

Strengthening Cybersecurity Across a Multi-Location Medical Practice

How a multi-year, risk-based penetration testing and vulnerability assessment program helped a Buffalo-area healthcare provider assess risk, prioritize remediation, and support audit-readiness.

Industry

Healthcare,
Multi-Specialty
Medical Practice

Footprint

7 clinical,
surgical & retail
locations

Partner Since

2015
Program active since 2020

Services

Internal & External
Penetration Testing,
Vulnerability
Assessment

THE CHALLENGE

The Client operates a large, multi-location medical practice across the Buffalo, New York area. Seven clinical, surgical, retail, and administrative sites all run on one shared, segregated network. As a healthcare provider handling protected health information (PHI) and payment data, the Client must manage rigorous security and privacy expectations, including HIPAA and applicable PCI DSS requirements. The testing program also provides documented evidence to support broader risk assessment, audit, and contractual obligations.

With clinical operations, surgical technology, retail point-of-sale systems, and administrative infrastructure sharing one segregated network, the Client needed a partner who could validate security across every layer of the environment.

THE LUME APPROACH

Lume Strategies began supporting the Client in 2015 and has delivered recurring internal and external penetration testing and vulnerability assessments since 2020. Completed testing cycles in 2020, 2024, and 2026 reflect an ongoing relationship shaped around the Client's evolving risk profile.

In 2024, the program included a full white-box network penetration test that combined manual and automated techniques aligned to NIST SP 800-115 and the Penetration Testing Execution Standard (PTES). This approach tested which vulnerabilities could realistically be exploited, as opposed to simply flagging theoretical exposure points. The March 2026 cycle combined internal and external vulnerability assessments across 248 hosts, giving leadership a comprehensive, current risk profile for clinical workstations, servers, and network infrastructure.

RESULTS & IMPACT

Each assessment translated raw technical findings into a clear, risk-ranked action plan:

- **Severity-based prioritization:** Vulnerabilities were categorized by criticality (critical, high, medium, low) so that the Client's IT team could focus efforts where they mattered most.
- **Exploitability-driven risk ranking:** Findings with publicly available exploits were specifically flagged as top-priority remediation targets, sharpening the plan from a checklist into a practical risk model.
- **An operational remediation tool:** The Client received a prioritized recommendation summary and a sortable workbook filterable by host, severity, and exploit availability. This live document facilitates effective remediation progress tracking.
- **Audit-support documentation:** Lume provides formal attestation for each completed engagement, giving the Client evidence to support HIPAA, PCI, and NY DFS audit and compliance requirements.



7

PRACTICE LOCATIONS
ASSESSED

248

HOSTS ASSESSED IN
THE LAST CYCLE

3

TESTING CYCLES
SINCE 2020

5

REGULATORY
FRAMEWORKS
ADDRESSED

AN ONGOING PARTNERSHIP

For the Client, security testing isn't a one-time event; it's a recurring discipline built into operations across all seven locations. By pairing rigorous testing with clear, actionable reporting, Lume Strategies has helped the Client turn vulnerability management into a repeatable, defensible program rather than a periodic scramble ahead of an audit.

Is your organization due for a security assessment? Contact Lume Strategies to learn how penetration testing and vulnerability assessment services can help you identify and address risks before they become incidents.