# VULNERABILITY SCANNING STANDARD

**Version 1.0**

**10/15/2024**

**Issued by: Eric Somogyi**

# Table of Contents

# 1.0 PURPOSE



1.1 This document has been developed to provide guidance on a vulnerability scanning policy in support of achieving and maintaining a security authorization that meets the PCI Data Security Standard.

1.2 Nessus Expert is a widely used industry standard vulnerability scanner that helps companies identify and fix security vulnerabilities in IT systems. Nessus automatically checks for a wide range of vulnerabilities, including software flaws, missing patches, malware, and misconfigurations across various devices, OS, and applications. Nessus provides comprehensive coverage, constantly updated weekly with the latest vulnerability information. Also, Nessus has a feature called Live results where Nessus performs intelligent vulnerability assessment in offline mode without having to run a scan. Lastly, it has pre-built templates and customizable reports to simplify vulnerability assessment and remediation.

1.3 In an effort to increase the effectiveness of the security of (Enter Company Here)'s network, we will implement the use of Nessus Expert to scan all internal systems and external systems connected to the cardholder data environment (CDE) for software vulnerabilities, malware, and misconfigurations with our own customization configuration. We will use the results of the daily scans to protect all systems against malware and regularly update anti-virus software and EDR programs. We will continuously monitor our network using the Live Results feature and configure Nessus to generate automated alerts to our management and employees to ensure a timely response. We will take the customized reports tailored to PCI-DSS and document them in our company logs and have these reports on hand as our official mechanism to verify compliance with other merchants and entities.

# 2.0 SCOPE

2.1 We will implement our vulnerability scanning standard by implementing the Tenable Security Center Architecture within our internal secure network. Since we have an unlimited budget, we will lease per hour an Amazon EC2 instance and we will have Tenable.sc running 24/7. This will manage and evaluate all vulnerability data across our enterprise. This will help speed up our response and remediation to reduce our overall risk and streamline compliance. On our Security Manager's authenticated devices in our Security Operations Center, we will be running 2 licenses of Nessus Manager and Nessus Expert through two firewalls which then connect to our Amazon EC2 instance. The tenable.sc will be streamlining compliance with our PCI DSS requirements and regulatory mandates and that will be able to be viewed through the Tenable.sc Continuous View monitoring platform in our company headquarters. This will ensure that all systems are constantly being monitored, logged, and through the ability of the Nessus Expert software, it will update our systems daily when vulnerabilities are found in any of the systems below or at least alert our cybersecurity team.

2.2 The systems below will be developed with configuration standards for all system components. All systems and processes below will be tested regularly and monitored daily. The types of systems that will be scanned are all based on the categories of the assets that are scanned. See the following:

- Cloud Assets in AWS, GCP, Azure, SFDC, and Zoom environments.
- Databases including: MySQL, Azure SQL, SQL Server, Oracle, Microsoft SQL, MongoDB, IBM DB2, PostgreSQL.
- Unsupported OS, 3rd Party Software, SSL/TLS Certificates.
- OS including Debian/Kali Linux, Fedora, FreeBSD, Mac OS, Red Hat, CentOS, Oracle Linux, SUSE Linux, Ubuntu, Windows Server 2008/2012/2016/2022
- Security Frameworks and APIs
- All company software and web applications and payment processing devices.
- "System components including: all network devices including routers, switches, firewalls, hotspots, wireless access points/extenders, IoT devices.
- Windows/Linux physical and VMs.
- Workstations that will be scanned are all company employee desktops, laptops, and employee-owned laptops (if applicable).

# 3.0 CATEGORIZATION

3.1 Vulnerabilities will be categorized based on the National Vulnerability Database Common Vulnerability Scoring System ("CVSS") metrics: Low, Medium, High, or Critical. These alerts will be configurated in our Nessus settings that meet the requirements. All vulnerabilities in the "report" page of Nessus Expert will have in the results the CVSS scoring system. When vulnerability is flagged in our scan results, anything with a CVSS score of 4.0 medium or above will be triggered to send an alert to our cybersecurity team that is currently on the clock.

3.2 After identifying these vulnerabilities with our Nessus system, our cybersecurity team will contact the Security Manager and discuss the potential impact of how that vulnerability could be exploited and how it could negatively affect our enterprises' confidentiality, integrity, and availability of our systems' environment.

3.3 This standard is only categorizing compliance requirements with PCI DSS. If a client's sensitive cardholder data is compromised, we will have our public outreach team contact the cardholder to notify them of the breach.

# 4.0 RULES TO FIX VULNERABILITIES



4.1 We use compensating controls when we cannot meet the requirement of PCI DSS to mitigate risk associated with being PCI DSS compliant. These controls have been approved by our PCI qualified assessor (QA). Before beginning to fix the vulnerability, the security team will investigate and refer to our **Incident Response Plan**. If after investigation, any kind of breach occurred, this vulnerability detected will be escalated to a breach and the steps taken by the security team will be following the incident response plan. This will be documented with our **Report on Compliance** per the PCI DSS requirements.

4.2 System administrators will update system configuration standards in the Nessus Expert system as new vulnerability issues are identified.

4.3 For vulnerabilities that are identified and fixed, the security team will maintain an inventory of those system components before and after the fix/update.

4.4 The security employees will confirm and recheck that all anti-virus software did not come out with an update right before the vulnerability was detected on all systems.

4.5 Strong Access control measures such as two-factor authorization from anyone outside the network will be used for vulnerability maintenance. This will be communicated in our **Authentication Policy** to all users.

4.6 The Nessus Administrators on our security team will use the remediation tool in the scanning software to keep track of our remediation goals for fixing vulnerabilities from our scan reports.

4.7 Vulnerability with risk rankings of the following have the following timelines for correction:

- Low: Patched or mitigated within 60 days.
- Medium: Patched or mitigated within 30 days.
- High: Patched or mitigated within 7 days.
- Critical: Patched or mitigated immediately within 24 hours.
- *These timeless can be adjusted based on specific circumstances, such as the availability of patches, the complexity of the remediation, and potential impact of the vulnerability.

4.8 The employee on the security team will review the vulnerabilities reported and then report to the Security Manager within 24 hours of being notified of new vulnerabilities once a scan is completed. Following, the security team employee responsible must notify the security management team of any un-remediated vulnerabilities not addressed within the timeframes from 4.7 as described in this standard so that the risk is accepted by the Security Management team.

# 5.0 EXCEPTIONS AND APPROVALS



5.1 We use compensating controls when we cannot meet the requirement of PCI DSS to mitigate risk associated with being PCI DSS compliant. These controls have been approved by our PCI qualified assessor (QA). Before beginning to fix the vulnerability, the security team will investigate and refer to our **Incident Response Plan**. If after investigation, any kind of breach occurs, this vulnerability status will be logged and documented to the entire security team and then the following actions in 5.2 and 5.3 will be taken for either an exception or an approval.

5.2 Exceptions and Approval Process:

5.2.1 - If our security team confirms through investigation that the vulnerability reported from the Nessus Expert scanner is relating to a 3rd party, any vulnerability relating to that entity where it is out of our company control will first go through a Risk Assessment to address the potential impact on our company and our client's cardholder data.

5.2.2 - After completing the assessment on that vulnerability, if it meets the requirements to possibly be an exception, then our security team will have an exception for not needing to correct the vulnerability according to the time frame in 4.7.

5.2.3 – The employee who's tasked with this must report to the security team the event and the security team will review that specific vulnerability event and confirm with the team that it is an exception. Examples of 3rd parties include but not limited to:

ISP's, VISA, Mastercard, Discover, any cardholder processing entity not mentioned, Amazon, Microsoft, Oracle, any Linux platform, Zoom, any telecommunications provider, any web/application developer not mentioned, or any hardware manufacturer/vendor not mentioned.

5.2.4 - Any vulnerabilities relating to customer cardholder data that is at medium or higher risk of being exposed in any way is always denied an exception except in the case that the vulnerability can be fixed. Any vulnerability relating to Amazon Web Services location where our Tenable.sc instance is hosted will be assessed in a case-by-case specific procedure. The only rule to this procedure is the Security Manager shall contact the business representative at AWS immediately or as soon as possible when a vulnerability event relating to the uptime of our Tenable.sc instance occurs.