Red Team Services: Network Vulnerability Assessment, Penetration Testing & Purple Team Exercises

Dragos Red Team Services provide comprehensive security evaluation and validation for industrial environments through three complementary offerings: Network Vulnerability Assessment, Network Penetration Testing, and Purple Team Exercises. These services help organizations identify vulnerabilities, validate security controls, and build detection capabilities against real-world adversary tactics, techniques, and procedures (TTPs) specific to industrial control systems (ICS) and operational technology (OT) environments.

Our Red Team experts leverage deep knowledge of industrial threats gained from Dragos Cyber Threat Intelligence to deliver practical, prioritized recommendations that strengthen your OT security posture while respecting operational constraints.

Why Organizations Choose Dragos Red Team Services

Industrial organizations face unique challenges in securing their OT environments. Unlike IT systems, OT networks require specialized expertise to evaluate safely without disrupting critical processes. Dragos Red Team Services address these challenges by:

Identifying Hidden Attack Paths

Discovering devices, applications, and network interfaces that could allow unauthorized access to critical ICS and OT assets

Validating Security Controls

Testing whether existing defenses actually prevent real-world attack scenarios.

Building Detection Capabilities

Training your team to recognize and respond to adversary behaviors in your environment.

Prioritizing Remediation

Providing risk-based recommendations that balance security improvements with operational requirements.

KEY BENEFITS ACROSS ALL RED TEAM SERVICES

- **Identify Weaknesses.** Get comprehensive visibility into exploitable attack paths, systemic vulnerabilities, and detection gaps across your industrial networks.
- **Prioritize Remediation Steps.** Receive practical, risk-prioritized recommendations aligned with your operational constraints and focusing on what matters most for your critical processes.
- **Build a Defensible Network.** Validate existing controls, identify missing safeguards, and enhance your team's ability to detect and respond to industrial cyber threats.
- **Leverage Industrial Threat Intelligence.** Benefit from Dragos's extensive knowledge of real-world ICS adversary TTPs to ensure testing reflects actual threats to your industry.

Service Offerings Overview

Choosing the Right Service for Your Needs

SERVICE	PRIMARY FOCUS	BEST FOR ORGANIZATIONS THAT...	KEY DELIVERABLE
Network Vulnerability Assessment	Identify vulnerabilities without exploitation	Need comprehensive vulnerability discovery and prioritization	Risk-prioritized vulnerability report with remediation roadmap
Network Penetration Testing	Validate controls through active exploitation	Want to prove security control effectiveness against attacks	Attack timeline with successful/failed exploitation paths
Purple Team Exercise	Build detection and response capabilities	Need to enhance threat detection capabilities and improve response to adversary behaviors	Detection capability assessment with improvement recommendations

Service Delivery Approach: Engagement Process

1 Pre-Engagement Planning

- Define scope and objectives
- Establish Rules of Engagement (ROE)
- Identify critical assets and operational constraints
- Schedule activities to minimize operational impact

2 Execution Phase

- **Vulnerability Assessment:** 3-5 days of data collection and analysis
- **Penetration Testing:** 5-10 days of active testing (varies by scope)
- **Purple Team Exercise:** 3-5 days of collaborative exercises

3 Analysis and Reporting

- Comprehensive analysis of findings
- Risk-based prioritization
- Development of practical recommendations
- Executive and technical reporting

4 Knowledge Transfer

- Detailed debrief sessions
- Q&A with technical teams
- Remediation guidance
- Follow-up support as needed

Network Vulnerability Assessment

Choosing the Right Service for Your Needs

Network Vulnerability Assessments identify vulnerabilities in industrial networks through systematic information gathering and configuration review without exploitation. Our red team experts use specialized tools and the Dragos Platform to catalog vulnerabilities across domains, hosts, networks, and devices, providing a holistic 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 comprehensive coverage
- Limited to 50 unique devices per engagement

What You Receive

- Comprehensive vulnerability inventory categorized by severity (Critical, High, Moderate, Low, Informational)
- Actionable recommendations tailored for your environment and circumstances
- Attack path analysis showing possible attack sequences
- Detailed technical evidence and remediation guidance
- Summary table for quick remediation planning

Network Data Collection with the Dragos Platform

The Dragos Platform enhances our Red Team Services by:

- Automating capture and analysis of network traffic
- Enabling weeks of data collection for complete asset inventories
- Providing risk-prioritized vulnerabilities with “Now, Next, Never” guidance
- Delivering high-fidelity evaluation of any existing compromise or threat

Network Penetration Testing

How Effective Are Your Security Controls at Preventing an Attack?

Network Penetration Testing actively attempts to exploit vulnerabilities to validate security controls in your OT environment. Our industrial penetration testers use real-world attack techniques to demonstrate how adversaries could move through your environment, escalate privileges, and potentially gain control of critical devices and processes.

Testing Scenarios

Test	Testing Scenario
IT/OT Boundary Penetration Test	• Begins from assumed breach position on corporate network • Tests ability to breach 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 OT environment • Assesses internal OT security controls • Tests privilege escalation and lateral movement capabilities • Mandatory white box methodology for active systems

What You Receive

- Detailed attack timeline showing successful attack paths
- Priority recommendations for protecting critical OT assets
- Comprehensive findings with technical evidence
- Failed control identification and remediation steps
- Risk-severity prioritized findings (Critical to Informational)

Service Requirements

- Documented Rules of Engagement (ROE) agreement
- Designated personnel for system restoration if needed
- Network packet captures not exceeding 30GB
- All necessary rights and licenses for tested equipment

Purple Team Exercise

Building Your Team's Detection and Response Capabilities

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. By working together, our Red Team (attackers) and Blue Team (defenders) help your security team gain practical experience in threat hunting and interpreting adversary activity in a safe, controlled manner.

How It Works

- ✓ **Tailored Threat Scenario**
  We propose an industry-specific threat scenario based on latest Dragos threat intelligence.
- ✓ **Parallel Execution**
  Red Team executes attack steps while Blue Team guides your security analysts through threat hunting.
- ✓ **Real-Time Learning**
  Your team uses existing security tools to detect and analyze each action.
- ✓ **Capability Assessment**
  We evaluate detection capabilities across your security stack.

Key Features

- Suitable for organizations at all maturity levels
- Leverages your existing security tools (SIEM, EDR, Dragos Platform)
- Safe, controlled execution with no operational impact
- Hands-on knowledge transfer during the exercise
- Industry-specific scenarios reflecting relevant threats

Requirements

- Dragos Platform deployment (can be part of the service)
- On-site engagement for proper knowledge transfer
- Assigned customer representatives with tool access
- Defined scenario and ROE documentation

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**
  Comprehensive report with test results and prioritized improvement recommendations.
- ✓ **Enhanced Capabilities**
  Improved ability to detect and respond to industrial cyber threats.

Why Dragos Red Team Services

Industrial Expertise. Our red team consists of industrial security experts who understand both OT environments and adversary behaviors specific to industrial sectors.

Threat Intelligence Integration. We leverage Dragos Cyber Threat Intelligence to ensure testing reflects real-world threats relevant to your industry and geography.

Safety First. All testing is conducted with operational safety as the top priority, using methodologies designed specifically for industrial environments.

Platform-Enabled Services. The Dragos Platform enhances our services with automated data collection, vulnerability prioritization, and threat detection capabilities.

Actionable Results. Our recommendations focus on practical improvements that can be implemented within your operational constraints

Getting Started

Dragos Red Team Services are designed to meet organizations wherever they are in their OT security journey. Whether you need to:

- Establish a baseline understanding of vulnerabilities (Network Vulnerability Assessment)
- Validate existing controls against real attacks (Network Penetration Testing)
- Build internal capabilities for threat detection and response (Purple Team Exercise)

Our experts will work with you to determine the right service or combination of services for your specific needs and maturity level.

Recommended Service Progression

- **Start with Network Vulnerability Assessment** to identify and prioritize security gaps
- **Follow with Network Penetration Testing** to validate remediation efforts and control effectiveness
- **Implement Purple Team Exercises** to build and maintain detection and response capabilities
- **Repeat annually or after significant changes** to maintain security posture