Network Vulnerability Assessment & Penetration Testing Services

Dragos Penetration Testing Services provide the specific, prioritized guidance organizations require to reduce risk and mature operational technology (OT) cyber defense. We provide two complementary security evaluation services for industrial environments: Network Vulnerability Assessment and Network Penetration Testing. Together, these services help organizations discover security gaps, prove the effectiveness of existing defenses, and receive actionable recommendations to strengthen their OT security posture against potential attacks.

The **Network Vulnerability Assessment** identifies potential security weaknesses through systematic information gathering and configuration review. The **Network Penetration Testing** actively attempts to exploit these vulnerabilities to validate security controls.

Identify Weaknesses

Get a visual on both exploitable attack paths and systemic vulnerabilities across industrial networks, providing comprehensive risk awareness.

Prioritize Remediation Steps

Know the critical security gaps needing immediate attention and get practical fixes aligned with your operational constraints.

Build a Defensible Network

Validate existing controls and know missing safeguards, to enable a more resilient industrial control system (ICS) environment.

NETWORK DATA COLLECTION WITH THE DRAGOS PLATFORM

Dragos Network Vulnerability Assessment and Penetration Testing services 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.

Network Vulnerability Assessment: A Data-Driven Approach to Identify OT Network Weaknesses

Network Vulnerability Assessments identify vulnerabilities in industrial networks through active and passive information gathering. The Services team samples systems and reviews configurations with privileged access to key systems. Our red team experts use specialized tools to catalog vulnerabilities across domains, hosts, networks, and devices without exploitation.

Leveraging existing network diagrams and asset lists, the red team delivers a report of vulnerabilities with recommendations for practical security improvements.

The Dragos Network Vulnerability Assessment employs a collaborative white box approach and utilizes specialized inspection and collection tools on target systems. The findings report prioritizes items based on risk severity (Critical, High, Moderate, Low, and Informational), rather than technical complexity. Special attention is given to vulnerabilities affecting critical or industrial control systems. A summary table provides an at-a-glance view of all findings for quick remediation and prioritization.

Classification Header	Description	Impact	Recommendation	References
Numbered and categorized by severity (e.g., "1.1 Software-Based PLC Version Allows Remote Code Execution")	Technical explanation of the vulnerability or security issue	Assessment of potential consequences if exploited, emphasizing operational risks	Actionable remediation guidance	Industry-standard identifiers like MITRE ATT&CK for ICS techniques or CVEs

Network Penetration Test: How Effective Are Your Security Controls at Preventing an Attack?

A Network Penetration Test uses expert testers armed with in-depth knowledge of how to exploit vulnerabilities in industrial control systems to expose weaknesses – and validate defenses. Testers attempt to gain access to ICS assets by targeting networks, VPNs, and servers, proving whether security measures prevent intrusion. We evaluate attack pathways, vulnerabilities, data hygiene, passwords, network design, location of key (crown jewel) OT assets, domain and information systems. The test report details successful attack paths, failed controls, and actionable recommendations to mitigate weaknesses. Findings include:

Attack Timeline	Priority Recommendations	Detailed List of Findings
Key steps in the attack are identified to explain how an adversary may approach the system, along with prevention opportunities.	Summary of key steps to take to protect critical OT assets, harden servers and networks to minimize the attack surface, fix misconfigurations, and mitigate risk.	Each finding provides a description of issues, technical evidence, and remediation steps. Findings are prioritized by severity — Critical, High, Moderate, Low, and Informational.

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**.