LevelBlue

SOLUTION BRIEF

LevelBlue Penetration Testing Service

Work Toward Satisfying PCI DSS Penetration Testing Requirements and Evaluate How Your Organization's Security Holds Up to Real-World Scenarios

Accelerate PCI DSS Compliance Readiness

Compliance with PCI DSS is essential for organizations that process credit, debit, or cash card data. Failure to comply can result in steep fines—and data breaches caused by non-compliance can have catastrophic implications.

To satisfy PCI DSS Requirement 11.3, organizations must conduct both internal and external penetration testing "at least annually," as well as after any significant change.

As a qualified third–party provider, LevelBlue Cybersecurity Consulting can complete internal and external penetration testing of your cardholder data environment (CDE) at the appropriate depth to meet PCI DSS requirements. Experienced LevelBlue consultants deliver a comprehensive report of verified exploitable vulnerabilities and other issues uncovered in your environment, giving you the guidance you need to prioritize and complete required remediation activities.

Explore Security Weaknesses Before an Attacker Does

A typical attacker won't go straight for your data center. Instead, they'll try to gain a foothold based on something seemingly harmless that hasn't been patched or secured, then move laterally through the network to evade detection and access valuable targets.

While automated vulnerability scanning can help you identify security flaws, it can't help you evaluate the strength of your organization's security controls against a human attacker.

LevelBlue Penetration Testing can reveal not only where your infrastructure is vulnerable, but also how critical those weaknesses are and how thoroughly they can be exploited by a motivated human attacker. Experienced LevelBlue consultants leverage creativity, expertise, and human problem-solving to emulate an attacker and evaluate how your security infrastructure holds up to real-world scenarios.

Benefits of LevelBlue Penetration Testing Service

- Meet penetration testing requirements for compliance regulations such as PCI DSS
- Identify and evaluate key attack vectors an attacker could leverage to compromise your organization's critical data and assets
- Understand the full business impact of a real-world attack
- Gain a thorough, third-party understanding of your organization's security posture
- Benefit from expert guidance on prioritization and remediation from LevelBlue Cybersecurity Consulting

How It Works

Test Internal and External Networks

Test your internal and external networks with a combination of automated sweeps and detailed manual testing performed by LevelBlue consultants. Benefit from LevelBlue consultants' custom tools and advanced manual testing techniques, which can reduce false positives and uncover complex, emerging, or obscure vulnerabilities that automated scans alone often miss.

Assess Your Defenses

Validate the effectiveness of your security controls during a simulated attack to learn how to strengthen your security posture. Discover not only how an attacker might breach your existing defenses, but how deeply they can penetrate your environment while escaping detection.

Evaluate Potential Exploits

Understand how an attacker might breach your defenses by testing the feasibility of different attack vectors, including multiple attack vectors at once. Evaluate how deeply an experienced, motivated attacker can penetrate your environment using security weaknesses that automated tools might miss, such as by exploiting a high-risk vulnerability created from a sequence of lower-risk vulnerabilities.

Document Essential Security Gaps

Receive a comprehensive report of identified vulnerabilities, including assessments of potential impact, exploit likelihood, effort to remediate, and recommended remediation path.

Work with Security Experts

Partner with expert LevelBlue consultants with years of penetration testing experience, including deep familiarity with how organizations run and how attackers operate. LevelBlue consultants can not only walk you through the process used to break through your defenses, but also articulate the magnitude of the impact to your organization and help you understand and prioritize remediation efforts.

Understand Potential Damages

Assess the extent of the organizational impact a breach might cause, including how effectively an attacker might compromise your organization's most critical assets. Drive security priorities based on organizational risk, with expert guidance from LevelBlue consultants.

Prioritize Remediation Efforts

Leverage prioritization and remediation guidance from expert LevelBlue consultants to determine your highest priorities for remediation.

Satisfy PCI DSS Pen Test Requirements

Achieve the appropriate depth of internal and external penetration testing to meet PCI DSS requirements with help from experienced LevelBlue consultants. Receive a detailed report of exploitable vulnerabilities, including prioritization and remediation guidance to help you meet vulnerability correction requirements.

Technical Findings Report

LevelBlue consultants summarize their findings in a comprehensive report including an executive summary, key findings, recommendations for remediation, and any other relevant supporting documentation.

For each individual finding, the report includes the following information:

Finding Description	Brief Technical Description of the Finding
Affected Systems	IP address, hostname, or description of the vulnerable systems.
Overall Risk Level	Rating of the overall risk to a system posed by a given finding, based on exploit difficulty and impact (High, Medium, or Low).
Exploit Impact	Rating of the impact a given finding has on a system when exploited (High, Medium, or Low).
Exploit Likelihood	Rating of the probability a potential vulnerability might be exercised within the context of the associated environment (High, Medium, or Low).
Effort to Remediate	Rating of the effort necessary to remediate the issue (High, Medium, or Low).
Remediation	Description of the suggested remediation path, which may include supplemental information such as typical remediation approaches or links to patch information.

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.