WHITE PAPER

SYNACK PCI DSS PENETRATION TESTING TECHNICAL WHITE PAPER

JOEL DUBIN | CISSP, QSA, PA-QSA
BHAVNA SONDHI | CISA, QSA (P2PE), PA-QSA (P2PE)

COALFIRE®

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Synack engaged Coalfire, a respected Qualified Security Assessor (QSA) for the Payment Card Industry (PCI) and Payment Application Qualified Security Assessor (PA-QSA) company, to conduct an independent technical assessment of their crowdsourced penetration testing service offering. Coalfire conducted assessment activities including review of i) technical documentation, ii) penetration testing methodology, (iii) penetration tester vetting processes, and (iv) compliance requirements.

In this paper, Coalfire will describe that Synack can meet the PCI Data Security Standard (PCI DSS) v3.2 penetration testing requirements based on the documentation review and evidence gathered during this assessment, assuming that the penetration testing scope is well-defined and appropriately executed.

ABOUT SYNACK

Synack is a company that provides crowdsourced security testing that uncovers vulnerabilities that often remain undetected by traditional penetration testers and scanners. Their technology involves crowdsourcing to globally sourced penetration testers for individual assignments. Synack has a methodology for thoroughly vetting penetration tester candidates based on their skill set, level of experience, and type of clients worked with. In addition to verifying and testing their skills, each candidate goes through initial and periodic background checks as well as continuous monitoring of their efficacy on the platform. The service Synack offers includes testing from the Synack Red Team (SRT), whose researchers represent over 55 countries around the world.

Synack offers a powerful platform to aid and augment the SRT. Its components - Hydra and LaunchPoint - together provide recon, suspected vulnerabilities, and a trusted, logged, and monitored environment for adversarial-style security research.

The Synack approach combines the best features of Application Security Testing tools, Penetration Testing engagements, and Bug Bounty programs to deliver a controlled, effective and efficient approach to digital security. This provides a proactive approach to penetration testing from the attacker's perspective—detecting and reporting vulnerabilities within web applications, host infrastructure, mobile apps, cloud and IoT software that often remain undetected by traditional security solutions

It should be noted that Synack is strictly a services offering and does not provide a physical product or application to its clients. It is also not a PCI Approved Scanning Vendor (ASV) and does not limit its penetration testing services to only vulnerability scanning.

AUDIENCE

This assessment white paper has three target audiences:

1. **QSA and Internal Audit Community:** This audience may be evaluating how the services offered by Synack, an external penetration testing provider, are leveraged within merchant or service provider environment for PCI DSS.
2. **Administrators and Other Compliance Professionals:** This audience may be evaluating Synack, an external penetration testing provider, for use within their organization for compliance requirements other than PCI DSS.
3. **Merchant and Service Provider Organizations:** This audience is evaluating how Synack’s external penetration testing services can be utilized to meet the penetration testing requirements set forth by PCI DSS.

METHODOLOGY

Coalfire completed a multi-faceted technical assessment using the below industry and audit best practices. Coalfire conducted review of technical documentation and penetration testing methodologies from April 12, 2018 to May 18, 2018.

At a high level, following tasks were performed for review of Synack's penetration testing methodologies:

1. Technical review of the documented penetration testing methodology used by Synack's penetration testing team, the SRT.
2. Review of the scoping methodology and how the SRT scopes an engagement, particularly regarding their clients using the Synack service for their annual penetration testing required by PCI. This includes a review of the Rules of Engagement Synack established for its SRT.
3. Review of how Synack vets penetration testers for joining the SRT and how individual engagements are then managed after the team is selected. This involved review of documentation detailing the vetting process and review of sample reports with results of the vetting process.
4. Review of penetration testing methodology used to confirm that testing by the SRT includes at least the following:
    a. Validation of segmentation
    b. Application-layer penetration testing
    c. Network-layer penetration testing
5. Review of sample penetration testing reports from engagements for PCI DSS annual penetration testing to verify they meet all relevant PCI requirements, such as Requirement 11.3 and its sub-requirements.
6. Review of lists of tools used to verify compliance with PCI penetration testing requirements.

SUMMARY FINDINGS

The following findings are relevant highlights from this assessment:

- The SRT is required to follow a documented penetration testing methodology developed by Synack. The methodology is in compliance with PCI DSS Requirement 11.3.
- Synack has a documented methodology for vetting its penetration testers to ensure they have the skill levels to meet PCI Requirements 11.3.1.b, 11.3.2.b and 11.3.4.c.
- Synack has a documented methodology for scoping of every penetration test engagement, including for PCI DSS Requirements 11.3, 11.3.1.a, and 11.3.2.a. The scoping includes working with its clients to clearly identify the cardholder data environment (CDE), hosts and applications to test, and network components to test. The scoping also includes both internal and external testing and testing to verify the effectiveness of network segmentation.
- The SRT generates a complete report of penetration test findings in compliance with PCI Requirements 11.3, 11.3.1.a, and 11.3.2.a.
- Synack uses a cloud-based portal to securely communicate with its clients the status of testing. The portal displays vulnerabilities found, ranks the risks of the vulnerabilities found, and the remediation status of patches implemented by the SRT. The portal serves as the primary point of contact for client support by Synack.
- Synack has clearly defined Rules of Engagement as part of its penetration testing methodology to define what its SRT can and cannot do as part of an engagement.

- The SRT uses a cloud-based approach to testing but also employs a site-to-site VPN for testing of PCI segmentation.
- Synack's penetration testing approach conforms with National Institute of Standards and Technology (NIST) SP800-15 CA-8 standards, and Synack's open vulnerability discovery testing option aligns with OWASP testing guidelines.

SYNACK PENETRATION TESTING METHODOLOGY

The Synack engagement consisted of the following phases:

- Phase One – Onboarding and Launch Preparation: This consists of the following tasks:
  - Reviewing scope and requirements, reviewing remediation plan, and scheduling the launch dates.
  - Client registration for Synack Portal, review of assessment details and coverage, interactions with the SRT, and generation of reports.
- Phase Two – Post Launch and Continuous Support: This consists of the following tasks:
  - Launch of the assessment for confirmed dates and times of SRT testing.
  - Review of vulnerability reports, implementation of patches as necessary, and post assessment reviews.

The Synack penetration testing methodology consists of the following five phases:

- Phase One – Reconnaissance and Discovery: This consists of automated reconnaissance through Hydra, exactly as would be done by a malicious attacker, to check for weak points and vulnerabilities in the client network and system.
- Phase Two – SRT Penetration Testing: The SRT utilizes a variety of tools and techniques similar to those used by a malicious attacker to test the weak points identified as part of the first phase of the process. All testing is routed through the Synack cloud-based gateway.
- Phase Three – Triage: All attack results are analyzed, prioritized, and then filtered to remove invalid or duplicate findings.
- Phase Four – Patch Verification: After a patch for the vulnerability is released, the client can request a re-test to verify the patch remediates the vulnerability. Once the remediation is verified, the client can close the vulnerability.
- Phase Five – Custom Reporting and Performance Consultation: During the entire engagement, the client has access to real-time reporting on demand for all testing activity. Reports can be customized based on the particular needs of the client, including time on target, number of SRT members involved, and tailor-made vulnerability reports.

ASSESSOR COMMENTS

The assessment scope put a significant focus on validating the use of the SRT by a merchant or service provider to meet compliance with PCI Requirement 11.3 for annual penetration testing. Based on Coalfire's review of Synack's documented penetration testing methodology, documented penetration tester vetting process, and reviews of sample penetration test reports, penetration testing conducted by Synack meets compliance with PCI Requirement 11.3.

It should also not be construed that the use of the Synack services guarantees full PCI DSS compliance. Disregarding PCI requirements and security best practice controls for systems and networks inside or outside of PCI DSS scope can introduce many other security or business continuity risks to the merchant. Security and business risk mitigation should be any merchant's goal and focus for selecting security controls. It should also be noted that PCI Requirement 11.3 calls for penetration testing to be done at least annually or after any significant change. It is the responsibility of the merchant to engage Synack annually and after any significant infrastructure or application upgrade or modification to meet this requirement. It is also important to note that the scope of services should include all testing or coverage that is part of Requirement 11.3.

Although this paper specifically addresses PCI compliance, the same basic security principles can be applied when implementing systems that comply with other similar regulations, such as the Gramm-Leach-Bliley Act (GLBA), Sarbanes Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), the EU Global Data Protection Regulations (GDPR), and regulations put forth by the North American Electric Reliability Corporation (NERC) or the Federal Energy Regulatory Commission (FERC).

REFERENCES

Synack website - https://www.synack.com/

PCI Data Security Standard, v3.2 – https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

PCI Penetration Test Guidance Special Interest Group - Penetration_Testing_Guidance_March_2015.pdf

NIST Technical Guide to Information Security Testing and Assessment: nistspecialpublication800-115.pdf

Synack Process & Portal Basics.pdf:

1. Synack Scoping Questionnaire – Defined Questions -May 2018.pdf
2. Host Pentest Report with Missions.pdf
3. WebApp PenTest Report with Missions.pdf
4. Template- Synack Handoff Document-Apr 2018.pdf
5. VettingProcess_01-2018.pdf
6. SRT Terms of USE.pdf

APPENDIX A: PCI REQUIREMENTS COVERAGE MATRIX

COMPLIANCE LEVEL	DESCRIPTION
✓	Compliance directly supported via use of the SRT
✓	Requires action by the organization for full compliance

PCI DSS REQUIREMENTS	COMPLIANCE SUPPORTED	ASSESOR COMMENTS
11.3 Implement a methodology for penetration testing that includes the following: • **Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)** • **Includes coverage for the entire CDE perimeter and critical systems** • **Includes testing from both inside and outside the network** • **Includes testing to validate any segmentation and scope-reduction controls** • **Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5** • **Defines network-layer penetration tests to include components that support network functions as well as operating systems** • **Includes review and consideration of threats and vulnerabilities experienced in the last 12 months** • **Specifies retention of penetration testing results and remediation activities results.**		
11.3 Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months	✓	Coalfire reviewed documentation, interviewed Synack personnel, and confirmed the following: • The SRT test report generated after the conclusion of penetration testing explicitly states it conforms to penetration testing requirements in NIST 800-53. The penetration testing methodology is documented in the Synack Scoping Questionnaire and requires coverage of the CDE perimeter and critical systems, testing both inside and outside the network, and verification of segmentation to all be scoped at the beginning of every pen test engagement. • Synack works with its clients to define the CDE, the hosts and applications to be tested, and the components required for network functionality. Synack then scopes the engagement based on the information provided by the client and only conducts penetration testing on the items the client permits. Part of the definition of the CDE is determined by the client. • Synack requests a list of existing vulnerabilities from the client and uses those to identify what are new vulnerabilities from their penetration test findings.

PCI DSS REQUIREMENTS	COMPLIANCE SUPPORTED	ASSESOR COMMENTS
• Specifies retention of penetration testing results and remediation activities results.		• The client is responsible for retaining the penetration test and remediation action results.
11.3.1 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).		
11.3.1.a Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows: • Per the defined methodology • At least annually • After any significant changes to the environment.	✓	Coalfire reviewed sample pen test reports, interviewed Synack personnel, and confirmed the following: The pen tests follow the documented testing methodology and include the following: • Scoping of the client environment is conducted to successfully determine the scale and technical objectives of the testing. • Quality standards are set to include reproducible steps for the testing. • The vulnerability proof of concept from Synack details remediating vulnerabilities. • Sample reports are clearly marked to indicate the dates of testing. • Sample reports detail the impact of the testing on the environment. However, it is still the responsibility of the Synack client to schedule the testing annually in order to meet PCI compliance.
11.3.1.b Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	✓	All SRT members go through an extensive vetting process to identify their skill sets, experience, and integrity, as outlined in their Vetting Process document.
11.3.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).		
11.3.2.a Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows. • Per the defined methodology • At least annually • After any significant changes to the environment.	✓	Coalfire reviewed sample pen test reports, interviewed Synack personnel, and confirmed the following: The pen tests follow the documented testing methodology and include the following: • Scoping of the client environment is conducted to successfully determine the scale and technical objectives of the testing. • Quality standards are set to include reproducible steps for the testing. • The escalation procedure by Synack details remediating vulnerabilities.

PCI DSS REQUIREMENTS	COMPLIANCE SUPPORTED	ASSESOR COMMENTS
		• Sample reports are clearly marked to indicate the dates of testing. • Sample reports detail the impact on the environment.
11.3.2.b Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	✓	All SRT members go through an extensive vetting process to identify their skill sets, experience, and integrity, as outlined in their Vetting Process document. The Vetting Process document outlines the steps in the process Synack uses for selecting members of the SRT. The process includes the following: • Review of the resume of the pen tester to check for the specific technical skills required by the SRT. • Written and practical testing of the specific skills of the pen tester to verify actual technical knowledge. • Testing of skills internally prepared by Synack, completed in one session, and only allowed to be taken once.
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.		
11.3.3 Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.	✓	Coalfire reviewed sample pen test reports, interviewed Synack personnel, and confirmed the following: • The pen test reports provide evidence that the vulnerability was remediated and verified as such through follow up testing. • The sample reports contain a section called Mission Execution Details, which describes each vulnerability found, the testing conducted, and how the vulnerability was remediated and retested.
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.		
11.3.4.a Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	✓	Coalfire reviewed sample pen test reports, interviewed Synack personnel, and confirmed the following: The pen test reports clearly define the scope of the engagement, the systems tested, and the objective of each test, such as verifying segmentation for PCI. However, it is the responsibility of the client to provide Synack with their segmentation methods and identify out-of-scope systems to not be included in the PCI testing.

PCI DSS REQUIREMENTS	COMPLIANCE SUPPORTED	ASSESOR COMMENTS
11.3.4.b Examine the results from the most recent penetration test to verify that: • Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	✓	Coalfire reviewed sample pen test reports, interviewed Synack personnel and confirmed the following: • Sample reports indicate the date ranges testing was conducted. • Sample reports indicate the scope of the environment tested, such as what network segments and applications were tested and the nature of the testing performed on each component. • Sample reports indicate whether the testing objective was specifically for PCI compliance, which includes verification of segmentation. However, it is still the responsibility of the Synack client to schedule the testing annually in order to meet PCI compliance and to provide details of segmentation so that the SRT can design its testing.
11.3.4.c Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	✓	All SRT members go through an extensive vetting process to identify their skill sets, experience, and integrity, as outlined in their Vetting Process document. The Vetting Process document outlines the steps in the process Synack uses for selecting members of the SRT. The process includes the following: • Review of the resume of the pen tester to check for the specific technical skills required by the SRT. • Written and practical testing of the specific skills of the pen tester to verify actual technical knowledge. • Testing of skills internally prepared by Synack, completed in one session, and only allowed to be taken once.
Note: This requirement applies only when the entity being assessed is a service provider. 11.3.4.1 Examine the results from the most recent penetration test to verify that: • Penetration testing to verify segmentation controls is performed at least every six months and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use.	✓	Coalfire reviewed sample pen test reports, interviewed Synack personnel and confirmed the following: • Sample reports indicate the date ranges testing was conducted. • Sample reports indicate the scope of the environment tested, such as what network segments and applications were tested and the nature of the testing performed on each component. • Sample reports indicate whether the testing objective was specifically for PCI compliance, which includes verification of segmentation. However, it is still the responsibility of the Synack client to schedule the testing every six months in order to

PCI DSS REQUIREMENTS	COMPLIANCE SUPPORTED	ASSESOR COMMENTS
- The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.		meet PCI compliance and to provide details of segmentation so that the SRT can design its testing.

ABOUT THE AUTHORS

Joel Dubin | Senior Consultant | Solution Validation

Joel Dubin (jdubin@coalfire.com) is a Senior Consultant and Application Security Specialist at Coalfire. Joel has several years of experience working as a QSA and PA-QSA helping clients develop systems and software for use in PCI DSS environments and has authored and spoken on multiple security topics including application security, cyber risk management, secure software development, and PCI DSS and PA-DSS compliance. He holds a CISSP, QSA, and PA-QSA.

Bhavna Sondhi | Senior Consultant | Solution Validation

Bhavna Sondhi is a Senior Consultant for the Solution Validation team at Coalfire. Bhavna is responsible for conducting PCI DSS, PA-DSS, and P2PE assessments as well as authoring technical whitepapers. Bhavna joined Coalfire in 2013 and brings over 11 years of software engineering and Information security experience to the team, leading extensive consulting and assessment engagements within USA, Europe, and Asia. As a lead PA-QSA and P2PE-QSA, Bhavna supports assessments for some of the largest payment software providers in the world and her software engineering experience plays a vital part in ensuring the teams recognize the importance of secure code development and information security within their operational practices.

Published June 2018.

ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.

Synack – PCI DSS Penetration Testing June 2018