bugcrowd

Next Gen Pen Test Compliance Applicability Review

January 2019

schellman

Statement Of Confidentiality

The sole purpose of this document is to provide Bugcrowd, Inc. (Bugcrowd) with the results of Schellman's review of their Next Generation Penetration Testing Service as it relates to the Payment Card Industry Data Security Standard (PCI DSS) and other regulatory and compliance requirements on penetration testing.

This document, and any other Bugcrowd related information provided, shall remain the sole property of Bugcrowd and may not be copied, reproduced, or distributed without the prior written consent of Bugcrowd.

Applicability

The information found in this white paper and the conclusions reached were dependent upon the complete and accurate disclosure of information by Bugcrowd.

QSA Independence Disclosure

Schellman & Company, LLC. ("Schellman") reviewed certain aspects of the Next Generation Penetration Testing Service for Bugcrowd from December 17, 2018, through January 11, 2019. During this time, Schellman did not hold any investment or control over Bugcrowd. During the course of this review, Schellman and the QSA did not market services for the purpose of assisting Bugcrowd in meeting any regulatory requirements pertaining to the penetration testing services reviewed as part of this white paper. No Schellman service was recommended during the course of the engagement.

Schellman also performed the SOC 2 type 1 and 2 and ISO 27001 examination for Bugcrowd concurrently with the assessment.

SECTION 1: EXECUTIVE SUMMARY

Purpose

Schellman performed a review of Bugcrowd's Crowdsourced Next Generation Penetration Testing (Next Gen Pen Test) service for alignment with applicable penetration testing requirements of the PCI Data Security Standard, ISO:IEC 27001 Annex A, and NIST 800-53 revision 4. This assessment was completed in January 2019 by Matt Crane, Senior Associate at Schellman & Company, LLC.

Objective

The objective of this assessment was to assist Bugcrowd in validating how the service enables its customers to meet applicable compliance requirements for penetration testing. This assessment specifically targeted the following areas:

- Standard agreements and instructions provided to customers
- Standard and customizable reports available to customers

schellman | bugcrowd

SECTION 1: EXECUTIVE SUMMARY

Company Background And Services Provided

Company Background

Bugcrowd is a crowdsourced security platform primarily used for vulnerability identification through the management of vulnerability disclosure programs, bug bounties, and crowdsourced penetration testing services. Bugcrowd's principle service offerings are fueled by a collective community of knowledge for the identification and reporting of security vulnerabilities, which are validated, triaged, and prioritized by Bugcrowd. Bugcrowd advocates that a community of researchers continuously testing an environment's security features is significantly more valuable than traditional penetration testing services. Bugcrowd provides its customers with access to a crowd of researchers without the management oversight needed by the customer to monitor.

Next Gen Pen Test

The Bugcrowd Next Gen Pen Test service aims to satisfy requirements from auditors and reviewers with security standards in mind to meet various regulatory and compliance requirements. In a traditional crowdsourced security program, where a defined methodology is difficult to track in the reporting of the vulnerabilities, the incentivization for reporting vulnerabilities quickly can pose issues for companies attempting to comply with regulatory and compliance standards. Bugcrowd has addressed this issue with the introduction of Next Gen Pen Test. In this model, Bugcrowd layers the continuous bounty-incentivized testing of the crowd with the grant-incentivized testing of dedicated pen testers and researchers following a defined methodology. Bugcrowd employees then review, validate, and triage all findings, before combining into a compliance friendly reporting format. This ensures a repeatable, defensible methodology is followed every time.

Bug Bounty Programs

Bugcrowd offers a managed bug bounty service in which they are the mediator between their customers and a crowd of researchers. The bug bounty program allows organizations to have their environments or applications tested by a large community of white hat hackers. Customers have the choice between a private bug bounty and a public bug bounty program. Private bug bounties are by invitation only and ensure all crowdsourced researchers involved have gone through a vetting process. Public bug bounties are available to the entire Bugcrowd community of researchers and are promoted and publicized by Bugcrowd on their website.

SECTION 1: EXECUTIVE SUMMARY

Summary Of Findings

During the review of Bugcrowd's Next Gen Pen Test, Schellman made the following observations that are further explained throughout the rest of this white paper:

- Bugcrowd's Next Gen Pen Test Service offering appears to directly assist organizations in meeting the requirements in PCI 6.6 for testing public facing web applications.
- The Next Gen Pen Test methodology directly supports organizations in achieving compliance with PCI requirement 11.3 for internal and external penetration testing as long as the customer adequately defines the scope of their environment.
- The service offering provided has a limited capacity to meet PCI requirements for segmentation testing. This limitation can be overcome if customers take a few extra steps in defining segmentation controls, and reviewing the results of segmentation testing to determine if the segmentation controls were adequate.
- Schellman reviewed the Next Gen Pen Test methodology in collaboration with a sample report and noted that the service offering directly supports NIST 800-53 rev4 CA-8 and ISO 27001 A.12.6.1 requirements for penetration testing.

Although the use of bug bounty programs can be useful in identifying vulnerabilities and increasing an organizations information security architecture, on their own they do not provide organizations with much assistance in meeting regulatory and compliance requirements.

SECTION 2: PENETRATION TESTING METHODOLOGY

Next Generation Penetration Testing Methodology

Alignment with Industry Standards

Schellman observed Bugcrowd's defined testing methodology and noted that it aligned with multiple industry standards for technical testing to include NIST SP 800-115 and the OWASP Testing Guide v4. Review of an example penetration testing report showed that alignment with the aforementioned industry standards was consistent and met various regularity and compliance requirements, such as the PCI DSS, NIST 800-53 rev4 and ISO 27001. Further review of the methodology, in conjunction with PCI requirements 6.6 and 11.3, can be found in section three of this white paper. Bugcrowd's methodology for conducting Next Gen Pen Tests directly uses the OWASP Testing Guide v4 and its web application security testing steps. Schellman observed an example Next Gen Pen Test report and noted that each step was included in the testing practices.

Service Options

Bugcrowd's Next Gen Pen Test service offering includes two options for its customers to choose from; time bound testing and ongoing. Time bound testing is done in a manner where the customer chooses the start and end date for which Bugcrowd will conduct the Next Gen Pen Test. All activities conducted by Bugcrowd and its pool of crowdsourced researchers are completed during the period identified by the customer. Customers were responsible for ensuring that the time frame of the timebound Next Gen Pen Test was adequate to meet various regulatory and compliance requirements.

Ongoing testing is where customers allow continuous testing of their environments. This assessment type provides more coverage of a customer's environment and allows Bugcrowd's crowdsourced researchers to conduct continuous testing. Ongoing testing allows Bugcrowd's pool of researchers continuous access to the customers environment. Constant testing allows customer environments to be tested after significant changes or as new vendor vulnerabilities are published. Furthermore, ongoing testing ensures that remediation activities can be adequately retested by a Bugcrowd employee.

SECTION 2: PENETRATION TESTING METHODOLOGY

Testing Methodology

The methodology for performing a Next Gen Pen Test is split into four phases; reconnaissance, enumeration, proof of concept, and documentation. When reviewing common industry penetration testing standards, such as NIST SP 800-115, Bugcrowd identified similarities in the workflow of industry standards and used these similarities to develop the methodology used in the Next Gen Pen Test. Schellman reviewed the defined testing methodology and confirmed that the phases adequately followed the guidance provided by NIST SP 800-115 on performing a phased information security assessment.

Each of the phases are executed in a cyclical manner allowing penetration testers to build upon findings and potentially uncover significant risks. The reconnaissance phase begins with the customer providing information regarding the scope of the Next Gen Pen Test. In this phase, customers will identify external URLs and IP addresses to be tested, provide access to internal environments, and provide information regarding the network architecture and segmentation controls. Additionally, the reconnaissance phase includes information gathering by the community of researchers selected for the Next Gen Pen Test.

The enumeration phase is where researchers identify attack vectors based on information gathered in the reconnaissance phase. Once a researcher has identified a vulnerability, they seek to verify the issue by creating a proof of concept to prove the existence of the vulnerability. The researcher then reports the vulnerability to Bugcrowd in the documentation phase. Bugcrowd personnel will then confirm the vulnerability is a legitimate issue that has not already been reported. If the vulnerability is real and has not been reported in the past, Bugcrowd will triage, prioritize, and attach remediation advice to the vulnerability before providing the information to the customer. Customers can see all confirmed vulnerabilities in the vulnerability analytics dashboard that they access through their account in Bugcrowd's Crowdcontrol platform.

Remediation Testing

As part of their Next Gen Pen Test service offering, Bugcrowd offers remediation testing to customers seeking to confirm that a vulnerability previously identified was successfully fixed. Bugcrowd employees conduct the test and update the vulnerability analytics dashboard, as well as the report. In a standard ongoing Next Gen Pen Test, there could be multiple instances in a given year where a confirmed vulnerability was remediated, and a Bugcrowd employee performed testing to confirm that remediation was effective.

SECTION 2: PENETRATION TESTING METHODOLOGY

Crowdsourced Researcher Selection

During the course of the engagement, Bugcrowd provided information regarding the selection and categorization of researchers in their crowdsourced community. Schellman did not perform testing or a review of this categorization process, but felt it was pertinent to include in this report. Only researchers that had undergone a background check and displayed an adequate level of skill were eligible to participate in Next Gen Pen Tests. In addition to requiring ID verification and background checks to meet various levels of trust, Bugcrowd uses these trust levels combined with a researcher's demonstrated skill to identify an elite group, referred to as the "Elite Crowd." These skilled penetration testers and white hat hackers are measured in two key areas: Skill and Trust.

SKILL

A standard of high-impact submissions, averaging only high and critical submissions across a range of specific attack surface areas.

TRUST

Proven trust through ID verification and success working on private programs for top customers.

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility		Assessor Findings
	Customer	Next Gen Pen Test	
PCI 6.6: For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:			
• Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods – as follows:		✓	Schellman observed Bugcrowd's Next Gen Pen Test methodology along with a sample penetration test report and noted that it meets the requirements of a manual application vulnerability security assessment.
• At least annually	✓	✓	A customer's use of a Next Gen Pen Test to meet this requirement on an annual basis is contingent upon the following: • Customers are responsible for ensuring all applicable public-facing web applications are identified and communicated to Bugcrowd • If a customer selects a timebound test, the customer is responsible for ensuring the time frame identified is adequate to allow for complete testing of the public-facing web application(s) in scope
• After any changes	✓	✓	Review of an example Next Gen Pen Test indicated that Bugcrowd's service offering directly supports testing changes to public-facing web applications with the following caveats: • Only changes made during the contracted testing window would be tested • If a timebound Next Gen Pen Test is selected by the customer, only changes that are made during the identified time frame will be tested
• By an organization that specializes in application security		✓	Schellman interviewed the Chief Security Officer at Bugcrowd and noted that researchers selected for Next Gen Pen Test specialized in application security. Furthermore, Bugcrowd utilized a process for selecting researchers based on skill* observed during previous private and public bug bounty programs. *Additional information regarding researcher skill determination can be found in Section 2 of this white paper.

SECTION 3:
COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility		Assessor Findings
	Customer	Next Gen Pen Test	
• That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment		✓	Schellman reviewed Bugcrowd's Next Gen Pen Test methodology and noted that application testing processes directly followed the OWASP Testing Guide v4, which includes testing of all vulnerabilities identified in requirement 6.5.
• That all vulnerabilities are corrected	✓		Bugcrowd customers are responsible for correcting all vulnerabilities identified. Bugcrowd provides some guidance for vulnerabilities identified during testing activities, but it is the customers responsibility to ensure all vulnerabilities are corrected.
• That the application is re-evaluated after the corrections.	✓	✓	Customers are responsible for notifying Bugcrowd that a vulnerability has been corrected. Bugcrowd will then task employees, not the pool of crowdsourced researchers, to confirm that remediation activities conducted by the customer were effective. In the event that a customer has elected to use the timebound Next Gen Pen Test service, the customer is responsible for ensuring that the time frame of the test allows Bugcrowd the ability to conduct remediation testing.
• Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	✓		Not applicable. Customers using Bugcrowd's Next Gen Pen Test service do not need to implement an automated technical solution to meet PCI requirement 6.6.

schellman | bugcrowd

SECTION 3:
COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility		Assessor Findings
	Customer	Next Gen Pen Test	
11.3: Implement a methodology for penetration testing that includes the following:			
• Is based on industry-accepted penetration testing approaches (for example, NIST SP 800-115)		✓	Schellman reviewed Bugcrowd's Next Gen Pen Test methodology and noted that it aligned with NIST SP 800-115 and the OWASP Testing Guide v4. As recommended by NIST SP 800-115, the methodology provided to Schellman was repeatable, included the objective of the testing and contained processes for defining and categorizing vulnerabilities. Bugcrowd's Next Gen Pen Test methodology also included each step defined in the OWASP Testing Guide v4.
• Includes coverage for the entire CDE perimeter and critical systems	✓	✓	Bugcrowd's customers are responsible for defining the scope of the environment to be tested. Once the customer has confirmed the scope of the assessment, they are responsible for providing this information to Bugcrowd and ensuring it includes the entire perimeter of the environment and all critical systems. In regard to internal penetration testing, Bugcrowd's Next Gen Pen Test can only cover systems and environments that the customer identifies and provides access to.
• Includes testing from both inside and outside the network	✓	✓	Bugcrowd's Next Gen Pen Test has the capacity to test various aspects of a customer's environment from both inside and outside of the network. It is the customer's responsibility to ensure Bugcrowd's researchers have access to systems inside the network if the customer desires internal testing to be completed. The customer is also responsible for granting access to internal network segments.

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility		Assessor Findings
	Customer	Next Gen Pen Test	
• Includes testing to validate any segmentation and scope-reduction controls	✓	✓	Customers are responsible for defining and determining the appropriateness of segmentation controls in their environments. Bugcrowd's Next Gen Pen Test has the capacity to assist in meeting PCI requirements for segmentation testing as long as the customer does the following: • Customers must request segmentation testing • Customers are responsible for defining segmentation controls and interpreting the results of the segmentation test to determine if segmentation controls implemented by the customer are operational and effective • Customers must include all segmentation controls/methods in the information provided to Bugcrowd in order to ensure all controls/methods are tested
• Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5		✓	Schellman observed Bugcrowd's Next Gen Pen Test methodology and noted that application testing processes directly followed the OWASP Testing Guide v4, which includes testing of all vulnerabilities identified in requirement 6.5.
• Defines network-layer penetration tests to include components that support network functions as well as operating systems	✓		Observation of example penetration tests conducted under the Next Gen Pen Test methodology indicate that customers are responsible for defining network-layer penetration tests. Through interviews with the Chief Security Officer at Bugcrowd, Schellman noted that Bugcrowd had the capacity to conduct network-layer penetration testing, but customers were responsible for defining and identifying components that support network functions, and customers must request network-layer penetration testing as part of their ongoing or timebound Next Gen Pen Test. Note: Schellman reviewed an example internal network penetration test conducted in 2016 that was performed as part of a different service offering prior to the development and offering of Next Gen Pen Test. It is reasonable to assume that Bugcrowd personnel have the capacity to perform network-layer penetration testing, but Schellman was unable to validate this as part of this assessment.

SECTION 3:
COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility		Assessor Findings
	Customer	Next Gen Pen Test	
• Includes review and consideration of threats and vulnerabilities experienced in the last 12 months	✓	✓	As part of Bugcrowd's broader vulnerability management service offerings, Bugcrowd offers customers access to a Crowdcontrol platform that contains a vulnerability analytics dashboard. Customers subscribing to the Next Gen Pen Test service offering have access to these services for viewing vulnerability information. Schellman observed an example of the vulnerability analytics dashboard and noted that it was designed to retain vulnerability information for the duration of a customer's relationship with Bugcrowd. Customers are responsible for retaining formal penetration test reports and findings delivered to them at the end of both timebound and ongoing Next Gen Pen Tests. Customers are also responsible for retaining records of any and all vulnerabilities identified prior to the start of services from Bugcrowd. Further, customers are responsible for maintaining a vulnerability management policy in conjunction with PCI requirement 6.1.
• Specifies retention of penetration testing results and remediation activities results.	✓	✓	Schellman observed Bugcrowd's penetration testing methodology and noted that retention of testing results would occur for the duration of the contracted relationship between Bugcrowd and their customers. Customers have a shared responsibility to maintain formal testing results as part of their applicable data retention and vulnerability management policies. Customers electing to use the timebound Next Gen Pen Test service offering are responsible for retaining all testing results after the defined period has concluded with Bugcrowd. Although Bugcrowd retains information regarding the vulnerabilities and results of testing, the customer is ultimately responsible for retaining formal reports for the purposes of meeting regulatory requirements to include the PCI-DSS.

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility		Assessor Findings
	Customer	Next Gen Pen Test	
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).			
PCI 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.	✓	✓	Schellman observed program details and an example penetration testing report under Bugcrowd's Next Gen Pen Test service offering and noted the following: • Customers are responsible for defining the scope of external penetration tests • Observation of the example penetration test shared with Schellman indicated the defined methodology was followed • Use of the Ongoing Next Gen Pen Test provides direct support of conducting external penetration testing on an annual basis with a formal report being delivered at an agreed upon date. • The Ongoing Next Gen Pen Test allows for continuous testing of customer environments to include after significant changes. Depending on the nature of a change, Customers will likely need to notify Bugcrowd to ensure ongoing testing includes checks for additional security issues introduced by the change to the customers environment. Customers electing a Timebound Next Gen Pen Test will need to ensure the duration of time is adequate to address significant changes and that a timebound penetration test is conducted at least annually.
PCI 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).		✓	Schellman interviewed the Chief Security Officer at Bugcrowd and noted that researchers selected for Next Gen Pen Test were qualified to conduct external penetration tests. Furthermore, Bugcrowd utilized a process for selecting researchers based on skill. Additional information regarding researcher skill determination can be found in section 2 of this white paper. Finally, Bugcrowd's Crowdsourced researchers were neither involved in remediation activities nor were they involved in remediation testing, thus indicating organizational independence.

SECTION 3:
COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility		Assessor Findings
	Customer	Next Gen Pen Test	
PCI 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).			
PCI 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.	✓	✓	Schellman observed program details and an example penetration test report under a predecessor of the Next Gen Pen Test service offering* and noted the following: • Customers are responsible for defining the scope of internal penetration tests • Observation of the example penetration test shared with Schellman indicated the defined methodology was followed • Use of the Ongoing testing service offering provides direct support of conducting internal penetration testing on an annual basis with a formal report being delivered at an agreed upon date. • The Ongoing Next Gen Pen Test allows for continuous testing of customer environments to include after significant changes. Depending on the nature of a change, customers will likely need to notify Bugcrowd to ensure ongoing testing includes checks for additional security issues introduced by the change to the customers environment. Customers choosing to conduct a Timebound Next Gen Pen Test will need to ensure the duration of time is adequate to address significant changes and that a timebound penetration test is conducted at least annually. *Schellman reviewed an example internal network penetration test conducted in 2016 that was performed as part of a different service offering prior to the development of the Next Gen Pen Test. It is reasonable to assume that Bugcrowd personnel have the capacity to perform network-layer penetration testing, but Schellman was unable to validate this as part of this assessment.

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility		Assessor Findings
	Customer	Next Gen Pen Test	
PCI 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).		✓	Schellman interviewed the Chief Security Officer at Bugcrowd and noted that researchers selected for Next Gen Pen Test were qualified to conduct internal penetration tests. Further, Bugcrowd utilized a process for selecting researchers based on skill. Additional information regarding researcher skill determination can be found in section 2 of this white paper. Finally, Bugcrowd's Crowdsourced researchers were not involved in remediation activities nor were they involved in remediation testing, thus indicating organizational independence.
PCI 11.3.3: Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.			
PCI 11.3.3 Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.	✓	✓	Because customers are responsible for all remediation activities, customers also share the responsibility for the re-evaluation of all corrected vulnerabilities. Customers are responsible for notifying Bugcrowd that an exploitable vulnerability previously identified by Bugcrowd has been remediated. Bugcrowd will then use Bugcrowd employees, not the pool of crowdsourced researchers, to confirm that remediation activities conducted by the customer were effective. In the event that a customer has elected to use the timebound Next Gen Pen Test service, the customer is responsible for ensuring that the period identified allows Bugcrowd the ability to conduct remediation testing.
PCI 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.			
PCI 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.	✓	✓	Customers are responsible for defining and determining the appropriateness of segmentation controls in their environments. Bugcrowd's Next Gen Pen Test has the capacity to assist in meeting PCI requirements for segmentation testing as long as the customer does the following: • Customers must request segmentation testing

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility		Assessor Findings
	Customer	Next Gen Pen Test	
PCI 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.	✓	✓	Customers are responsible for defining segmentation controls and interpreting the results of the segmentation test to determine if segmentation controls are operational and effective Customers must include all segmentation controls/methods in the information provided to Bugcrowd in order to ensure all controls/methods are tested
PCI 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).	✓	✓	Schellman interviewed the Chief Security Officer at Bugcrowd and noted that researchers selected for Next Gen Pen Test were qualified to conduct segmentation penetration tests. Further, Bugcrowd utilized a process for selecting researchers based on skill. Additional information regarding researcher skill determination can be found in section 2 of this white paper. Finally, Bugcrowd's Crowdsourced researchers were not involved in remediation activities nor were they involved in remediation testing, thus indicating organizational independence. Customers are responsible for ensuring the organizational independence of individual(s) that review the segmentation test findings to determine if segmentation controls implemented by the customer are operational and effective.

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility		Assessor Findings
	Customer	Next Gen Pen Test	
PCI 11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.			
PCI 11.3.4.1.a Examine the results from the most recent penetration test to verify that: • Penetration testing is performed to verify segmentation controls at least every six months 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.	✓	✓	Bugcrowd's Next Gen Pen Test has the capacity to assist in meeting PCI requirements for segmentation testing as long as the customer does the following: • Customers must request segmentation testing to be conducted every six months • Customers are responsible for defining segmentation controls and interpreting the results of the segmentation test to determine if segmentation controls implemented are operational and effective • Customers must include all segmentation controls/method in the information provided to Bugcrowd in order to ensure all controls/methods are tested
PCI 11.3.4.1.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).	✓	✓	Schellman interviewed the Chief Security Officer at Bugcrowd and noted that researchers selected for Next Gen Pen Test were qualified to conduct segmentation penetration tests. Further, Bugcrowd utilized a process for selecting researchers based on skill. Additional information regarding researcher skill determination can be found in section 2 of this white paper. Finally, Bugcrowd's Crowdsourced researchers were not involved in remediation activities nor were they involved in remediation testing, thus indicating organizational independence. Customers are responsible for ensuring the organizational independence of individual(s) that review the segmentation test findings to determine if segmentation controls implemented by the customer are operational and effective.

SECTION 3:
COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility		Assessor Findings
	Customer	Next Gen Pen Test	
NIST 800-53 Rev4 CA-8. The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].	✓	✓	Schellman reviewed the methodology for the Next Gen Pen Test used by Bugcrowd and an example report and noted that testing performed by Bugcrowd supports this control.
ISO 27001 Annex A.12.6.1. Management of technical vulnerabilities. Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	✓	✓	Schellman reviewed the methodology for the Next Gen Pen Test and an example report and noted that identification of vulnerabilities during the ongoing, or timebound service offering supported the identification of vulnerabilities in a timely manner. Further, noted that customers were responsible for taking appropriate measures to address any risks identified during the Next Gen Pen Test.

schellman

www.schellman.com