

Recurring External Penetration Testing for a Five-Brand Professional Services Enterprise

THE CHALLENGE

The Client is the shared infrastructure backbone for five separate operating companies under one professional and managed services umbrella. That means one security posture supports every sibling brand that relies on it. The Client needed evidence, not assumptions, that its external defenses could hold up. Independent, recurring validation supports its compliance and audit programs, giving each operating company confidence in shared systems.

THE LUME APPROACH

Lume Strategies has delivered a recurring external penetration testing program for the Client since 2018, with the most recent cycle completed in January 2026. This is not a one-time compliance check. It is a standing program through which the Client regularly validates and strengthens its security posture. Each cycle combines three layers — technology, process, and people — through complementary testing methods:

- **Manual and automated external vulnerability scanning** to actively probe the Client's external footprint
- **Open-source intelligence (OSINT) reconnaissance** to validate what's visible about the Client on the open internet
- **A live social engineering/phishing simulation** to test how employees respond under realistic conditions

Overview

Industry

Professional & managed Services

Footprint

Shared infrastructure, 5 operating companies

Partner Since

2018

Services

External Penetration Testing, OSINT, Social Engineering

RESULTS & IMPACT

- **Layered defenses held under real pressure.** Although a portion of targeted employees engaged with the simulated phishing attempt, the enforced multi-factor authentication and other controls prevented the simulated attacker from completing an account takeover. The exercise demonstrated that these defenses functioned as designed.
- **No exploitable vulnerabilities were identified.** Automated scanning found no vulnerabilities of concern, a good reflection of the Client's existing patching and hardening discipline.
- **No confidential information exposed.** OSINT reconnaissance found no confidential company information within reviewed open-source locations.
- **A practical hardening roadmap.** The engagement surfaced a targeted set of lower-severity opportunities, each paired with clear remediation guidance so the Client's team could effectively prioritize next steps.
- **Useful, defensible documentation.** Each engagement is documented and attested, giving the Client evidence for its broader compliance and audit programs, reinforcing trust with the operating companies it serves.



5

OPERATING COMPANIES
RELYING ON THIS
INFRASTRUCTURE

2018

MARKED THE START
OF THIS TESTING
PARTNERSHIP

3

TESTING LAYERS
COMBINED EACH CYCLE

0

EXPLOITABLE
VULNERABILITIES FOUND
IN THE LATEST SCAN

AN ONGOING PARTNERSHIP

For the Client, security testing isn't a scramble before an audit. It's embedded into holistic operations across every brand under its umbrella. Lume Strategies provides recurring, reliable validation, so the Client can provide its sibling companies and auditors evidence that the shared systems are secure.

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