Payment Card Industry Data Security Standard (PCI DSS)

Achieve Compliance with Automated Security Validation

The security testing requirements of PCI DSS have evolved significantly, emphasizing risk-based strategies, regular testing, and continuous improvement in place of traditional point-in-time penetration tests. Manual testing methods fall short in addressing the latest PCI DSS requirements due to their limited scope, frequency, and scalability. Pentera simplifies PCI DSS compliance by automating penetration testing across your cardholder data environment (CDE). Continuously validate your security controls, assess the risk posed by vulnerabilities and weaknesses by seeing their potential impact, and easily retest to confirm that exposures have been corrected.

Key Capabilities

Automate Testing Across Your Environment

Scale penetration testing across your entire cardholder data environment and critical systems, leveraging Pentera's extensive library of adversary techniques. Run tests on demand or at your desired cadence.

Accelerate Remediation of Your Highest-Risk Exposures

Identify exploitable vulnerabilities and security weaknesses in your cardholder data infrastructure. Prioritize exposures based on risk and remediate efficiently using Pentera's clear guidance.

Simplify Evidence Gathering for Compliance

Repeat testing to verify that exposures have been corrected. Conduct thorough evaluations of your deployed security controls and obtain comprehensive reports for PCI DSS compliance reviews.

Introduction to PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a globally recognized standard aimed at protecting cardholder data and securing payment ecosystems. Developed by the PCI Security Standards Council (PCI SSC), it mandates essential security practices to prevent breaches and maintain trust in the payment industry. PCI DSS applies to all entities handling cardholder data, including merchants, financial institutions, and service providers, regardless of size or location.

The key requirements of PCI-DSS are categorized as follows:

- **Build and Maintain a Secure Network and Systems**
  Implementing security controls and applying secure configurations to all systems
- **Protect Account Data**
  Protecting data in storage and during transmission
- **Maintain a Vulnerability Management Program**
  Building secure systems and protecting from malware
- **Implement Strong Access Control Measures**
  Restricting access to cardholder data and authenticating users
- **Regularly Monitor and Test Networks**
  Ongoing security testing and access monitoring
- **Maintain an Information Security Policy**
  Creating organizational policies and programs

Security Testing: Key to PCI DSS Compliance

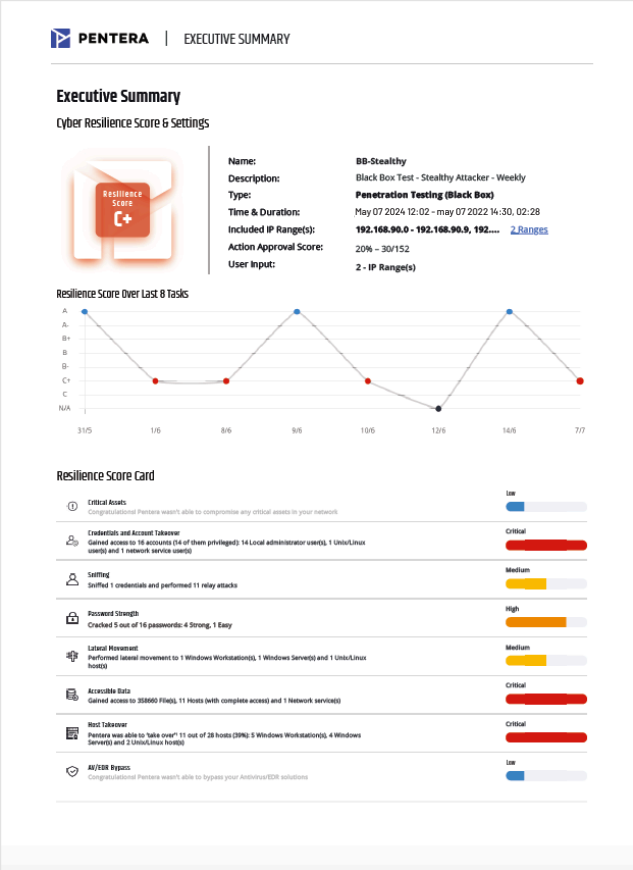
PCI DSS requires that organizations test their security systems and processes on a regular basis to ensure the ongoing security of the cardholder data environment (CDE). Testing coverage must include the entire CDE perimeter and all critical systems, both from inside and outside the network. PCI DSS v4, the latest version of the standard, puts greater emphasis on continuous testing and remediation of exploitable vulnerabilities and weaknesses, rather than point-in-time tests.

To meet these compliance requirements, automated testing is no longer a nice-to-have, but a staple to address the need for continuous testing at scale.

Highlighted PCI DSS Requirements Addressed by Pentera

PCI DSS Requirement	Pentera Capabilities and Features
Requirement 1: Install and Maintain Network Security Controls	Validates that firewall and network security controls are properly implemented and configured.
Requirement 2: Apply Secure Configurations to All System Components	Identifies misconfigurations in system components across the tested environment.
Requirement 3: Protect Stored Account Data	Validates that systems storing cardholder data are not susceptible to cyber attacks due to misconfigurations, software vulnerabilities, compromised identities or security hygiene gaps.
Requirement 4: Protect Cardholder Data During Transmission	Tests secure transmission methods (e.g. TLS) to ensure they cannot be manipulated or bypassed by adversary techniques.
Requirement 5: Protect Systems and Networks from Malware	Emulates malware and ransomware scenarios to validate the effectiveness of antivirus and endpoint protection solutions.
Requirement 6: Develop and Maintain Secure Systems	Identifies vulnerabilities and performs testing to validate their exploitability and potential impact.
Requirement 8: Identify and Authenticate Access to Systems	Validates MFA implementations, tests password strength policies, and identifies exposed or reused credentials.
Requirement 10: Track and Monitor All Access	Tests logging and monitoring systems to ensure critical events are captured.
Requirement 11.3.1: Internal Vulnerability Scanning	Conducts automated internal scans to uncover vulnerabilities within the cardholder data environment (CDE).
Requirement 11.3.2: External Vulnerability Scanning	Dynamically maps external assets and performs scans to protect the external attack surface.*
Requirement 11.4.2: Internal Penetration Testing	Tests internal networks with a wide range of testing scenarios, such as black box and gray box.
Requirement 11.4.3: External Penetration Testing	Performs ongoing monitoring and automated penetration testing of the external attack surface.
Requirement 11.4.4: Correction of Exploitable Vulnerabilities & Weaknesses	Provides risk-based prioritization of exploitable security gaps and detailed remediation guidance. Automated test runs can be repeated to verify that gaps are no longer detected.
Requirement 12: Maintain an Information Security Policy	Provides detailed, actionable reports to support compliance audits and enforcement of security policies.

*** Note:** Pentera is not a PCI SSC Approved Scanning Vendor (ASV). Pentera can be used to continuously assess the external attack surface, identify exploitable vulnerabilities and weaknesses, and verify that corrections were implemented properly, resulting in improved ASV scan results.


PENTERA | EXECUTIVE SUMMARY

Executive Summary

Cyber Resilience Score & Settings

Resilience Score C+

Name:	BB-Stealthy
Description:	Black Box Test - Stealthy Attacker - Weekly
Type:	Penetration Testing (Black Box)
Time & Duration:	May 07 2024 12:02 - may 07 2022 14:30, 02:28
Included IP Range(s):	192.168.90.0 - 192.168.90.9, 192.... 2 Ranges
Action Approval Score:	20% – 30/152
User Input:	2 - IP Range(s)

Resilience Score Over Last 8 Tasks

A, A-, B+, B, B-, C+, C, N/A

31/5 1/6 8/6 9/6 10/6 12/6 14/6 7/7

Resilience Score Card

Critical Assets Congratulations! Pentera wasn't able to compromise any critical assets in your network	Low
Credentials and Account Takeover Gained access to 16 accounts (14 of them privileged): 14 Local administrator user(s), 1 Unix/Linux user(s) and 1 network service user(s)	Critical
Sniffing Sniffed 1 credentials and performed 11 relay attacks	Medium
Password Strength Cracked 5 out of 16 passwords: 4 Strong, 1 Easy	High
Lateral Movement Performed lateral movement to 1 Windows Workstation(s), 1 Windows Server(s) and 1 Unix/Linux host(s)	Medium
Accessible Data Gained access to 358660 File(s), 11 Hosts (with complete access) and 1 Network service(s)	Critical
Host Takeover Pentera was able to 'take over' 11 out of 28 hosts (39%): 5 Windows Workstation(s), 4 Windows Server(s) and 2 Unix/Linux host(s)	Critical
AV/EDR Bypass Congratulations! Pentera wasn't able to bypass your Antivirus/EDR solutions	Low

Perform Testing Regularly at Scale with Pentera Automated Security Validation

The Pentera platform rigorously tests security systems, processes, and tools at scale by emulating real-world attacker tactics, continuously challenging defenses. Pentera identifies exploitable vulnerabilities that put cardholder data at risk, and prioritizes security gaps based on evidence of potential risk impact. Pentera can be scheduled to run at any cadence—daily, weekly, or monthly—enabling coverage of the entire CDE and critical systems. This approach reduces the cost, time, and effort associated with traditional manual penetration testing while maintaining compliance with PCI DSS requirements.

About Pentera

Pentera is the market leader in Automated Security Validation, empowering companies to proactively test all their cybersecurity controls against the latest cyber attacks. Pentera identifies true risk across the entire attack surface, guiding remediation to effectively reduce exposure. The company's security validation capabilities are essential for Continuous Threat Exposure Management (CTEM) operations. Thousands of security professionals around the world trust Pentera to close security gaps before threat actors can exploit them.

Visit: **pentera.io** for more information or contact us to discuss how we can assist your compliance efforts.