bugcrowd

Next Gen Pen Test & Classic Pen Test Compliance Applicability Review

June 2020

schellman

Statement of Confidentiality

The purpose of this document is to provide Bugcrowd, Inc. (Bugcrowd) with the results of Schellman's review of their Classic Penetration Testing (Classic Pen Test) and Next Generation Penetration Testing (Next Gen Pen Test) services 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 Test and Classic Pen Test Services for Bugcrowd from June 15, 2020, through June 19, 2020. 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 2 and ISO 27001 examination for Bugcrowd prior to the assessment.

Table of Contents

SECTION 1: EXECUTIVE SUMMARY

Purpose

Schellman performed a review of Bugcrowd's Crowdsourced Classic Penetration Testing (Classic Pen Test) and Next Generation Penetration Testing (Next Gen Pen Test) services for alignment with applicable penetration testing requirements of the PCI Data Security Standard v3.2.1, ISO:IEC 27001 Annex A, Cybersecurity Maturity Model Certification CA.4.164, and NIST 800-53 revision 4. This assessment was completed in June 2020 by Todd Busswitz, 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

SECTION 1: EXECUTIVE SUMMARY

Company Background & Services Provided

Company Background

Bugcrowd is a Crowdsourced security platform that helps customers infuse the power of the Crowd into all of their security testing initiatives. The platform provides solutions for secure vulnerability disclosure, bug bounties, penetration testing, and attack surface management. Bugcrowd's principal service offerings are fueled by a collective community of knowledge for the rapid identification and reporting of previously unknown attack surface and security vulnerabilities, which are validated, triaged, and prioritized by Bugcrowd. Real-time vulnerability view, and 24/7 reporting are offered via the Bugcrowd customer console for enhanced visibility throughout every engagement. Bugcrowd advocates that a community of highly vetted researchers provides significantly more value than traditional penetration testing services.

Next Gen Pen Test

Bugcrowd Next Gen Pen Test aims to encourage greater vulnerability discovery while helping organizations satisfy various regulatory and compliance requirements. In a traditional pay-for-results crowdsourced security program, researchers are incentivized to find vulnerabilities before the competition, which is at odds with the motivation to follow a defined methodology. This can pose issues for companies attempting to leverage a bug bounty program for compliance purposes. Bugcrowd has addressed this issue with the introduction of Next Gen Pen Test. In this model, Bugcrowd deploys bounty-incentivized researchers alongside grant-incentivized pen testers to ensure a defined methodology is completed in full. They accomplish this with the help of their CrowdMatch Skills Selection technology to identify the proper resource(s) with the appropriate knowledge and demonstrated aptitude for the environment to be tested. Additional service options for Next Gen Pen Test include premium Service Level Agreements (SLA), coverage analysis, and vulnerability retesting. Bugcrowd employees review, validate, and triage all findings, before combining them into a compliance friendly reporting format. This ensures a repeatable, defensible methodology is followed every time.

SECTION 1: EXECUTIVE SUMMARY

Classic Pen Test

Bugcrowd Classic Pen Test aims to satisfy requirements from auditors and reviewers in a pay-for-time format that may be more amenable to certain procurement or budgetary requirements. In this model, Bugcrowd leverages the same global Crowd of talent, automatically matched, and managed for each testing engagement, though unlike Next Gen Pen Test, researchers are not incentivized for findings beyond completion of the standardized methodology. Bugcrowd employees perform the same review, validation, and triage for all findings, before combining them into a compliance friendly reporting format. Coverage analysis, premium SLAs, and options for continuous testing are not available through Classic Pen Test, though expedited reporting and vulnerability retesting can be added for an additional charge.

Summary of Findings

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

- Bugcrowd Classic Pen Test and Next Gen Pen Test Service offering appear to directly assist organizations in meeting the requirements in PCI 6.6 for testing public-facing web applications.
- The penetration testing methodology, for both Classic Pen Test and Next Gen Pen Test, directly support organizations in achieving compliance with PCI requirement 11.3 for internal and external penetration testing when the customer adequately defines the scope of their environment.
- Classic Pen Test and Next Gen Pen Test have the capacity to meet PCI requirement 11.3.4 and 11.3.4.1 for segmentation testing, as long as the customer defines segmentation controls and reviews the results of segmentation testing to determine if the segmentation controls were adequate.
- Schellman reviewed the Classic Pen Test and Next Gen Pen Test methodologies in collaboration with sample reports and noted that the service offering directly supports NIST 800-53 rev4 CA-8, Cybersecurity Maturity Model Certification CA.4.164 and ISO 27001 A.12.6.1 requirements for penetration testing.

Although the use of bug bounty programs can assist in identifying vulnerabilities to enhance an organization's information security architecture, on their own they do not provide 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, Web Application Hacker Handbook Methodology (WAHHM), SANS Top 25, Council of Registered Ethical Security Testing (CREST), Open Source Security Testing Methodology Manual (OSSTMM), Web Application Security Consortium (WASC), Penetration Testing Execution Standard (PTES) and the OWASP Testing Guide v4. Review of example penetration testing reports showed that alignment with the aforementioned industry standards was consistent with various regulatory and compliance requirements, such as the PCI DSS v 3.2.1, Cybersecurity Maturity Model Certification CA.4.164, 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 a Next Gen Pen Test directly uses the OWASP Testing Guide v4 and its web application security testing steps. Schellman observed example Next Gen Pen Test reports 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 continuous. 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.

The continuous testing service is the most commonly chosen delivery format for Next Gen Pen Test, and provides ongoing testing throughout the year, with methodology-based testing triggered whenever the client specifies. This testing type provides a select subset of researchers and pen testers controlled, continuous access to the customer's environment. Continuous testing allows customer environments to be tested after significant changes,

SECTION 2: PENETRATION TESTING METHODOLOGY

upon request, or as new known Common Vulnerabilities and Exposures (CVEs) are published. When a new methodology-driven report is requested, the customer must notify Bugcrowd to arrange for this style of testing to commence. Retesting can also be requested when vulnerabilities are remediated, in order to ensure a clean compliance report.

Testing Methodology

The methodology for performing a Next Gen Pen Test is split into four phases: reconnaissance, enumeration, exploitation, 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 move to the exploitation phase and seek to verify the issue by creating a proof of concept to prove the existence of the vulnerability. The researcher completes the four phased process by reporting 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 can be validated, 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.

SECTION 2: PENETRATION TESTING METHODOLOGY

Retesting

As part of their Next Gen Pen Test solution, Bugcrowd includes re-testing services 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 would 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.

Classic Penetration Testing Methodology

Alignment with Industry Standards

Bugcrowd Classic Pen Test utilizes the same defined testing methodology as is leveraged for Next Gen Pen Test. Review of example Classic Pen Test reports showed that the alignment with the aforementioned industry standards was consistent between the two solutions. 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 a Classic Pen Test uses the same OWASP Testing Guide v4 and its web application security testing steps as the Next Gen Pen Test. Schellman observed example Classic Pen Test reports and noted that each step was included in the testing practices.

Service Options

Bugcrowd's Classic Pen Test service offering includes a standard penetration test for its customers with the ability to add on additional services such as expedited testing and retesting. Customers are responsible for ensuring that the scope of the Classic Pen Test engagement is adequate to meet various regulatory and compliance requirements.

Testing Methodology

The methodology for performing Classic Pen Test is split into the same four phases as was enumerated for Next Gen Pen Test above. 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

SECTION 2: PENETRATION TESTING METHODOLOGY

assessment. The process for each of the four phases is the same as the Next Gen Pen Test process listed above. Similar to Next Gen Pen Test, customers can see all vulnerabilities as soon as they are submitted, in the vulnerability analytics dashboard which can be accessed through their account in the Bugcrowd platform.

Retesting

As an add-on to their Classic Pen Test service offering, Bugcrowd offers retesting 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. When the retesting option is added to Classic Pen Test, a Bugcrowd employee performs the retesting to confirm that the remediation was effective for the identified vulnerabilities and provides an updated report.

Researcher & Pen Tester Selection

During the course of the engagement, Bugcrowd provided information regarding the selection and categorization of security testers 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 and pen testers that meet strict trust and skill requirements and have demonstrated success in the environment requiring testing are eligible to participate in Classic and Next Gen Pen Test engagement. Depending on customer requirements, this level of vetting may include ID verification, background checks, and geolocation. Exceptionally talented and trusted testers are placed into the category of "Elite Crowd," reserved for certain advanced engagements.

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	Classic Pen Test	Next Gen Pen Test (including Timebound)	
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 Classic and Next Gen Pen Tests methodologies along with sample penetration test reports for each type and noted that they meet the requirements of a manual application vulnerability security assessment.
• At least annually	✓	✓	✓	A customer's use of a Classic and 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 Next Gen Pen 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 example Classic and Next Gen Pen Test reports indicated that Bugcrowd's service offering directly support 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 • Only applicable for a Classic Pen Test if the change occurred just prior to the penetration test being performed

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility			Assessor Findings
	Customer	Classic Pen Test	Next Gen Pen Test (including Timebound)	
• By an organization that specializes in application security		✓	✓	Schellman interviewed the Head of Operations at Bugcrowd and noted that researchers selected for Classic and Next Gen Pen Tests 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.
• That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment		✓	✓	Schellman reviewed Bugcrowd's Classic and Next Gen Pen Test methodologies 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 guidance for remediating the vulnerabilities identified during the testing period, but it is the customer's 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 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 retesting. For a Classic Pen Test, in order for the customer to have their remediation efforts confirmed, they would have to purchase the retesting add-on from Bugcrowd as it is not included as part of the basic Classic Pen Test package.

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility			Assessor Findings
	Customer	Classic Pen Test	Next Gen Pen Test (including Timebound)	
• 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 Classic and Next Gen Pen Test services do not need to implement an automated technical solution to meet PCI requirement 6.6.
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 Classic and Next Gen Pen Test methodologies and noted that they 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 Classic and Next Gen Pen Test methodologies 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. Regarding internal penetration testing, Bugcrowd's Classic and Next Gen Pen Test solutions can only cover systems and environments for which the customer identifies and provides access. Further, the Next Gen Pen Test Essential service tier does not include internal testing. Customers would need to purchase either a Professional or Enterprise Next Gen Pen Test to ensure internal testing is included.

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility			Assessor Findings
	Customer	Classic Pen Test	Next Gen Pen Test (including Timebound)	
• Includes testing from both inside and outside the network	✓	✓	✓	Bugcrowd's Classic and Next Gen Pen Test solutions have 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 testers 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. Further, the Next Gen Pen Test Essential service tier does not include internal testing. Customers would need to purchase either a Professional or Enterprise Next Gen Pen Test to ensure internal testing is included.
• 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 Classic and Next Gen Pen Test solutions have 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 Classic and Next Gen Pen Test methodologies and noted that application testing processes directly followed the OWASP testing Guide v4, which includes testing of all vulnerabilities identified in requirement 6.5.

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility			Assessor Findings
	Customer	Classic Pen Test	Next Gen Pen Test (including Timebound)	
• Defines network-layer penetration tests to include components that support network functions as well as operating systems	✓			Observation of example penetration tests conducted under Classic and Next Gen Pen Test methodologies indicate that customers are responsible for defining network-layer penetration tests. Through interviews with the Head of Operations 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 Classic or Next Gen Pen Test engagements.
• 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 platform that contains a vulnerability analytics dashboard. Customers of the Classic and Next Gen Pen Test solutions have access to these services for viewing and progressing vulnerabilities through the security development lifecycle. 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 the formal penetration test reports and findings delivered to them at the end of both Classic and Next Gen Pen Test engagements (continuous and/or timebound). Customers are also responsible for retaining 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.

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility			Assessor Findings
	Customer	Classic Pen Test	Next Gen Pen Test (including Timebound)	
• 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 Classic and timebound Next Gen Pen Test solutions are responsible for retaining all testing results after the defined period has concluded with Bugcrowd. Although Bugcrowd retains information regarding the vulnerabilities, 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	Classic Pen Test	Next Gen Pen Test (including Timebound)	
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 example penetration testing reports under Bugcrowd's Classic and Next Gen Pen Test solutions and noted the following: • Customers are responsible for defining the scope of external penetration tests • Observation of the example penetration test reports shared with Schellman indicated the defined methodology was followed • Use of Next Gen Pen Test provides direct support for conducting external penetration testing on an annual basis with a formal report being delivered at an agreed upon date. Additional testing periods and subsequent reports can be purchased on top of any Next Gen Pen Test engagement. Next Gen Pen Test allows for ongoing testing of customer environments. Depending on the significance of a change, customers will likely need to notify Bugcrowd to ensure the methodology includes checks for additional security issues introduced by the change to the customers environment.
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 Head of Operations at Bugcrowd and noted that pen testers selected for Classic and Next Gen Pen Tests were qualified to conduct external penetration tests. Furthermore, Bugcrowd utilized a process for selecting testers based on skill*. Finally, Bugcrowd's Crowdsourced researchers were neither involved in remediation activities nor were they involved in retesting thus indicating organizational independence. *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	Classic Pen Test	Next Gen Pen Test (including Timebound)	
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 example penetration test reports for the Classic and Next Gen Pen Test service offerings* and noted the following: • Customers are responsible for defining the scope of internal penetration tests • Observation of the example penetration tests shared with Schellman indicated the defined methodology was followed • Use of the continuous testing service option provides direct support for conducting internal penetration testing on an annual basis with a formal report being delivered at an agreed upon date. • The continuous testing service option for Next Gen Pen Test allows for ongoing testing of customer environments after incremental changes to the environment. Depending on the nature of a change, customers will likely need to notify Bugcrowd to ensure 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 any significant changes and that a Classic or timebound penetration test is conducted at least annually. *The customer would have to select an additional option to include the internal network and segmentation in their penetration testing and report. The Next Gen Pen Test Essential service tier does not include internal testing. Customers would need to purchase either a Professional or Enterprise Next Gen Pen Test to ensure internal testing is included.

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility			Assessor Findings
	Customer	Classic Pen Test	Next Gen Pen Test (including Timebound)	
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 Head of Security at Bugcrowd and noted that pen testers selected for Classic and Next Gen Pen Tests 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 pen testers were not involved in remediation activities nor were they involved in re retesting 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 service option for Next Gen Pen Test, the customer is responsible for ensuring that the period identified allows Bugcrowd the ability to conduct retesting. For customers choosing Classic Pen Test, they will have to notify Bugcrowd of their desire for the add-on of retesting in order to confirm the vulnerability remediation.

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility			Assessor Findings
	Customer	Classic Pen Test	Next Gen Pen Test (including Timebound)	
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 Classic and Next Gen Pen Test solutions have 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 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 • Customers using Next Gen Pen Test must purchase the Professional or Enterprise tier as the Essential tier does not include internal segmentation testing

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility			Assessor Findings
	Customer	Classic Pen Test	Next Gen Pen Test (including Timebound)	
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 and determining the appropriateness of segmentation controls in their environments. Bugcrowd's Classic and Next Gen Pen Test solutions have the capacity to assist in meeting PCI requirements for segmentation testing as long as the customer does the following: • Customers must request segmentation testing as a part of the annual penetration test report • Customers must request a segmentation only penetration test at the midpoint between the two annual reports (six month mark) • 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 • Customers must inform Bugcrowd of and segmentation changes to controls/methods and the requirement to perform a penetration test to prove the change did not have a negative security impact • Customers using Next Gen Pen Test must purchase the Professional or Enterprise tier as the Essential tier does not include internal segmentation testing Note: For Classic Pen Test a separate penetration test will be required for the semi-annual segmentation test. For customers choosing timebound Next Gen Pen Test, a separate penetration test may be required depending on the time period for the pen test.

schellman | bugcrowd

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility			Assessor Findings
	Customer	Classic Pen Test	Next Gen Pen Test (including Timebound)	
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 Head of Operations at Bugcrowd and noted that researchers selected for Classic and Next Gen Pen Test engagements 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 retesting thus indicating organizational independence. Customers are responsible for ensuring the organizational independence of individuals 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	Classic Pen Test	Next Gen Pen Test (including Timebound)	
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 Classic and Next Gen Pen Test solutions have 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 to ensure all controls/methods are tested • Customers using Next Gen Pen Test must purchase the Professional or Enterprise tier as the Essential tier does not include internal segmentation testing

schellman | bugcrowd

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility			Assessor Findings
	Customer	Classic Pen Test	Next Gen Pen Test (including Timebound)	
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 Head of Security at Bugcrowd and noted that researchers selected for Classic and Next Gen Pen Tests 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 retesting thus indicating organizational independence. Customers are responsible for ensuring the organizational independence of individuals that review the segmentation test findings to determine if segmentation controls implemented by the customer are operational and effective.
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 methodologies for Classic and Next Gen Pen Test solutions used by Bugcrowd and example reports for each and noted that testing performed by Bugcrowd supports this control.

SECTION 3: COMPLIANCE REQUIREMENT COVERAGE

Compliance Requirements	Responsibility			Assessor Findings
	Customer	Classic Pen Test	Next Gen Pen Test (including Timebound)	
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 methodologies for the Classic and Next Gen Pen Tests and example reports for each and noted that identification of vulnerabilities during Classic and Next Gen Pen Test engagements 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 Classic and Next Gen Pen Test engagements. Customers were solely responsible for the remediation of any vulnerabilities and then requesting retesting to prove the remediation is in place.
Cybersecurity Maturity Model Certification CA.4.164. Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts.	✓	✓	✓	Schellman reviewed the methodologies for Classic and Next Gen Pen Test used by Bugcrowd and example reports for each and noted that testing and resource selection performed by Bugcrowd supports this control.

schellman

www.schellman.com