

Bridging IT and OT Security: A Vulnerability Testing Partnership for a Manufacturing Leader

How Lume Strategies helped a multi-site manufacturer validate security across its office IT and industrial operational technology environments.

Industry

Manufacturing,
Automotive Security
Hardware/OEM
Supplier

Footprint

Multi-site
manufacturing
environment spanning
corporate IT and plant-
floor OT systems

Partner Since

2021

Services

Internal and External
Penetration Testing,
Vulnerability
Assessment,
Managed IT Services

THE CHALLENGE

The Client is a multi-site manufacturer of automotive security hardware whose production equipment, engineering systems, and corporate IT converge on a single network. Traditional IT vulnerability scanning alone cannot reveal the full risk when industrial control systems, connected physical security devices, and other plant-floor technologies share that network with email, file servers, and workstations.

The Client needed independent external and internal vulnerability testing to validate security across this converged environment and support the regulatory, commercial, and contractual requirements of a manufacturing supplier.

THE LUME APPROACH

Since 2021, Lume has delivered a combined external and internal vulnerability assessment and penetration testing program as part of its broader managed IT services relationship with the Client. The repeatable engagement gives the Client a consistent, trackable view of risk over time.

Testing aligns with guidance in NIST SP 800-115 and combines automated vulnerability scanning, credentialed internal assessments that provide deeper system visibility, and external penetration testing that evaluates what an attacker could exploit from outside the network. Engagements have covered more than 1,000 internal endpoints across multiple network segments, along with the Client's externally facing systems. The resulting analysis gives leadership a consolidated view of risk across office IT and plant-floor technology.

RESULTS & IMPACT

- **Risk-ranked findings:** Vulnerabilities are categorized by severity and known exploit availability, giving the Client's IT team a clear order for remediation.
- **OT-aware assessment:** Testing accounts for the Client's operational technology environment, helping ensure manufacturing and physical security systems are not overlooked.
- **Actionable remediation tools:** The Client receives a detailed narrative report and a sortable, filterable workbook that supports remediation tracking over time.
- **Compliance-supporting documentation:** Each engagement is documented, providing evidence for regulatory, insurance, and customer-driven security requirements.
- **Integrated service delivery:** Vulnerability testing is coordinated within Lume's broader managed IT services relationship, giving the Client a partner familiar with its environment and operating context.



2021

YEAR PARTNERSHIP
BEGAN

1,000+

INTERNAL ENDPOINTS
ASSESSED

IT & OT

ENVIRONMENTS ASSESSED

Ongoing

MANAGED SERVICES
RELATIONSHIP

Ongoing Security Testing Within a Broader Partnership

Security testing is part of the Client's ongoing managed IT relationship with Lume, which also spans infrastructure, endpoint management, and cybersecurity. This broader context gives Lume familiarity with both office IT and plant-floor technology, supporting more informed testing and practical remediation.

Need a clearer view of exposure across a converged IT and OT environment? Contact Lume Strategies to learn how vulnerability assessment and penetration testing can help.