabilities across your security stack.

WHY DRAGOS

Why Dragos Red Team Services

OT Expertise

Our red team consists of OT security experts who understand operational environments, the protocols that run them, and the adversary behaviors specific to the sectors we serve, drawn from over a decade of frontline OT engagements.

Safety First

All testing is conducted with operational safety as the top priority, using methodologies designed specifically for xOT environments where a misstep can affect physical processes.

Actionable Results

Recommendations focus on practical improvements prioritized by operational relevance, so your team knows what to fix now, next, or never within your operational constraints.

Threat Intelligence Integration

Testing reflects the real-world adversary TTPs Dragos tracks through the Dragos Intelligence Fabric, including dozens of named OT threat groups, so scenarios map to actual threats to your industry and geography.

Platform-Enabled Services

The Dragos Platform adds automated data collection, vulnerability prioritization, and threat detection to every engagement, giving testers and defenders a shared view of the environment.

Getting Started

Dragos Red Team Services meet you at any stage of your OT security journey, tailoring services to your needs and maturity level.

Step 1

Start with Network Vulnerability Assessment to identify and prioritize security gaps.

↓

Step 2

Follow with Network Penetration Testing to validate remediation efforts and control effectiveness.

↓

Step 3

Implement Purple Team Exercises to build and maintain detection and response capabilities.

↓

Step 4

Repeat annually or after significant changes to maintain security posture.

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