Synack

DATA SHEET

PCI DSS Testing from Synack

Fulfilling Payment Card Industry testing requirements

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.

PCI DSS outlines regular testing requirements of Cardholder Data Environments (CDEs) in part 11 of the PCI DSS Standard.

Synack's methodology and benefits

On-demand testing from a diverse skill set of global researchers - the Synack Red Team (SRT)

Includes coverage for the entire CDE perimeter and critical systems

Internal and external network testing

Addressing PCI with Synack's vulnerability checklists

Synack's Vulnerability Checklists are derived from guidelines like the OWASP Web Security Testing Guide (WSTG) and the OWASP Top Ten.

The Vulnerability Checklists will produce reports that detail the work performed by SRT members. These reports provide proof of work, and can be shown to the Qualified Security Assessor (QSA) that will certify your organization's status as PCI compliant.*

Synack offers Vulnerability checklists for both web and host assets to test your CDEs:

- Vulnerability Checklist (Web)
- Vulnerability Checklist (Host)

PCI REQUIREMENT	SYNACK SOLUTION
PCI DSS 11.3.1 - External Penetration Testing PCI DSS 11.3.2 - Internal Penetration Testing	Both requirements are solved with Synack's Premium Vulnerability Checklists, which consist of a comprehensive set of vulnerability checks and generate proof-of-work reports.
PCI DSS 11.3.3 - Vulnerability Remediation	While remediation is ultimately up to the organization being tested, Synack offers on-demand patch verification within the Synack Platform, so you can verify your remediation efforts.
PCI DSS 11.3.4 - CDE Network Segmentation Testing	Synack provides network segmentation testing to assess the isolation of CDE networks from non-CDE networks.

*Synack is not a QSA.

Vulnerability checklist contents

Issues checked for by Synack Red Team researchers include:

- Authentication vulnerabilities
- Business logic
- Code injection
- Cryptography vulnerabilities
- Directory traversal
- Password cracking
- Privilege escalation
- Remote code execution

The Vulnerability Checklists contain the above items and much more, derived from both open-source checklists like OWASP testing guides and proprietary Synack methodologies. These vulnerability checklists serve to fulfill the testing requirements outlined in 11.3.1 and 11.3.2. For a full list detailing the contents of the vulnerability checklists, reach out to your Synack representative.