Trellix

DATA SHEET

ICS Vulnerability Assessment & Testing Services

Protecting Industrial Systems. Preventing Downtime.

Deliverables

Asset & Vulnerability Inventory

- Prioritized Remediation Plan

- Root Cause & Exposure Analysis

- Strategic Risk Mitigation Recommendations

- Executive Summary Report

Why It Matters

ICS environments have unique security needs that differ from traditional IT networks. Our assessment helps you:
- Prevent downtime from malicious attacks
- Identify and prioritize risks to operations
- Strengthen compliance with OT security frameworks
- Build resilience in critical infrastructure environments

Overview

Industrial Control Systems (ICS) are increasingly targeted by threat actors due to their critical role in national infrastructure and manufacturing environments. Trellix Guardians' non-disruptive ICS vulnerability assessment is designed to identify, analyze, and help mitigate exploitable weaknesses across control networks, devices, and operational systems.

Our ICS Security Assessment Services

1. Host & Service Enumeration
Identify all live ICS systems, exposed services, and communication protocols. Gather OS, application, and network fingerprinting data across your control environment.

2. *Vulnerability Testing*
Combine automated scans with manual testing to uncover misconfigurations, default settings, missing patches, weak passwords, and chainable vulnerabilities.

3. *Configuration & Authentication Review*
Assess access controls, weak credentials, and legacy defaults. Identify insecure authentication schemes and exposed interfaces.

4. *Patch & Protocol Analysis*
Evaluate patch levels across ICS software, firmware, and infrastructure. Identify unnecessary services, insecure protocols, and lateral exposure points.

5. *Data Protection Validation*
Confirm use of secure channels, validate encryption protocols, and detect insecure storage or error leakage of sensitive information.

For more information or to schedule a consultation, please contact us at Guardians@Trellix.com