Logically
CYBER FIRST. FUTURE READY.

Penetration Testing

Uncover Blind Spots Across Your Network, Applications, and Cloud Environment

Mid-market organizations are increasingly targeted by attackers exploiting weak configurations, mismanaged credentials, and unpatched vulnerabilities. Many of these exposures aren't detected by automated scanners—and by the time they're exploited, it's too late.

Logically's Penetration Testing services simulate real-world adversaries to uncover blind spots across your network, applications, and cloud environments. Each test is tailored, safe, and supported by detailed reporting mapped to your regulatory and operational needs.

- 93% of breaches in mid-market environments start with exploited vulnerabilities (Verizon Data Breach Investigations Report, 2024)
- Many SMBs operate for years without ever conducting a formal pen test (Trustwave Global Security Report)

WHAT YOU'LL GAIN

Network Penetration Testing – Identify perimeter gaps, insecure protocols, and firewall misconfigurations

Internal Penetration Testing – Simulate insider threats and lateral movement post-compromise

Web App & API Testing – Uncover OWASP top 10 flaws in SaaS, portals, and custom applications

Cloud Security Testing – Assess misconfigured S3 buckets, exposed services, and IAM gaps

Credential & Access Testing – Detect weak authentication, privilege escalation, and brute-force vectors

Red Team Simulation (Optional) – Emulate advanced threat actors for high-value target testing

Compliance Reporting – Deliverables aligned to HIPAA, PCI-DSS, SOC 2, and CMMC frameworks

WHO IT'S FOR

CIOs and CISOs preparing for compliance or cyber insurance renewals

Security teams needing third-party validation of defenses

Mid-sized orgs without internal offensive security capabilities

Clients bundling testing into Logically's SecureCare roadmap

WHAT'S INCLUDED

- Pre-engagement scoping and objective setting
- Testing of external, internal, cloud, and/or application layers
- Vulnerability exploitation simulation and lateral movement analysis
- Executive and technical reports with prioritized findings
- Remediation guidance mapped to NIST and CIS benchmarks
- Optional quarterly or annual re-testing packages
- Available standalone or integrated into full vCISO or SecureCare programs

USE CASE SNAPSHOT

A 400-user hospitality brand preparing for a PCI-DSS audit turned to Logically to proactively test their defenses and meet third-party assessment requirements.

Logically performed external, internal, and web application testing across their reservation system, Wi-Fi guest networks, and back-office infrastructure. The engagement revealed five exploitable vulnerabilities—including unauthenticated access to an outdated admin panel. All issues were prioritized, remediated, and re-tested within two weeks.

Result:

- Identified and closed five high-risk vulnerabilities
- Achieved full PCI compliance with no auditor findings
- Gained executive buy-in for continuous testing every six months

Logically. Cyber-First. Future Ready

www.logically.com hello@logically.com