Tenable Cyber Exposure Study - PCI DSS v4.0

Last Revised: July 17, 2025

Copyright © 2025 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

PCI DSS v4.0 Overview	4
How Tenable Helps	
Control Objective 1: Build and Maintain a Secure Network and Systems	
PCI Requirements Under This Objective Supported by Tenable	
Cloud Environments	15
Control Objective 2: Protect Account Data	
PCI Requirements Under This Objective Supported by Tenable	17
Compliance Audit Files	
Secure Sockets Layer	19
Web Application Scanning	
Control Objective 3: Maintain a Vulnerability Management Program	
PCI Requirements Under This Objective Supported by Tenable	23
Web Application Scanning	23
Tenable Security Center	24
Tenable Vulnerability Management	
Antivirus	27
Control Objective 4: Implement Strong Access Control Measures	
PCI Requirements Under This Objective Supported by Tenable	
Control Objective 5: Regularly Monitor and Test Networks	
PCI Requirements Under This Objective Supported by Tenable	
Tenable Web App Scanning	
Control Objective 6: Maintain an Information Security Policy	
PCI Requirements Under This Objective Supported by Tenable	

- Ø

References	

— Ø –

PCI DSS v4.0 Overview

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all organizations that accept, process, store, or transmit credit card information maintains a secure environment. The PCI DSS standard was developed by the PCI DSS Council. The council is made up of credit card companies such as Visa, MasterCard, American Express, Discover, and JCB. PCI DSS version 3.2.1 was officially retired on March 31, 2024 and version 4.0 became the industry standard moving forward. On March 31, 2025 all version 4.0 requirements will become mandatory.

Note: On June 11, 2024 PCI DSS v4.0.1 was released. This latest release is a "limited revision of PCI DSS v4.0" which includes corrections for typographical and other minor errors. There are no new requirements, and no requirements have been added or removed. Additional information on the summary of changes can be found in the References section at the end of this document.

PCI-DSS has 12 main requirements and more than 300 sub-requirements. These 12 requirements are technical and operational. The requirements are organized into six control objectives, and cover areas such as network security, password management, data protection, and access control.

PCI DSS v4.0.x has the following six control objectives:

- 1. Build and Maintain a Secure Network and Systems
- 2. Protect Account Data
- 3. Maintain a Vulnerability Management Program
- 4. Implement Strong Access Control Measures
- 5. Regularly Monitor and Test Networks
- 6. Maintain an Information Security Policy

Compliance with PCI DSS is required for any organization that stores, processes, or transmits cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). This requirement includes all entities involved in payment processing – merchants, processors, acquirers, issuers, and other service providers. Cardholder data and sensitive authentication data are defined as:

Sensitive

	Authentication Data
Primary Account Number (PAN)	Full track data (magnetic stripe data or chip equivalent on a chip)
Cardholder Name	Card verification code
Expiration Date	PINs/PIN blocks
Service Code	

Depending on the number of transactions an organization processes annually and the specific payment brand involved, there are four different levels of compliance validation requirements, commonly known as classifications:

- PCI Level 1 Businesses processing over 6 million transactions annually
- PCI Level 2 Businesses processing 1 to 6 million transactions annually
- PCI Level 3 Businesses processing 20,000 to 1 million transactions annually
- PCI Level 4 Businesses processing less than 20,000 transactions annually

Currently, PCI Level 1 requires an annual report be conducted by a Qualified Security Assessor (QSA), or an Internal Security Assessor (ISA). A QSA will typically visit the organization to conduct an audit, while the ISA can be a member of the organization, who is properly trained to conduct an assessment, and act as a liaison to external auditors. PCI Level 1 is the strictest of all classifications. Any organization, regardless of classification, is subject to an external audit, even if the organization is not a PCI Level 1 merchant.

In addition, all PCI Level merchants also require the following:

• Vulnerability Scanning to be completed Quarterly. Tenable's PCI ASV (Approved Scanning Vendor) streamlines the quarterly external vulnerability scan submission and dispute process as required by PCI 11.3.2. With pre-configured scan templates and an efficient evidence/dispute resolution process, Tenable can quickly prepare an Attestation of Scan Compliance (AOSC) for merchants and service providers.

- Annual or Semi-annual Penetration Test, as required by PCI 11.4.3, depending on the organizational PCI requirements (Note: Not required for PCI Level 3 or PCI Level 4 Merchants, however these organizations would benefit from conducting a penetration test, as least annually)
- Completion of a Self-Assessment Questionnaire (SAQ). Note: There are different types of SAQ depending on the scope of the audit. See PCI DSS documentation for more information.
- Completion of an Attestation of Compliance (AOC). This form states you have complied with the required standards to satisfy PCI DSS requirements.
- PCI Requirement 11.3.1 makes vulnerability scanning mandatory at least once every three months, and recommends more frequent scanning depending on network complexity.

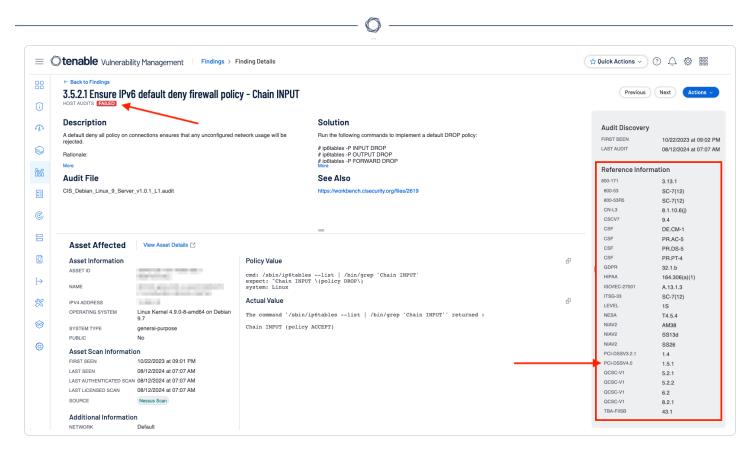
Organizations can best determine their level of PCI compliance by coordinating with their service provider.

Failure to comply with PCI DSS can result in fines imposed by credit card companies, restriction or limitations on processing payments, and reputational damage arising from security breaches. Therefore organizations handling credit card information are strongly encouraged to adhere to PCI DSS standards to protect cardholder data and maintain trust with their customers.

How Tenable Helps

The Tenable solution starts with a foundation of <u>Tenable Security Center</u> or <u>Tenable Vulnerability</u> <u>Management</u>, for compliance and vulnerability scanning, which include internal and external scanning templates to meet the mandatory PCI scanning requirements of PCI DSS Requirement 11.3.1. Both solutions provide the ability to gather security data from across your organization using sources such as active and passive monitoring. Next building upon the foundation by adding <u>Tenable PCI ASV</u>, to meet the external vulnerability scanning requirements. Tenable (an Approved Scanning Vendor) can quickly prepare a compliant scan report for merchants and service providers with PCI ASV, streamlining the quarterly external vulnerability scan submission and dispute process as required by PCI DSS. Finally, <u>Tenable Web App Scanning</u>, as a dedicated PCI web app scan, to be combined with Tenable PCI ASV, as needs require the identification of vulnerabilities for public facing applications.

As part of the Vulnerability Management solution, Tenable provides audit files which contain cross references to a wide range of benchmarks, standards, and frameworks. In the following example, a Center for Internet Security (CIS) audit file is utilized in a scan against a Debian server running software version 9.7. Reviewing a single response for policy check CIS 3.5.2.1 - Ensure IPv6 default deny firewall policy, 25 other cross references are mapped, including PCI-DSSv4.0 Requirement 1.5.1. This CIS audit check applies to all the listed cross references, including PCI-DSS 1.5.1. The significance of this specific audit check is if IPv6 is enabled on a system, IP tables should be configured. A default deny-all policy on all connections ensures that any unconfigured network usage will be rejected. If not configured properly, and failure of the check is recorded, as shown here:



This embedded cross reference data is utilized to present and report compliance information within Tenable Vulnerability Management and Tenable Security Center using a variety of dashboards and reports highlighted in this guide.

For more information related to cross references, review the Cyber Exposure Study: <u>Host Audit</u> <u>Data</u>

Note: This document only presents solutions for portions of PCI DSS version 4 that can be measured and validated using automated processes. There are many policy specific items with the PCI DSS rules and guidelines that require organizations to manually create, develop, or review documented procedures, interview personnel, validate training, or examine procedures. These items can not be tested and therefore will not be referenced in this document.

Control Objective 1: Build and Maintain a Secure Network and Systems

This objective includes installing and maintaining firewalls, and firewall configurations to protect cardholder data, and not using vendor supplied credentials (default credentials) for system passwords or security parameters. This control objective covers the following PCI DSS requirements:

Requirement 1: Install and maintain network security controls

Requirement 2: Apply secure configurations to all system components

The PCI Security Standards Council defines network security controls (NSCs) as firewalls and other network security technologies, which typically control network traffic between two or more logical or physical network segments (or subnets) based on predefined policies or rules. Traditionally, this function has been provided by firewalls, but may be provided by virtual devices, cloud access controls, virtualization/container systems, and other software-defined networking technologies.

PCI Requirements Under This Objective Supported by Tenable

Requirement 1: Install and maintain network security controls

Firewalls, routers, and cloud virtual networks are configured with access control lists to control network traffic flowing inbound and outbound from the CDE. Ensure only acceptable ports, and protocols are being used. Configuration standards may outline what is acceptable and permitted on the network.

Examine configuration settings for all NSCs and verify that only approved services, protocols, and ports are in use. Compromises often occur due to insecure services such as telnet and FTP. Unsecure or unmanaged ports, services, and protocols can not only give attackers a point of entry, but they are additionally often overlooked and unpatched. By identifying all ports, protocols, and services, entities can ensure that unnecessary ports, protocols, and services that do not have a defined business need are disabled or removed.

Any network configuration setting changes are identified. Changes should not introduce misconfigurations, insecure services, or unauthorized network connections. Changes include the addition, removal, or modification of any connection, and include changes to the component and the components security functionality.

Security controls are implemented on any computing device, including company and employee owned devices, (desktops, laptops, tablets, smart phones, and any other mobile computing device) that connects to both untrusted networks (including the internet) and the CDE. Ensure that security controls are implemented and running, (firewall software or other endpoint protection solutions). Split Tunneling is a VPN technology that supports VPN clients to send only specific traffic over the VPN, while the rest travels over the local network to the internet. This setting is often used with remote workers or associated with remote sites. Split Tunneling is very dangerous, as the malicious users are given the ability to maneuver over the VPN tunnel and grain access to protected resources. Because of the risk exposed when split tunneling, the PCI requirement suggests strictly prohibiting the use of split tunneling of all employee-owned, corporate-owned, and mobile devices.

Tenable has published several audit files that have checks for split-tunneling in Juniper and Cisco devices:

- DISA_Juniper_SRX_Services_Gateway_VPN_v2r2_STIG.audit
- DISA_STIG_Cisco_IOS_XE_Router_RTR_v2r9.audit
- DISA_Juniper_EX_Series_Switches_Router_v1r3_STIG.audi
- DISA_STIG_Cisco_IOS_XE_Switch_RTR_v2r5.audit
- DISA_STIG_Cisco_IOS-XR_Router_RTR_v2r4.audit

Requirement 2: Apply secure configurations to all system components

Default passwords are well known allowing bad actors (both external and internal) often use default passwords and other default vendor settings to compromise systems. Changing default passwords, removing unnecessary software, accounts, and services, reduces the attack surface.

Many operating systems and applications have known weaknesses by default. System configuration standards should be analyzed, and verified as being updated as new vulnerabilities are identified and immediately after a system is connected to a production environment. Keeping up to date with current industry standards will help maintain secure configurations. Numerous security organizations such as Center for Internet Security (CIS), International Organization for Standardization (ISO), and the National Institute of Standards and Technology (NIST), have established standards, recommendations, and system hardening guidelines.

Organizations should ensure that only necessary services, protocols, daemons, and functions are enabled on systems. Unnecessary functionality may include scripts, drivers, features, subsystems, file systems, interfaces (both USB and Bluetooth), as well as unnecessary web servers. Encrypted communications should be used, and all clear text protocols should be avoided (HTTP, Telnet, etc). Certificates should be trusted, using strong encryption methods, and should not fall back to weaker insecure protocols or methods. Wireless Access Points, if used, should not have default encryption keys, SNMP defaults, or vendor defaults.

For Tenable Vulnerability Management the Build and Maintain a Secure Network and Systems widget provides details on each of the compliance controls for the compliance family group being referenced.

	FAILED	WARNING	PASSED
1.5.1	22	10	4
2.2.4	10	7	11
2.2.7	8	0	0
1.3.2	6	0	6
1.4.1	2	2	2
1.2.1	2	2	2

This widget focuses on the category Build and Maintain a Secure Network and Systems, which covers topics within PCI requirement 1 and 2. Both of these requirements cover installing and maintaining a firewall configuration to protect cardholder data, and the use of vendor supplied default credentials. This widget provides the count of audit checks according to the checks result.

The compliance control reference number is followed by a count, and compliance result for the compliance control displaying a count of passed, failed, and warning.

Compliance results are a product of Tenable Compliance audit files. Audit files contain tests for file permissions, configurations and access control. Audit files compare an organization's configuration to a secure standard, such as those available by the Center for Internet Security (CIS). A wide variety of audit files can be <u>downloaded here</u>.

Clicking on the cell within the matrix, allows the user to drill down into the compliance data, opening the findings page and displaying the results (1). In this instance drilling down into the failed items under Requirement 1.5.1, the analysis is presented with the 22 failed compliance concerns. Selecting the first item opens a details pane (2), for that particular finding. The detail pane includes an overview as well as the actual audit output.

Findings 🗅			1					
Vulnerabilities	Cloud Misconfigurations Host Audi	ts Web Application Fir	dings					
> 7 Advance		mework is equal to PCI-DS84 ND Compliance Control is equ	. ,	equal to "B	uild and Maintain a Secure Network and Syst	ems" AND Last Audited	within last 90 days) AND Result is	× ,
= 1 Host Au	udit selected Select all 22 host audit	Add Recast Rule [→ Export	I More		Fetched At: 03:51 PM	Grid Basic View ~ Coli	umns 🗸 1 to 22 of 22 🗸 🔣 🤇	Page 1 of 1 🔿
Audit Na	ame	Audit File	Re	sult	Asset Name	State	Asset Tags	Actio
3.5.2.1	Ensure IPv6 default deny firewall policy - Chain	CIS_Debian_Linux_9	_Server_v1.0.1_L1.audit 🖉	Failed	demoio-gcp-prod-us-east4-debis-19-1.c	Active	Cody: SatTest	1
3.3.1 Er	sure TCP Wrappers is installed	CIS_Debian_Linux_9	_Server_v1.0.1_L1.audit ⊘	Failed	demoio-gcp-prod-us-eastr-debian9-1.c	Active	Cody: SatTest	1
3.5.2.1	Ensure IPv6 default deny firewall policy - Chain	CIS_Debian_Linux_9	_Server_v1.0.1_L1.audit	Failed	demoio-gcp-prod-us-east4-debian9-2.c	Active	Cody: SatTest	1
3.5.1.1	Ensure default deny firewall policy - Chain INPU	T CIS_Debian_Linux_9	_Server_v1.0.1_L1.audit	Failed	demoio-gcp.prod-us-east4-debian9-2.c	Active	Cody: SatTest	1
3 5 2 1 Epour	ID: C defeult de su fireurell se li							
	e IPv6 default deny firewall poli		n					See All Deta
Asset Informatio	on .	Host Audit Informatio		Overv	iew Audit Output			See All Deta
	n		3.5.2.1 Ensure IPv6 default deny firewall policy - Chain OUTPUT		iew Audit Output			See All Deta
Asset Informatio	n	Host Audit Informatio	3.5.2.1 Ensure IPv6 default deny firewall policy - Chain	Desc A defa	ription ult deny all policy on connections ensures the	at any unconfigured netw	vork usage will be rejected.	See All Deta
Asset Informatic NAME IPV4 ADDRESS	n Linux Kernel 4.9.0-8-amd64 on Debian	Host Audit Informatio	3.5.2.1 Ensure IPv6 default deny firewall policy - Chain OUTPUT CIS_Debian_Linux_9_Server_v	Desc A defa Ratior	ription ult deny all policy on connections ensures that rate:	, ,		
Asset Informatic NAME IPV4 ADDRESS OPERATING SYSTEM SYSTEM TYPE NETWORK	Dn Linux Kernel 4.9.0-8-amd64 on Debian 9.7	Host Audit Informatio	3.5.2.1 Ensure IPv6 default deny firewall policy - Chain OUTPUT CIS_Debian_Linux_9_Server_v 1.0.1_L1.audit	Desc A defa Ratior With a usage	ription ult deny all policy on connections ensures the	, ,		
Asset Informatic NAME IPV4 ADDRESS OPERATING SYSTEM SYSTEM TYPE	Linux Kernel 4.9.0-8-amd64 on Debian 9.7 general-purpose	Host Audit Information AUDIT NAME AUDIT FILE BENCHMARK BENCHMARK	3.5.2.1 Ensure IPv6 default deny firewall policy - Chain OUTPUT CIS_Debian_Linux_9_Server_v 1.0.1_L1.audit CIS Debian 9 v1.0.1	Desc A defa Ratior With a	ription ult deny all policy on connections ensures the vale: . default accept policy the firewall will accept a	, ,		
Asset Informatic NAME IPV4 ADDRESS OPERATING SYSTEM SYSTEM TYPE NETWORK DNS (FQDN)	n Linux Kernel 4.9.0-8-amd64 on Debian 9.7 general-purpose Default	Host Audit Informatic AUDIT NAME AUDIT FILE BENCHMARK BENCHMARK SPECIFICATION NAME BENCHMARK VERSION PLUGIN NAME	3.5.2.1 Ensure IPv6 default deny frewall policy - Chain OUTPUT CIS_Debian_Linux_9_Server_v 1.0.1_L1.audit CIS Debian 9 v1.0.1 CIS Debian 9 1.0.1 Unix Compliance Checks	Desc A defa Ratior With a usage Less	ription ult deny all policy on connections ensures the ale: default accept policy the firewall will accept a than to black list unacceptable usage.	, ,		
Asset Informatic NAME IPV4 ADDRESS OPERATING SYSTEM SYSTEM TYPE NETWORK DNS (FQDN) Asset Scan Infor	n Linux Kernel 4.9.0-8-amd64 on Debian 9.7 general-purpose Default mation	Host Audit Informatic AUDIT NAME AUDIT FILE BENCHMARK BENCHMARK SPECIFICATION NAME BENCHMARK VERSION PLUGIN NAME RESULT	3.5.2.1 Ensure IPv6 default deny frewall policy - Chain OUTPUT CIS_Debian_Linux_9_Server_v 1.0.1_L1.audit CIS Debian 9 v1.0.1 CIS Debian 9 1.0.1 Unix Compliance Checks ⊘ Failed	Desc A defa Ratior With a usage Less Solut	ription ult deny all policy on connections ensures the ale: default accept policy the firewall will accept a than to black list unacceptable usage.	any packet that is not con		
Asset Information NAME IPV4 ADDRESS OPERATING SYSTEM SYSTEM TYPE NETWORK DNS (FQDN) Asset Scan Infor FIRST SEEN	n Linux Kernel 4.9.0-8-amd64 on Debian 9.7 general-purpose Default mation 10/22/2023 at 09.01 PM	Host Audit Informatic AUDIT NAME AUDIT FILE BENCHMARK BENCHMARK SPECIFICATION NAME BENCHMARK VERSION PLUGIN NAME	3.5.2.1 Ensure IPv6 default deny frewall policy - Chain OUTPUT CIS_Debian_Linux_9_Server_v 1.0.1_L1.audit CIS Debian 9 v1.0.1 CIS Debian 9 1.0.1 Unix Compliance Checks	Desc A defa Ratior With a usage Less Solut	ription ult deny all policy on connections ensures the ale: default accept policy the firewall will accept a than to black list unacceptable usage.	any packet that is not con		
Asset Information NAME IPVA ADDRESS OPERATING SYSTEM SYSTEM TYPE NETWORK DNS (PGDN) Asset Scan Infor FIRST SEEN LAST SEEN	Linux Kernel 4.9.0-8-amd64 on Debian 9.7 general-purpose Default mation 10/22/2023 at 09:01 PM 08/12/2024 at 07:07 AM	Host Audit Informatic AUDIT NAME AUDIT FILE BENCHMARK BENCHMARK SPECIFICATION NAME BENCHMARV CERSION PLUGIN NAME RESULT STATE	3.5.2.1 Ensure IPv6 default deny frewall policy - Chain OUTPUT CIS_Debian_Linux_9_Server_v 1.0.1_L1.audit CIS Debian 9 v1.0.1 CIS Debian 9 1.0.1 Unix Compliance Checks ⊘ Failed	Desc A defa Ratior With a usage Less Solut Run th # ip6tt	ription uit deny all policy on connections ensures the ale: default accept policy the firewall will accept a than to black list unacceptable usage. ion te following commands to implement a defaul ables -P INPUT DROP	any packet that is not con		
Asset Information NAME IPVA ADDRESS OPERATING SYSTEM SYSTEM TYPE NETWORK DNS (PGDN) Asset Scan Infor FIRST SEEN LAST SEEN	n Linux Kernel 4.9.0-8-amd64 on Debian 9.7 general-purpose Default Default 10/22/2023 at 09:01 PM 08/12/2024 at 07:07 AM	Host Audit Informatic AUDIT NAME AUDIT FILE BENCHMARK BENCHMARK SPECIFICATION NAME BENCHMARK VERSION PLUGIN NAME RESULT	3.5.2.1 Ensure IPv6 default deny frewall policy - Chain OUTPUT CIS_Debian_Linux_9_Server_v 1.0.1_L1.audit CIS Debian 9 v1.0.1 CIS Debian 9 1.0.1 Unix Compliance Checks ⊘ Failed	Desc A defa Ration With a usage Less Solut Run th # ip6tt # ip6tt	ription uit deny all policy on connections ensures the ale: default accept policy the firewall will accept a than to black list unacceptable usage.	any packet that is not con		

The specific PCI-DSSv4 requirements referenced in this widget are: 1.4.3 | 2.2.2 | 1.5.1 | 1.2.1 | 1.3.1 | 2.2.3 | 1.4.2 | 1.4.5 | 2.2.4 | 1.4.1 | 1.3.2 | 1.1.2 | 2.2.7.

Dashboards such as the Compliance Benchmarks by Category dashboards, available for:

- Microsoft Security Compliance Toolkit (MSCT)
- <u>Tenable Best Practices (TNS)</u>
- Defense Information Systems Agency (DISA)
- Center for Internet Security (CIS)

mputer (1)		chmarks by Category (Explore) (All ~) (Jume DISA Compliance Benchmarks By Plugin Category (Explore)					All ∨ Jump to Deshboard ∨ EB Deshboards (E1 Share) + Export ∨ + Hore ∨						
puter 🐨	Computer (1)	TNS Compliance Benc	hmarks By Plugin Catego	ry (Explore)				Jump to D	lashboard -	irds 🔁 Share	Export •	More ~	
05 Deltare 9 v1.0.1		Computer ①	\equiv \bigcirc tenable v.	Inerability Managem	nent Dashboa	ards > Selected Dasht	oard					🕸 Quick Actions 🗸) 0 🖉 🏾 1
Editor Company Editor vi La			MSCT Compliance	Benchmarks By	Plugin Catego	ory (Explore)			All	Jump to Dashb	oard 👻 🔠 Dashba	oards 📑 Share	(> Export ~
10 obuerou 12.04 (75 57.1.2			Computer (1)					: N	etwork ①				
				PASSED		FAILED	WARNING			FAILED		WARNING	PASSED
		the fit has been been by	—				WARNING		MILT Metaorik Berchmark	221		0	0
ication 🕕		The second second second	and the second design	744		6	1		MC ¹ Second Rectoration	87		57	0 49
		the first tip have direct a	and tangent factor	374		2	1		MCT Instanti Benchmark I	64		78	49
		the lot but he have been	-						MCT Issuer's Benchmark I	75		0	0
	Application (1)		MET Company March	51		339	0		MUT tenent Benchmark I	47		0	70
			AND COMPANY REAL PROPERTY.	335		2	1		MUT Senart Benchmark	69		50	0
CO. Dellage Text 2.1									MUT Interest Rescharges 1	46		0	65
	-	Application ()		5		318	1		MCT Network Benchmark 1	0		42	64
And a state of the			MALL COMPANY REAL PROPERTY	48		311	0		MSC ¹ National Banchmark 1 MSC ¹ National Banchmark 1	58		0	0
			WAR									0	
		.00.02 (2015)	Application ①					: 0	loud (1)				
			0	WARNING	ERROR	PASSED	FAILED			WARNING	ERROR	PASSED	FAILED
		11111111111	1007 (0410) (041)	91	25	9	1		MICT Could Benchmark 1	91	25	9	1
				62	0	3	33		WSC? Cloud Newtywork 3	62	0	3	33

These dashboards for Tenable Vulnerability Management focus on best practice checks for the following four categories, Computer, Network, Application, and Cloud. This information allows organizations to review information related to secure systems configuration and systems hardening related to a specific set of compliance standards. Similarly, the <u>CIS Audit Summary Dashboard</u> for Tenable Security Center provides compliance results for numerous devices.



Cloud Environments

Cloud services are an integral part of business operations, offering scalability, flexibility, and accessibility. Cloud environments store vast amounts of sensitive data, including personal information, financial records, intellectual property, and proprietary business data. Ensuring robust security measures protects this information from unauthorized access, breaches, or theft.

Protecting cloud environments is vital for protecting data, ensuring compliance with regulatory requirements, maintaining operational continuity, managing risks, and optimizing business efficiency. Tenable Cloud Security provides out-of-the-box, continuously updated support for all major compliance frameworks, and best practices. Tenable Cloud Security provides the ability to create customized frameworks to meet the exact needs of your organization. Using customized reports, communicate with stakeholders on internal compliance, external audit and daily security activities.

Compliance reporting is available by navigating to the Compliance tab. On the Compliance dashboard, analysts have the option to select the appropriate compliance benchmark from the list. By default, this dashboard reports compliance details for all Benchmarks combined if no option is selected.

Cloud Secu	urity Q Search users, roles & resources		All accounts 🗸	
=	Compliance Organization ~			
Dashboard	Name	Status S	ummary	Ć
Dinventory				
I Findings	O Tenable Best Practices - Secure your environment with policies that were hand-picked by Tenable. This standard includes policies used by a large number of customers, and is based on Tenable's extensive experience solving cloud security issues.		- 64%	<u>1</u>
Activity Log	Key Key Key Key Key Key Key Key Key		67%	1
iam 🗟	in the cloud	-		_
Workload	CIS AKS 1.2.0 - Prescriptive guidance for running Azure Kubernetes Service following recommended security controls		67%	<u>1</u>
₭ubernetes	> (R CIS AWS 2.0.0 - An objective, consensus-driven security guideline for the Amazon Web Services cloud provider		46%	<u>1</u>
Policies	> 🙃 CIS Azure 2.0.0 - An objective, consensus-driven security guideline for the Microsoft Azure cloud provider			<u>1</u>
Compliance	CISEKS 1.2.0 - Prescriptive guidance for running Elastic Kubernetes Service following recommended security controls		67%	<u>1</u>
Accounts	> (iii CIS GCP 1.3.0 - An objective, consensus-driven security guideline for the Google Cloud Platform		50%	<u>1</u>
R Audit	> (as CIS GCP 2.0.0 - An objective, consensus-driven security guideline for the Google Cloud Platform		50%	<u>1</u>

To view details, analysts can drill down into any of the findings. In this example, drilling down into the **CIS AWS 2.0.0** item provides details on the root account.

			Ø					
			9					
Ctenable Cloud Sect	urity		Q Search users, roles & resource	ces			All acco	ounts ~ JC
=	Compliand	ce Organization ~						
C Dashboard	Name					Status	Summary	Ø
Inventory								
Findings	> O		ur environment with policies that were hand-picked by Tenable. This standa omers, and is based on Tenable's extensive experience solving cloud securit			•		<mark>■ 64% <u>↓</u></mark>
Activity Log	0	AWS Well Architected - Key concer	ots, design principles, and architectural best practices for designing and run	ning workloads		_		
👼 IAM	> <mark>%</mark>	in the cloud						67% <u>1</u>
C Workload	> @	CIS AKS 1.2.0 - Prescriptive guidance	for running Kzure Kubernetes Service following recommended security con	trois		-		67% <u>1</u>
	~ (CS	CIS AWS 2.0.0 - An objective, conserved	sus-driven security guideline for the Amazon Web Services cloud provider	Ļ		-		• 46% <u>1</u>
Policies		✓ 1. Identity and Access Management	ıt					- 43%
Compliance		1.4 Ensure no root user accour	nt access key exists					
In Reports		 The root user account is the me 	ost privileged user in an AWS account. AWS Access Keys provide programma ed that all access keys associated with the root user account be removed.	atic access to a given				100%
ය. Accounts		Platform	Policy	Failed Resources	Scanned Resources		Summary	
🖸 Audit		aws	Root user has access key	0 root users	2 root users		-	100%
		 1.5 Ensure MFA is enabled for 1 The root user account is the maprotection on top of a usernam 	ost privileged user in an AWS account. Multi-factor Authentication (MFA) add	is an extra layer of				
			er for administrative and daily tasks access to and control over all resources in the AWS account. It is highly reco vveryday tasks.	mmended that the use				100%

Control Objective 2: Protect Account Data

This includes protecting stored cardholder data, encrypting transmission of cardholder data across networks, and ensuring encryption keys are stored properly. This control objectives covers the following PCI DSS requirements:

Requirement 3: and passively detected assets

Requirement 4: Asset discovery statistics

Note: Notes related to Requirement 3. This requirement is related to the controls around account data that is printed or stored in any form. Account data is both cardholder data and sensitive authentication data. While this requirement is not supported by Tenable directly, the recommended practice here is to keep storage of account data to a minimum. Do not store sensitive authentication data (SAD) after authorization. Restrict the display of the full primary account number (PAN) and cardholder data. And secure the PAN, account data, and any cryptographic keys used to protect the data when they are stored.

PCI Requirements Under This Objective Supported by Tenable

Requirement 4: Protect cardholder data with strong cryptography during transmission over open, public networks

Requirement 4 applies only to the transmissions of PAN unless specifically called out in an individual requirement. PAN transmissions can be protected by encrypting the data before transmission, or by encrypting the session over which the data is transmitted or both. PCI DSS v4 does not require that strong cryptography be applied at both the data level and the session level, but they do recommend both.

At the session level, system configurations should be verified to ensure strong cryptography and security protocols are implemented, and that keys and/or certificates that can not be verified are rejected. Some protocol implementations, such as SSL, SSH v1.0, and earlier versions of TLS have known vulnerabilities. Entities should be aware of industry defined depreciation dates for the cipher suites that are in use. Certificates should be verified to ensure integrity of all secure connections.

For Tenable Vulnerability Management the Protect Account Data widget provides details on each of the compliance controls for the compliance family group being referenced.

Protect Account Data - PCI-DSSv4.0 (Explore) ①								
	FAILED	PASSED						
4.2.1	57	42						
3.5.1	14	14						
3.3.2	14	14						

This widget focuses on the category Protect Account Data, which covers topics within PCI requirement 3 and 4. Both of these requirements cover protecting stored cardholder data, and the encrypted transmission of cardholder data. This widget provides details on each of the compliance controls for the compliance family group being referenced. The compliance control reference number is followed by a count, and compliance result for the compliance control. The specific controls being referenced are: 4.2.1|3.5.1|3.3.2|3.2.1

Compliance Audit Files

Additionally, audit files such as the TNS File Analysis - Credit Card Number audit file contains a number of file content checks. Files such as pdf, docx, txt, xls and more, are searched using this audit file for major credit cards (American Express, Discover, Maestro, MasterCard, VISA, UnionPay) and any potential credit card number, CVV or PIN. This .audit file searches the first 50k bytes looking for valid credit card numbers using regular expressions. Since potential credit card data may be found only the last four digits of the number are shown in the output. An example is shown below:

```
<item>
              : FILE CONTENT CHECK
type
description : "PII - Determine if a file contains a valid American Express credit card number."
file extension : "pdf" | "doc" | "xls" | "xlsx" | "xlsm" | "xlsb" | "xml" | "xltx" | "xltm" | "docx"
| "docm" | "dotx" | "dot" | "txt"
              : "([^0-9-]|^)(3[47][0-9]{2}(|-|)[0-9]{6}(|-|)[0-9]{5})([^0-9-]|$)"
regex
              : "American Express" | "CCAX" | "amex" | "credit" | "AMEX" | "CCN"
expect
              : "50K"
max_size
             : "4"
only_show
regex_replace : "\3"
</item>
```

Secure Sockets Layer

SSL and TLS are both cryptographic protocols which provide data encryption between network devices. The National Institute of Standards and Technology has stated that Secure Sockets Layer (SSL) v3.0 is no longer acceptable for protection of data due to inherent weakness within the protocol. As such, no version of SSL meets the PCI DSS definition of "strong cryptography."

SSL remains a common component of web security to encrypt data being transmitted between a browser and website, ensuring that sensitive information, such as login information and payment details are protected from eavesdropping. Therefore organizations should assess all their SSL/TLS implementations. Dashboards such as the <u>Maintaining Data Protection Controls</u> for Tenable Security Center, contain components which report on SSL/TLS, Encryption, Certificate Status, and more, assisting organizations in demonstrating to third parties and regulatory bodies that sensitive data is protected in accordance with Data Loss Prevention requirements.

antaini	ing Data Protection	Controls					2 Refresh All	Switch Dashba	oard * Options
cryption	- Cryptographic Compliance Con	cerns			SSL/TLS Discovery - SSL/TLS Vulnerat	pilities By Type			
8 Items			1 to 5 of 88 《	< Page 1 of 18 > »		Systems	Active		Passive
JGIN ID	NAME		SEVERITY	TOTAL	SSLv2	14	30		0
					SSLv3 TLS 1.0 (Deprecated)	277 2087	698 2491		27 0
73	SSL Medium Strength Cipher	Suites Supported (SWEET32)	Medium	2438	TLS 1.0 (Deprecated)	2087	4989		13
321	SSL RC4 Cipher Suites Suppor	ted (Bar Mitzvah)	Medium	680	TLS 1.2		4870		
91	SSL Certificate Signed Using V	Veak Hashing Algorithm	Medium	668	TLS 1.3	6	12		0
551	SSI Cortificate Chain Contains	s RSA Keys Less Than 2048 bits	Low	313					
					Last Updated: 9 minutes ago				
558	SSH Server CBC Mode Ciphers	s Enabled	Low	291	Windows File Contents Audit Results	- Compliance Summary			
Jpdated: 4 h	nours ago								
novahi-	Madia and Content Audite CDD	OM, Floppy, Other Storage Audit Checks			Check Count	Passed	Manual Check		Failed
lovable	meana and concent Audits - CDR	ow, noppy, other storage Audit Checks			Check Count Check Ratio	0	0		0
	Passed	Manual	Faile	ed.	System Count	0	0		0
	BitLocker	BitLocker	BitLoc		System Ratio	0	0		0
	CDROM	CDROM	CDRO						
	Remote Storage Removable Media	Remote Storage Removable Media	Remote S Removable		Last Updated: 9 minutes ago				
	Removable Storage	Removable Storage	Removable						
				storage					
	floppy	floppy	flopp	and the second	Unix File Contents Audit Results - Co	mpliance Summary			
	floppy	floppy		and the second	Unix File Contents Audit Results - Co		Manual Check		Failed
Updated: 9 r	floppy minutes ago	floppy		and the second	Unix File Contents Audit Results - Co Check Count	mpliance Summary Passed 0	Manual Check 0		Failed 0
				and the second	Check Count Check Ratio		Manual Check 0 0		Failed 0 0
	floppy minutes ago ction - Data at Rest - Encryption (and the second	Check Count Check Ratio System Count	Passed 0 0 0	0		0 0 0
ta Protec			Порр	and the second	Check Count Check Ratio	Passed 0	0		0
Updated: 9 r Ita Protec Items			Порр	ру	Check Count Check Ratio System Count	Passed 0 0 0	0		0 0 0
ta Protec Items ME	ction - Data at Rest - Encryption (Compliance	fiop 1 to 5 of 6 ≪	ey < Page 1 of 2 → ≫	Check Count Check Ratio System Count System Ratio	Passed 0 0 0	0		0 0 0
ta Protec Items ME 4 Ensure	tion - Data at Rest - Encryption C	compliance	Ropp 1 to 5 of 6 < SEVERITY High	ry < Page 1 of 2 → ≫ TOTAL 3	Check Count Check Ratio System Count System Ratio	Passed 0 0 0	0		0 0 0
tems ME 4 Ensure 9.67.3 Er	ction - Data at Rest - Encryption C configuration File Encryption is S -sure 'Allow indexing of encrypted	Compliance iet files' is set to 'Disabled'	fiop 1 to 5 of 6 ≪	Py ← Page 1 of 2 → ≫ TOTAL	Check Count Check Ratio System Count System Ratio Last Update: 9 minutes apo Data Protection - Certificate Status	Passed 0 0 0 0	000000000000000000000000000000000000000	SelSimed Certs	0 0 0
a Protect tems ME 4 Ensure 9.67.3 Er	tion - Data at Rest - Encryption C	Compliance iet files' is set to 'Disabled'	Ropp 1 to 5 of 6 < SEVERITY High	ry < Page 1 of 2 → ≫ TOTAL 3	Check Count Check Ratio System Count System Ratio	Passed 0 0 0 0	0	Self-Signed Certs 2185	0 0 0
tems ME 9.67.3 Er .9 Ensure	ction - Data at Rest - Encryption C configuration File Encryption is S -sure 'Allow indexing of encrypted	compliance iet files' is set to 'Disabled' y is configured - rpm	Ropp 1 to 5 of 6 < SEVERITY High	ry < Page 1 of 2 → ≫ TOTAL 3	Check Count Check Ratio System Count System Ratio Lett Updated 9 minutes apo Data Protection - Certificate Status Certs Found Expired	Passed 0 0 0 0	0 0 0 0 Untrusted 5SL Certs		0 0 0 Veakness
ta Protect Items ME 4 Ensure 9.67.3 En 6.9 Ensure	ction - Data at Rest - Encryption C configuration File Encryption Is S nsure 'Allow indexing of encryptee NIST FIPS-validated cryptograph	compliance iet files' is set to 'Disabled' y is configured - rpm y is configured - proc	Ropp 1 to 5 of 6 < SEVERITY High	ry < Page 1 of 2 → ≫ TOTAL 3	Check Count Check Ratio System Count System Ratio Lett Updated 9 minutes apo Data Protection - Certificate Status Certs Found Expired	Passed 0 0 0 0	0 0 0 0 Untrusted 5SL Certs		0 0 0 Veakness
ta Protect Items ME 4 Ensure 9.67.3 En .9 Ensure .9 Ensure .9 Ensure	ction - Data at Rest - Encryption C configuration File Encryption is S rsure 'Allow indexing of encryptec e NIST FIPS-validated cryptograph e NIST FIPS-validated cryptograph e NIST FIPS-validated cryptograph	compliance iet files' is set to 'Disabled' y is configured - rpm y is configured - proc	Ropp 1 to 5 of 6 < SEVERITY High	ry < Page 1 of 2 → ≫ TOTAL 3	Check Count Check Ratio System Count System Ratio Lat Updated 9 minutes ago Data Protection - Certificate Status Certs Found Expired 2217 10	Passed 0 0 0 0 0 Certs Expliring Soon 3 334	0 0 0 Untrusted SSL Certs 2197		0 0 0 Veakness
ta Protect Items ME 4 Ensure 5.9 Ensure 5.9 Ensure 5.9 Ensure 5.9 Ensure	ction - Data at Rest - Encryption C configuration File Encryption is S rsure 'Allow indexing of encryptec e NIST FIPS-validated cryptograph e NIST FIPS-validated cryptograph e NIST FIPS-validated cryptograph	Compliance iet files' is set to 'Disabled' y is configured - proc y is configured - grub	Ropp 1 to 5 of 6 < SEVERITY High	ry < Page 1 of 2 → ≫ TOTAL 3	Check Count Check Ratio System Count System Count System Ratio Last Updated: 3 minutes ago Last Updated: 3 mours ago Last Updated: 3 mours ago Last Updated: 3 mours ago	Passed 0 0 0 0 0 Certs Expliring Soon 3 334	0 0 0 Untrusted SSL Certs 2197	2135	0 0 0 Veakness
ta Protect ME 4 Ensure 9.67.3 Er .9 Ensure .9 Ensure .9 Ensure .9 Ensure ta Protect	ction - Data at Rest - Encryption C configuration File Encryption Is S ssure 'Allow indexing of encryptec e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph core spo ction - Confidentiality of Protected	Compliance iet files' is set to 'Disabled' y is configured - proc y is configured - grub	Ropp 1 to 5 of 6 < SEVERITY High High High High	Page 1 of 2 → ≫ TOTAL 3 2 1 1	Check Count Check Ratio Check Ratio System Count System Ratio Last Updated: 9 minutes ago Data Protection - Certificate Status Certs Found Expired 2217 10 Last Updated: 3 hours ago Data Protection - Removable Media to	Passed 0 0 0 0 0 Certs Expliring Soon 3 334	0 0 0 Untrusted SSL Certs 2197	2135	0 0 0 Weakness 581
tems ME 4 Ensure 9.67.3 Er 9 Ensur 9 Ensur 9 Ensur 9 Ensur 10 9 Ensur 10 10 10 10 10 10 10 10 10 10 10 10 10	ction - Data at Rest - Encryption C configuration File Encryption Is S ssure 'Allow indexing of encryptec e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph core spo ction - Confidentiality of Protected	Compliance iet files' is set to 'Disabled' y is configured - proc y is configured - grub	Ropp 1 to S of 6 < SEVERITY High High High High High High	Page 1 of 2 > > TOTAL 3 2 1 1 1 4 Page 1 of 2 > >	Check Count Check Raio System Count System Raio Latt Updated: 9 months ago Data Protection - Certificate Status Certs Found Expired 2217 10 Latt Updated: 3 hours ago Latt Updated: 3 hours ago Latt Updated: 3 hours ago	Passed 0 0 0 0 0 Certs Expiring Soon 8 334 noexee, nosuid, nodev Compliance	0 0 0 Untrusted SSL Certs 2197	2135 1 to 6 of 12 <	0 0 0 0 Weakness 581
tems ME 4 Ensure 9.67,3 Er 9 Ensur 9 Ensur 9 Ensur 19 Ensur 19 Ensur 19 Ensur 10 E	ction - Data at Rest - Encryption C configuration File Encryption Is S ssure 'Allow indexing of encryptec e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph cos ago ction - Confidentiality of Protected	Compliance iet ifiles' is set to 'Disabled' y is configured - rpm y is configured - proc y is configured - grub id Information Concerns	Ropp 1 to S of 6 SEVERITY High SEVERITY	Page 1 of 2 → ≫ TOTAL 3 2 1 1	Check Count Check Raio Check Raio System Count System Raio Latt Updated: 9 months ago Data Protection - Certificate Status Certs Found Expired 2217 10 Latt Updated: 3 hours ago Antipicated Status Ant	Passed 0 0 0 0 0 Certs Expiring Soon 8 334 noexec, nosuid, nodev Compliance novable media partitions	0 0 0 Untrusted SSL Certs 2197	2135 1 to 6 of 12 « SEVERITY	0 0 0 0 Weakness 581 Veakness S81 C Page 1 of 2 > > TOTAL
ta Protect MME 4 Ensure 9.67.3 Er 9.9 Ensuru 9.9 Ensuru 9.9 Ensuru 1.9 Ensuru	ction - Data at Rest - Encryption C configuration File Encryption (sure 'Allow indexing of encryptec e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph cos spo ction - Confidentiality of Protected Ensure 'Enable Windows NTP Serv	compliance iet ifiles' is set to 'Disabled' y is configured - rpm y is configured - grub ifiles' ifiles' is set to 'Disabled' (MS only) - Disabled	Ropp 1 to 5 of 6 SEVERITY High High	Page 1 of 2 > > TOTAL 3 2 1 1 1 4 Page 1 of 2 > >	Check Count Check Raio System Count System Raio Latt Updated: 9 minute ago Data Protection - Certificate Status Certs Found Expired 2217 10 Latt Updated: 9 hours ago Latt Updated: 9 hours ago Latt Updated: 9 hours ago Data Protection - Removable Media at 12 Items NAME 1.1.18 Ensure nodev option set on reference	Passed 0 0 0 0 0 Certs Expiring Soon 8 334 noexec, nosuid, nodev Compliance novable media partitions movable media partitions	0 0 0 Untrusted SSL Certs 2197	2135 1 to 6 of 12 « SEVERITY	0 0 0 0 Weakness 581 Crite 5
ia Protect tems ME 4 Ensure 9.9 Ensur 9 Ensur 9 Ensur 9 Ensur 9 Insur 9 Ensur 9 Ensur 10 Insur 11 Items ME 8.53,1,2 7.6 Ensur	ction - Data at Rest - Encryption C configuration File Encryption C ssure 'Allow indexing of encryptec e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph cos spo ction - Confidentiality of Protected Ensure 'Enable Windows NTP Serv rer 'Interactive logon: Number of J	Compliance iet if files' is set to 'Disabled' is set to 'Disabled' is configured - rpm is configured - grub is con	r is High	Page 1 of 2 > > TOTAL 3 2 1 1 1 4 Page 1 of 2 > >	Check Count Check Raio System Count System Raio Latt Updated: 9 minutes ago Data Protection - Certificate Status Certs Found Expired 2217 10 Latt Updated: 9 hours ago Latt Updated: 9 hours ago Latt Updated: 9 hours ago Data Protection - Removable Media at 12 items NAME 1.1.18 Ensure nodev option set on ref 1.1.19 Ensure nodev option set on ref	Passed 0 0 0 0 0 Certs Expiring Soon 8 334 noexec, nosuid, nodev Compliance novable media partitions movable media partitions emovable media partitions	0 0 0 Untrusted SSL Certs 2197	2135 1 to 6 of 12 « SEVERITY	0 0 0 0 Weakness 581 Crite 5
a Protect ME 4 Ensure 9.67.3 Er 9.9 Ensur 9.9 Ensur 10 Japane: 41 11 tems 8.853.1.2 7.6 Ensur 8.37.1 Er	ction - Data at Rest - Encryption C configuration File Encryption C ssure 'Allow indexing of encryptec e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph cos spo ction - Confidentiality of Protected Ensure 'Enable Windows NTP Serv re 'Interactive logon: Number of rssure 'Enable RPC Endpoint Mapp	Compliance Compliance iet if files' is set to 'Disabled' if softigured - rpm is configured - proc iy is configured - grub is configured	I to Sof 6 < SEVERITY High High High High SEVERITY High ris High High	Page 1 of 2 > > TOTAL 3 2 1 1 1 4 Page 1 of 2 > >	Check Count Check Raio System Raio System Raio Latt Updated 3 minutes spo Data Protection - Certificate Status Certs Found East Updated 3 hours spo Latt Updated 3 hours sp	Passed 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 Untrusted SSL Certs 2197	2135 1 to 6 of 12 « SEVERITY	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
ta Protect Items 4 Ensure 9 .67.3 Er 9 .67.3 Er 9 Ensur 9 Ensur 9 Ensur 9 Ensur 9 Ensur 10 Items ME 8.53.1.2 7.6 Ensu	ction - Data at Rest - Encryption C configuration File Encryption C ssure 'Allow indexing of encryptec e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph e NIST FIPS validated cryptograph cos spo ction - Confidentiality of Protected Ensure 'Enable Windows NTP Serv re 'Interactive logon: Number of rssure 'Enable RPC Endpoint Mapp	Compliance iet if files' is set to 'Disabled' is set to 'Disabled' is configured - rpm is configured - grub is con	I to Sof 6 < SEVERITY High High High High SEVERITY High ris High High	Page 1 of 2 > > TOTAL 3 2 1 1 1 4 Page 1 of 2 > >	Check Count Check Raio System Count System Raio Latt Updated: 9 minutes ago Data Protection - Certificate Status Certs Found Expired 2217 10 Latt Updated: 9 hours ago Latt Updated: 9 hours ago Latt Updated: 9 hours ago Data Protection - Removable Media at 12 items NAME 1.1.18 Ensure nodev option set on ref 1.1.20 Ensure nodev option set on ref 1.2.20 Ensure nodev option set on ref	Passed 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 Untrusted SSL Certs 2197	2135 1 to 6 of 12 « SEVERITY	0 0 0 0 Weakness 581 Crage 1 of 2 → ≫ TOTAL 5 5 5 5 5 5 4

O

Tenable Vulnerability Management widgets such as the **SSL Certs That are Expired or Soon-to-Expire** and the **SSL -TLS Insecure Communications Issues and Info** widgets, list assets that have SSL Certificates that have already expired or will soon expire and current SSL and TLS insecure communication exposures in the environment respectively.

SSL - TLS Insecure Communications Issues and Info (Explore)

Updated 5/20/2024

Plugin Name	First Value of Severity	Count	
SSL Certificate Cannot Be Trusted	Medium	123	
SSL Self-Signed Certificate	Medium	84	
SSL RC4 Cipher Suites Supported		81	
SSL 64-bit Block Size Cipher Suit	Medium	78	
TLS Version 1.0 Protocol Detection	Medium	64	
TLS Version 1.1 Protocol Depreca	Medium	60	
SSL Medium Strength Cipher Suit	High	57	
SSL Expired Certificate Detection	Medium	37	

O

÷

÷

SSL Certs That are Expired or Soon-to-Expire (Explore)

Updated 5/20/2024

Plugin Name	First Value of Severity	Count
SSL Certificate Expiry	Medium	27
SSL Certificate Chain Contains Ce	① Info	9
SSL Certificate Expiry - Future Ex	Info	9

Web Application Scanning

Tenable Web App Scanning contains a predefined scan policy which allows for deep analysis of the SSL configuration of a web server on the public internet. This scan result provides insight into the organization's SSL/TLS configuration based on industry standards.

$\equiv \bigcirc$	tenable	Web App Scanning		© ((°°¢ III 😶
ស		Create Scan Template 의		×
□ ©	Scans	 Standard Scan Duration: A few hours This scan focuses on misconfigurations, the component vulnerabilities and the common generic vulnerabilities. 	SSL-TLS Scan - User Defined An audit of web application implementation of SSL/TLS. Basic Advanced	Scan Template
0	Saved	Log4Shell Detection of Apache Log4J CVE-2021-44228	General Template Name	
	0	Overview Scan A scan that outlines URL paths and builds a site map.	SSL-TLS Scan - User Defined Description Example: This is my daily scan	t of 0 → →
		CI ASV Scan A WAS scan used for PCI ASV scans.	Example, rins is my uany scan	
		Ouick Scan Duration: Few minutes This scan focuses on configuration issues related to SL/TLS and HTTP security headers.	User Permissions	
		Custom Scan Duration: Variable Control all settings and choose the plugins you want to run.	Default No Access	
		An audit of web application implementation of SSL/TLS.	Cancel Sa	ve Template

Control Objective 3: Maintain a Vulnerability Management Program

This objective focuses on proactively updating antivirus software, maintaining secure systems and applications, and implementing strong access control methods. All systems that are susceptible to malware are protected with antivirus software. All antivirus software should be kept up to date. Malware detection scans are run periodically, and all infected systems should be remediated. Patches and updates should be installed within one month of release for critical systems. Maintaining a strong vulnerability management program ensures that security concerns are addressed before they can be exploited, safeguarding cardholder data and meeting PCI DSS compliance standards.

This control objectives covers the following PCI DSS requirements:

Requirement 5: Protect all systems and networks from malicious software.

Requirement 6: Develop and maintain secure systems and software.

PCI Requirements Under This Objective Supported by Tenable

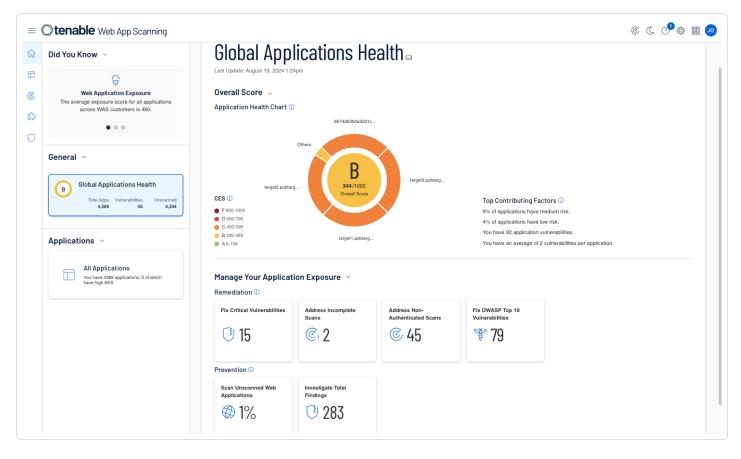
PCI Requirement 5: Protect All Systems and Networks from Malicious Software

Malicious software, often referred to as malware is any software that is designed to harm, exploit, or otherwise compromise the confidentiality, integrity, or availability of a computer system, network, or device. Included are a variety of tactics such as viruses, ransomware, spyware, and adware. Malware can enter the environment through many business approved activities, such as email, or the approved use of storage devices. Using antivirus or anti-malware software, combined with a robust vulnerability scanning program helps address these concerns. Performing periodic scanning or continuous monitoring of the environment will help ensure that previously undetected malware is identified. Scans should include all systems in the CDE.

When protecting systems and networks is paramount, Tenable has a comprehensive security solution that provides continuous visibility, critical context and actionable intelligence. These products provide purpose built PCI compliance dashboards, Assurance Report Cards (ARCs) to assist organizations in monitoring ongoing compliance with PCI DSS.

Web Application Scanning

Tenable Web App Scanning provides comprehensive vulnerability scanning for modern web applications. Accurate vulnerability coverage minimizes false positives and false negatives to ensure that security teams understand the true security risks in their web applications. Tenable Web App Scanning provides safe external scanning so that production web applications do not experience disruptions or delays. Information presented allows organizations to categorize findings and remediate vulnerabilities quickly.



Tenable Security Center

There are a series of PCI dashboards for Tenable Security Center that assist in supporting an organization's PCI compliance journey. These dashboards focus on PCI control objectives. The information contained within the dashboards provide insight to help organizations secure their systems against vulnerabilities that could lead to data breaches.

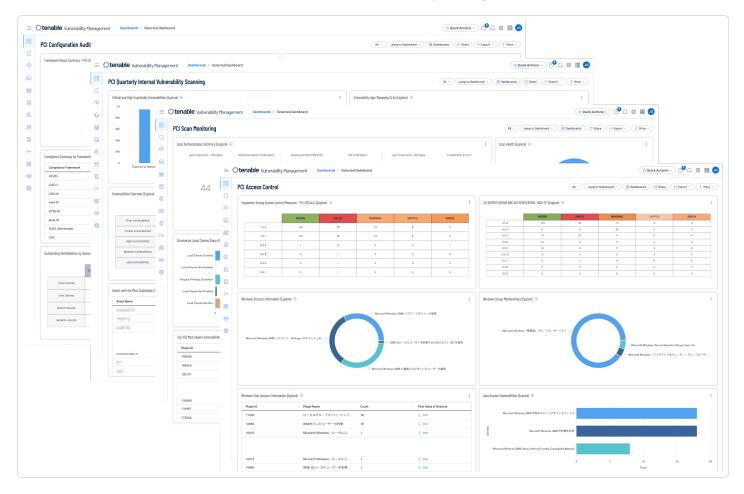
onfiguration Audit	0					Refresh All III Switch Dashboard > Options >			
I Monitoring - Configuratio	on Trends		I CSF - Com	pliance Checks By Keyword		1			
4,000		_			(Last 7 Days)	Passed Manual Failed			
3.000	5010 H 11 1		~~~~	AI 65	•	SIN IN SIN SIN	h Dashboard v Ø Options v		
1.000	PCI Scan Monitoring 🗅					D Refresh All	Nusindoard V Uptions V		
o 2006 7106 7106 7106 7106 7106 7106 7106 7	Tenable Admin - Nessus Scanning St	atus	i Vulnerability Summary -	Exploitable Vulnerabilities		Vulnerability Summary - 3-Month Trend of Vulnerabilitie	8 1		
	Systems Scans (Last 14. Scan) 1.523 010	Errers Scan Duration Thorough Tests C PCI Quarterly Internal Vulne	redentiated Ch	IV Accessible Windows Man QS X	LingeUNX	10,000	C Refresh All E Switch Dashboard ~	Options ~	
aat Updaled: 1 minute ago	Last Updated: 2 minutes ago	PCI Monitoring - Mitigated Critica	al and High Vulnerabilities		1	PCI Monitoring - Vulnerability Trends		1	
PCI Monitoring - Configurat		Total Vulnerabilities	Migaled <10d M	ligated 10-30d Mitigated >00d	_	4,000	-	_	
	Track Mitigation Progress - Vulnera	Criscal	50% 29% 61%	10% 60% 10% 10% 10% 10% 10% 10% 10% 10% 10% 1		2,000		~	
Check Count Check Ratio	Mitigated Unv Total 2,203 1					1.000			
System Count System Ratio	Critical 358 High 1.168 8 Medum 599 0	Last Updated: 20 minutes ago						8 2 7 9 2	
	Low 78							80000	
aat Updated: 1 minute ago		PCI Monitoring - Most Vulnerab	PCI Access Control 🙃				C Refr	ash All 🛛 🗱 Switch Dashboard 🗸	© Options ~
	Last Updated: 2 minutes ago	25 ltem(s)	CSF - User Access and Least Privilege Com	pliance Checks	PCI Monito	ring - Account Compliance			1
Inderstanding Risk - Reme	PCI Monitoring - Mitigated Vulnerat	IP Address DNS		eed Manual Failed Hosts with F	999 liem/s			110 5 of 999 < < Pa	ige t of 200 → Э
100 Item(s)	Missied	TARK INCOME	Bysiens Scans (Last Pas Account 40 C C Admin.Root 41 C C	sed Manual Failed Hosts with E 5 53% 47% 54	Name			Severity ~	Total
Steps to Remediate Apply KB5043051: Windows 10 *	Total Vulnerabilities 20%	110.00	Password/Cr. 37 © 3 800-53 (A &. 36 © 44	n 0/1 201 31 n 01 01 32 n 01 01 32		e 'HTTP source restriction' is set to an authorized IP address		нын	6
Install patch 119757-45 or higher	High 22% Medium 20%	10.00	CIS COC 5 & 20 O 14 CSF PR.AC-1 27 O 45	rs 645 6875 20 rs 645 5275 20		025 - Teredo packets must be blocked inbound to the enclave and outbound fro		HIGH	6
Fix RHEL 7 : nss (Unpatched Vu	Low 29%					020 - Teredo packets must be blocked inbound to the enclave and outbound fro	m the enclave 'outside out ACL'	нюн	6
Install the Apr2024 CPU from the		Last Updated: 40 minutes ago	Last Updated: 15 minutes ago			Network element is not password protected Network devices must be password protected 'ASDM authentication'		нын	6
Apply Security Updates for Micro	Last Updated: 2 minutes ago								
ant Updated: 1 minute ago		PCI Monitoring – Most Mitigatec	Account Weakness - Access Control Compl	lance Issues I	Last Updated	16 minutes ago			View Data >
		0 litern(s)	20 ltem(s)	1 to 7 of 20 € ⊂ Page 1 of 3 > >	CSF - Acce	ount and Group Information			1
		Plugin ID Name	Plugin ID Name	Severity v Total	8 Item(s)			thoSofii < <	Page 1 of 2 > >
			1004978 NET0433 - Network devices must us 1004979 NET0433 - Network devices must us		Plugin ID	Name	Family	Severity	Total ~
		Last Updated: 40 minutes ago	1004979 NET0433 - Network devices must us		71246	Enumerate Local Group Memberships	Windows	INPO	14
			1005030 NET1639 - The network element mut	t tim HIGH 6	72684	Enumerate Users via WMI	Windows	INFO	12
			1005034 NET1639 - The network element mut		38680	Microsoft Windows SMB Last Logged On User Disclosure Microsoft Windows SMB : Obtains the Password Policy	Windows . User management	NFO INFO	10
			1005035 NET1640 - Network devices must log		10902	Microsoft Windows 'Administrators' Group User List	Windows : User management	INFO	10
			1005037 NET1647 - The network device must		Last Updated 1	16 minutes son			View Data >
		_	Refreshing	View Data >	Law spedied				view para 2
					_				

Within the Access Control dashboard, user account focused widgets are provided to help analysts see activities detected in the organization around user accounts. All user accounts such as regular user accounts and administrative accounts should be monitored for unusual activity. Multiple industry recommendations from standards such as PCI and NIST CyberSecurity Framework (CSF) are provided to help analysts see potential malicious indicators around user accounts. Examples of these indicators, such as privilege changes and group membership changes, alert analysts as changes may not be expected and should be validated. Analysts can use these widgets to help determine what typical activity should be on a network and then be more aware of when abnormal activity takes place within the organization.

The PCI Scan Monitoring dashboard provides security teams with detailed insight into their organization and vulnerability management posture. Vulnerabilities are filtered by severity and exploitability to identify at-risk hosts. Detailed information about remediation opportunities and risk issues are presented. Indicator matrices alert to the detection of specific exploitable vulnerabilities and patch management details. Nessus scans are monitored for progress and errors, and vulnerability trend data is presented. By effectively monitoring the network for vulnerabilities and remediation options, security teams can better ensure network integrity and security.

The PCI Configuration Audit dashboard presents extensive data about the configuration status of the network based on the available data. The dashboard can be used to gain insight into all configuration results, or can be modified to focus exclusively on the results related to the cardholder data environment (CDE). Organizations can configure repositories or asset lists in order to tailor the focus of the dashboard.

The PCI Quarterly Internal Vulnerability Scanning dashboard presents extensive data about the vulnerability status of the network based on the available data. The dashboard can be used to gain insight into all vulnerability results, or can be modified to focus exclusively on the results related to the cardholder data environment (CDE). Organizations can configure repositories or asset lists in order to tailor the focus of the dashboard.



A similar series of dashboards exist for Tenable Vulnerability Management.

Tenable Vulnerability Management

Tenable Vulnerability Management PCI-DSSv4.0 Audit Summary dashboard.

Oten	able [:] Vul	nerability i	1anagemer	nt Da	ishboards > Si	elected Dashboard						1	Vuick Action	s ~) ⑦ [🍨 🔅 嘂
CI-DSSv4	.0 Audit	Summar	y (Explor	·e)						All - Ju	Imp to Dashboard 🗸	B Dashboard	is 🗹 Share	[→ Export	 More
Framework Res	ult Summary	()			:	Control Summary	0			:	Audit Check Type	Summary 🛈			:
	F	PASSED ~				Compliance Fa	mily Re	eference Count	All Val	ue of Result	Plugin Name	R	eference Count	All Valu	ue of Result
						Implement Stro	ong 24	173			Unix Compliar	nce C 38	587		
						Build and Main	itain 20	040			Windows Corr	iplian 16	345		
						Regularly Mon		95	_		OpenShift Cor		1	_	
					RROR	Maintain a Vul					Palo Alto Netw				
					ARNING	Protect Accour					Brocade Fabri				
						TOIGGT ACCOUR	. Jaia 20				Juniper Junos				
		FAILED -									SonicWALL Se				
											BlueCoat Prox	ySG 60)		
2.2.4	PASSED 293	FAILED	SKIPPED 34	WARNING	ERROR 7	7.2.2	PASSED 705	FAILED 335	WARNING 82	SKIPPED 8		FAILED	PASSED	WARNING	ERROR
1.4.1	291	131	0	31	7	7.2.1	705	335	82	8	5.2.1	58	24	2	0
1.2.1	291	131	0	31	7	8.2.8	61 5	53	0	0	6.3	56	14	26	2
1.5.1	260	134	0	0	0	8.2.3	14	4	0	0	6.3.3	54	12	25	2
2.2.7	81 43	98	0	0	0	8.2.2	14	4	0	0					
1.4.2	43	46	0	0	0	8.4.1	0	3	0	0	6.3.1	39	14	12	0
1.4.3	0	6	0	0	0	8.4.3	2	3	2	0	5.3.1	0	1	0	0
	t Data 🛈				i	Regularly Monitor a	and Test Network	ks 🛈		÷					
Protect Accoun		PASSED	FAILED		VARNING	10.2.2 10.3.3 10.3.2	PASSED 293 3 24	FAILED 202 34 13	SKIPPED 0 0 8	WARNING 0 0 5					
Protect Accoun			66		2	10.6 10.6.1 10.6.2 10.6.3 10.2.1.7	0 0 0 0 5	16 16 16 16 0	0 0 0 0	0 0 0 0 0					
Protect Accoun		69						0	0	0					
4.2.1 3.3.2		69 28	13		9	10.2.1 10.2.1.6 10.2.1.5 10.2.1.4 10.2.1.1	5 5 5 5 5	0 0 0 0	0 0 0 0	0 0 0 0					

Antivirus

There are a number of plugins available which detect if an antivirus product is installed, running, and up-to-date. These include:

- 24232 BitDefender Check
- <u>20284</u> Kaspersky Anti-Virus Check
- <u>12107</u> McAfee Anti Virus Check

- 21608 NOD32 Antivirus System Check
- <u>12106</u> Norton Anti Virus Check
- <u>12215</u> Sophos Anti Virus Check
- 20283 Panda Antivirus Check
- <u>21725</u> Symantec Anti Virus Corporate Edition Check
- 16192 Trend Micro Anti Virus Check
- 24344 Windows Live OneCare AntiVirus Check

PCI Requirement 5.3 requires that anti-malware mechanisms and processes are active, maintained, and monitored. For anti-malware solutions to be effective, they need to be functional, and have the latest updates and signatures. The above plugins only report an issue if a problem is found with the detected antivirus solution. Nessus also has plugin #<u>16193</u> which aggregates the results from these and other plugins. This is useful if you are in a multiple anti-virus solution environment and just want to find hosts that have a solution installed and operational. While the individual product detect plugins only report an issue if a problem is found with the detected antivirus solution, plugin <u>16193</u> reports if a system does have a known working anti-virus solution. Further details can be viewed by reviewing the plugin output. In this example, the plugin output for 16193 displays the antivirus application, file path, version, antivirus engine version, and antivirus signature version.

Findings 🗅		dia. Make Annifestion Fin	dia an				Includ	de Info Sev	erity 🚺 🤇	√ All Time
Advanced	Saved Filters v Search by Asset N		-							
Plugin ID: is equal to 161 Al Inventory 118 Vulnerat	Group By None Asset Plugin		\mathbf{X}		Fetched At: 11:53 AM	Grid: Basic View $ \sim $	Columns v	1 to 50 of	118 ~ K < F	'age 1 of 3 → ⊃
Asset Name		Se Plugin Name		Sv3 Base State	Scan Origin	Asset Tags	ACR	AES	Last Seen	Actions
		Ini Antivirus Software Ch	leck	New	Tenable.io		N/A 6	N/A	10/31/2023	1
	(Ini Antivirus Software Ch	leck	Active	Tenable.io	10.00	4 😡	629	08/19/2024	1
 		Ini Antivirus Software Ch								
_		Int Antivirus Coffware Ch		Active	Tenable.io	10,000	4 😡	601	12/11/2022	
ntivirus Softw		Int Antivinus Coffware Ch	innt	Loss.	Tanahla ia	10.040	4 6			: : See All Details
ntivirus Softw		•	ion	Active Iver Overview Plugin O	Tanahla ia	111 1/10	4 6			: : See All Details
ntivirus Softw sset Information	are Check	 Int Antivirus Coffware Ch Vulnerability Informat 	innt	Loss.	Tanahla ia					
ntivirus Softw sset Information ME 44 ADDRESS	are Check	Vulnerability Informat	ion () Info	Overview Plugin O	Tanahla ia utput		4 @			
ntivirus Softw seet Information ME 44 ADDRESS ERATING SYSTEM	are Check	Vulnerability Informat SEVERITY PLUGIN ID PORT PROTOCOL	ion () Info 16193 [2] 445 TCP	Overview Plugin Ou Plugin Output	Tapable is					
ntivirus Softw set Information ME 4 ADDRESS ERATING SYSTEM STEM TYPE	are Check	Vulnerability Informat SEVERITY PLUGIN ID PORT	ion () Info 16193 (2 445	Overview Plugin Ou Plugin Output Forefront_Endpoint	Terable is utput Protection : alware product i ;	s installed on t	A compared to the remote ho	eno ost :	12/(1/2022	
ntivirus Softw sset Information ME 44 ADDRESS VERATING SYSTEM STEM TYPE TWORK	are Check Microsoft Windows Server 2022 Standard Build 20348 general-purpose	Vulnerability Informat SEVERITY PLUGIN ID PORT PROTOCOL LIVE RESULT	ion () Info 16193 [2] 445 TCP	Overview Plugin Ou Plugin Output Forefront_Endpoint A Microsoft anti-m	Terable is utput Protection : alware product i ;	s installed on th	A compared to the remote ho	eno ost :	12/(1/2022	
ntivirus Softw seet Information ME /4 ADDRESS reparting system stem type twork is (FQDN)	are Check Microsoft Windows Server 2022 Standard Build 20348 general-purpose Default	Vulnerability Informat SEVENTY PLUGIN ID PORT PROTOCOL LIVE RESULT Discovery	ion info 16193 [2 445 TCP No	Overview Plugin Ou Plugin Output Forefront_Endpoint A Microsoft anti-m Product name Path 8-0\ Vorsion	Tanabla in utput 	s installed on ti Windows Defender Ci VPogrambata\M. 4.18.2300.2008	A compared to the remote ho	eno ost :	12/(1/2022	
ntivirus Softw sset Information ME 44 ADDRESS ERATING SYSTEM STEM TYPE TWORK IS (FODN) Additional Informat OUD	are Check Microsoft Windows Server 2022 Standard Build 20348 general-purpose Default	Vulnerability Informat SEVERITY PLUGIN ID PORT PROTOCOL LIVE RESULT	ion () Info 16193 [2] 445 TCP	Overview Plugin Ou Plugin Output Forefront_Endpoint A Microsoft anti-m Product name Path 8-0\ Vorrion Engine version Antivirus signat	Tanabla ia utput Protection : alware product i 	s installed on th Mindows Defender (c) kProgramData\M: 4.18.23090.2007 1.1.23090.2007 1.1.2390.2320.	A compared to the remote ho	eno ost :	12/(1/2022	
ntivirus Softw set Information ME 44 ADDRESS ERATING SYSTEM STEM TYPE TWORK 55 (FQDN) Hditional Informat QUD SCONFIGURATIONS	are Check Microsoft Windows Server 2022 Standard Build 20348 general-purpose Default	Vulnerability Informat SEVERITY PLUGIN ID PORT PROTOCOL LIVE RESULT Discovery FIRST SEEN	tion ① Info 16193 [2] 445 TCP No 10/31/2023 at 09:25 AM	Overview Plugin Ou Plugin Output Forefront_Endpoint A Microsoft anti-m Product name Path 8-0\ Vorrion Engine version Antivirus signat	Tanabla in utput Protection : halware product i : : : :	s installed on th Mindows Defender (c) kProgramData\M: 4.18.23090.2007 1.1.23090.2007 1.1.2390.2320.	A compared to the remote ho	eno ost :	12/(1/2022	
ntivirus Softw sset Information ME 44 ADDRESS VERATING SYSTEM STEM TYPE TWORK STEM TYPE TWORK SSTEM TYPE TWORK SSTEM TYPE TWORK SSTEM SSCONFIGURATIONS SSSET SSEEN	are Check Microsoft Windows Server 2022 Standard Build 20348 general-purpose Default	Anticipus Software Ch Vulnerability Informat SEVERITY PLUGIN ID PORT PROTOCOL LIVE RESULT Discovery FIRST SEEN LAST SEEN LAST SEEN	ion () Info 16193 (2) 445 TCP No 10/31/2023 at 09:25 AM 10/31/2023 at 09:25 AM	Overview Plugin Ou Plugin Output Forefront_Endpoint A Microsoft anti-m Product name Path 8-0\ Vorrion Engine version Antivirus signat	Tanabla ia utput Protection : alware product i 	s installed on th Mindows Defender (c) kProgramData\M: 4.18.23090.2007 1.1.23090.2007 1.1.2390.2320.	A compared to the remote ho	eno ost :	12/(1/2022	

Requirement 6: Develop and Maintain Secure Systems and Software

Bad actors are always searching for vulnerabilities which can provide an easy method for gaining access to systems and networks. Keeping systems updated and patched mitigate the majority of these potential entryways. PCI DSS requires that all system components have all the appropriate software patches installed to protect against the exploitation and compromise of account data. Appropriate patches are defined by PCI DSS as those patches which have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations.

Prioritizing patches for critical infrastructure will ensure that high priority systems and devices are protected from vulnerabilities as quickly as possible after a vendor releases an update. Public facing websites are primary targets for attackers and should be tested for vulnerabilities on a regular basis.

Tracking updates for the constantly changing landscape of assets is important to identify legacy code and asset footprint. The Outstanding Remediations Tracking dashboard, shown below for <u>Tenable Vulnerability Management</u> and <u>Tenable Security Center</u>, focuses on legacy patches and assets to reduce management effort and reactive firefighting. Organizations can identify parts of their network that have been missed by patching cycles, or where traditional mitigation methods no longer apply.

by breaking - 1	e Der Mit Auflahr D	e Inde				1.1	Datasetsy Rose	at Armilaine	The size field if	Matte Dytest 🕈							
	Name	1984		Pater.	100				101101	1784		max.					
- 10.04	1.1						- 36.0	÷					4				
1.1.1.1	1.1	Outstanding Rene	diations Track	ing o									Ohie	an) (Blanco	dinasi -	(Balan -	
11-100 (repri																	
and input	2.0	Outstanding from all	allona - Time Deva	Patrick/Patriceline	(America)					Existing Para	dations by Device Ty	pe Phyleretellities)					
ing Thermodiation of the	lein 'geligiet (LITTLE Transformer Little Little Little Little	-				1			ton faith Tac boose States of States States of States	international and a second sec	1952 4 19 10 10 10	21+1+	100 10 10 10 10 10 10 10 10 10 10 10 10		1 1 1 1 1 1 1 1	
	-																
Cross Devices.		Tel: State of the second								Lat good interrup							
and the local data										Debd Likebolies	+ Defection						
		famolation hash	ng - Kup Ki Barnad	ignis.na													
		A THINK I					10000		1 C 10 C	To have		Pareto:		Territy .		har I	
Internal Control	· ·	Dage to Recedulate			Real Reduction	Red To	ni Teal	Doore -	0.05	North National States	- 1.4	temp		Children of		1	
		Appa KEDOGER, West	tes Unipolar (UC)	10 (m) (m) ()	1.0-1	+	-04	4,010	8.004	Tenane Tenne Ager		Mar.			_		
		100 per 1077-0	- 10		1.041	+		1.010	+	Rector Drapheria		(beneral)			-	1	
		Autority Processing	nar severity		10%		-	1.118	-	Datase Linux Mid. (1)	tel	deneral		2014		1	
		A stat the report of the			4.546	1	*	**	178	TaxITS 814-(14)		Therapeut .			-	1.00	
		Apply Decemp (School)	www.work.iktiinee	NUCL OF COMPANY	4.0%	+		- 14	1.0	tor some rooms						Verlage 1	
		Configurated Workson and							Tee Data (s	tar and there are							

R

The Maintain a Vulnerability Management Program widget for Tenable Vulnerability Management focuses on the category Maintain a Vulnerability Management Program, which covers topics within PCI requirement 5 and 6. Both of these requirements cover the need for maintaining a vulnerability management program to protect systems against malware, and develop and maintain secure systems and applications. This widget provides details on each of the compliance controls for the compliance family group being referenced. The compliance control reference number is followed by a count, and compliance result for the compliance control. The specific controls being referenced are: 5.3.1|6.5.3|6.3|5.3.3|6.3.1|6.3.3|5.3.2|5.2.1

	FAILED	WARNING	PASSED
1.5.1	22	10	4
2.2.4	10	7	11
2.2.7	8	0	0
1.3.2	6	0	6
1.4.1	2	2	2
1.2.1	2	2	2

O

For example, reviewing the details of the cell for failed checks, in the row for PCI Requirement 6.3, clicking within the cell will drill down into the details. The next screen presented is the findings page, shown below:

				~			
Findings o 💊							
Vulnerabilities Doub	Record return Hethadte Webdapt	Lation Pindinga					
	teed Filters = C. Compliance Prevanet in a party operators to	POLOSSI AL IND Compliance Parti	Sama is again to Maintain a Webanielity Manag	ement Program AND Last challest aitNet last in	lohaya 1847 Nasadri kudi kari ta sat anpat to As	nghal) Mil Panat is agus to Palas Arili Complexe.	Grantin x J Apply
· Brochels	() hetwee				Page 10, 10, 10, 10, 10, 10, 10, 10, 10, 10,	041 Ball Part - Talance - 15,52 (1) -	C C Page 141 S - S
Auto Nama		Autoritie		hand	Asia funa	donat Taga	Birtists.
 b10 Devices 	Addeds Log Hard events for Oracle or Update Public IP Ad	de co.wood.Asse.fo	No.11.1124.00	S name	Contraction of Contraction	100,000,000	1
115 Dawn and	and, paches, and additional security software are reason	08.0908.068.04	S.L.I. Severandt	O rated	and Street	and install	1
 BADeve be 	Animity Log Plant anistic for Datein Nation & Descriptions	e CitationitAnd.to	Market (11), 100	C Faled		10.716	1
 Altilants 	e Antoly Log Net and the Dalate Public IP Address rule	City and Assoched	Market (115) and	C Falar	11.00.000		1
 Al2 have be 	forticity Log Hart aniato for Graate or Upriate NOL Scenar	n. Children da	Market Citation	(C) Failed			1
D MARDING M	Autority Log Hart evidents October 508, Server Frended Riv	a constant	Mine. #11.11 add	O failed			1
 13.0 December 	Autority Log Plant and the Date in 202, Server Frend Pl	de CELMINISTANIA	and and the lot and	O Falled	and stated		1
	Automa Lag Alari annas la Dalvia Materick Berunia Bro-			() Pated			
	at Auto provinsioning of Long-Amplytics against hot Agains 1944			(1 Faler	100.000		
beent Information	e, patches, and additional security so	Not built information		Overview Rollt Output			Dec Al Decelor
AVE TWODIESD		ALC: WHE	1.3.5 Ensure updates, patches, and antitional security schears are modern	Poles laive			
MENTRO PRIMA	Linux Renal 5 10.5-514.10.3 eff al8, bit on CentOD Linux release 7.4 1011 (Cent)	AMP YOU	05.5m05.0nx,7.411.11.5mm and	real: 14 (histopia reard-specia)	then anto "pass"): Hi		
KETEN TYPE	perient-populate Delauli	BOVO-644N	Citil Carefold Linux Tilleminerark/Litil Server et 0.5	unberry , beaul		/	
elterolek mit (Falm)	Darry .	ISONO-INVESTIGATION INVESTIGATION	CIE DeriGIE Linux Tillemiterant UI Server	Actual Value			
keet Scen Information		INCOMENTATION OF STREET	4.8.5	The summer of the data stands	aphotos the estimate the state of the state		
NUT OF IN	DET/CTOCH wilds THE ALA DEF/CEDCH will DE MAR	covimo, e	This hand for the full of the second se	Doubed ploping : Destautation			
INF SITE AND IN A REAL	INFORMATION AND ADDRESS	10.1000 MME	いんホスングライアンスチェック	A borner adjated manufa From Authors	and togething		
AND CONTRACTOR	SP/0300H will 10.08-AM	P60147	(3) Palmi	· spale mirrors around the	K		
Conce.	Name Tax	10,000	Available	· spinses alova, resta, lati.	and the former and		
		And and American Street		Genilly, add, 44 Batterie Blackager, com, 54	12120-01-01-02	lower contract and	
		Audit Discovery		Betwee Official period lines, and the second s	11110-0-0-0173	cardinal and	
		LAST NUDIT	CREDITION & TODA HM CREDITION & TODA HM	Betwee Kinnepet-42(), add, 34 Betwee Manager (2011), add, 34	1+1-19-0-0-417.3	sandret was	
				4411.489.84	1.1.(1)-(0, 617	lowing law	
		Reference Information		alignetic and the second secon	1.1.81.80	lager lager	
		00007	14	wathroad1.p. #84_04	4-1-1-20-00-00.7	Training Contraction (1997)	
		00010	13	avail-soluting_abl_	4.4.X2-00.807 8.4.4.4.00.407	la marte	
		oane	1.4	heads +100, 14	411.44-00.817.8 1971.01.01.01.95.Ph.011.01.05	regardine was	
		140%	14	In the Area in the second s	104-114-04-05-075-05	cinded and	

 \cap

Checking the filters presented allows verification of the data being presented. In this case, Compliance Framework PCI-DSSv4.0, the PCI Objective is to Maintain a Vulnerability Management Program, Results are Failed audit items, and the PCI Requirement is 6.3. Selecting an Audit Item (1.2.5 Ensure updates, patches, and additional security software are installed) presents additional details at the bottom of the page, including the results from a yum check-update command. Nessus ran the command during the audit to check for updates to any installed packages. The results were captured and logged. Those results are available in the Audit Output tab. Since there are a number of updates that are available, this check has failed. Once updates are applied, this audit item will then be displayed in the pass column.

Control Objective 4: Implement Strong Access Control Measures

This objective ensures that access to cardholder data is restricted to only authorized users with a legitimate need. Access is to be controlled by business need-to-know, and each person with computer access is assigned a unique identifier (ID). Access is to be authenticated to all system components ensuring individual accountability. By regulating who has access to certain systems, networks, or files, organizations can reduce the risk of unauthorized actions, data breaches, or fraud. This control objectives covers the following PCI DSS requirements:

Requirement 7: Restrict access to system components and cardholder data by business need-toknow.

Requirement 8: Identify users and authenticate access to system components.

Requirement 9: Restrict physical access to cardholder data. **

Note: ** Notes related to Requirement 9. This requirement is related to the controls around physical access to cardholder data or systems that store, process, or transmit cardholder data. While this requirement is not supported by Tenable directly, the recommended practice here is to restrict data and access to authorized individuals only and remove systems or hard copies containing this data.

PCI Requirements Under This Objective Supported by Tenable

Requirement 7: Restrict access to system components and cardholder data by business need-toknow

Controlling and restricting access to sensitive systems and devices is important for many reasons, especially in protecting cardholder data. Strong access control maintains the confidentiality and integrity of systems, and ensures that only authorized users can access sensitive data, such as financial records, personal information, and proprietary business information. By controlling who can perform certain actions within a system, strong access control prevents unauthorized modifications, deletions, or additions to data, maintaining the integrity and reliability of the systems and information. PCI DSS requires that access levels must be "need to know" and "least privilege", providing the least amount of access, with minimum privileges to perform a job. These requirements apply to all service and user accounts for employees, contractors, consultants, and internal or external vendors and other third parties.

Requirement 8: Identify users and authenticate access to system components

PCI DSS states, two additional fundamental principles of identifying and authenticating users are to 1) establish the identity of an individual or process on a computer system, and 2) prove or verify the user associated with the identity. The identity aspect is the account identifier, such as a user, system, or application ID. The element that proves or verifies the identity is the authentication factor. Authentication factors are something you know, such as a password, something you have, such as a token or smart card, and something you are, such as a biometric element. These elements are based on industry standards and best practices. <u>NIST 800-63</u>, <u>Digital Identity</u> Guidelines provides additional information.

Tenable Identity Exposure helps organizations validate Active Directory and Entra ID environments for weakness, misconfigurations, and activity that can lead to damaging attacks. Such as removing inactive accounts not used for 90 days, verification of timeouts, or idle time, and Multi-Factor Authentication (MFA).

For more information on getting started with AD Security, and Tenable Identity Management, reference this <u>Identity and Access Control guide</u>.

The Implement Strong Access Control Measures widget covers topics within PCI requirement 7 and 8.

	PASSED	FAILED	WARNING	SKIPPED	ERROR
7.2.2	289	206	64	8	0
7.2.1	289	206	64	8	0
8.2.8	35	37	0	0	0
8.3.4	1	26	0	0	1
8.2.3	16	6	0	0	0
8.2.2	16	6	0	0	0
8.4.3	0	0	2	0	0
8.4.1	0	0	2	0	0

Audit items checked and validated include, but not limited to: Ensuring accounts are secured, root accounts are secured, permissions to files related to authentication are correct, SELinux policies are configured (if appropriate for the system in question), and more.

Both of these requirements cover the need to restrict access to cardholder data by business need to know, identify and authenticate access to system components, and restrict physical access to cardholder data. This widget provides details on each of the compliance controls for the compliance family group being referenced. The compliance control reference number is followed by a count, and compliance result for the compliance control. The specific controls being referenced are: 8.3.1|8.2.2|7.2.1|8.2.3|7.2.2|8.4.3|8.2.1|8.3.4|8.2.8|8.2.6|8.4.1

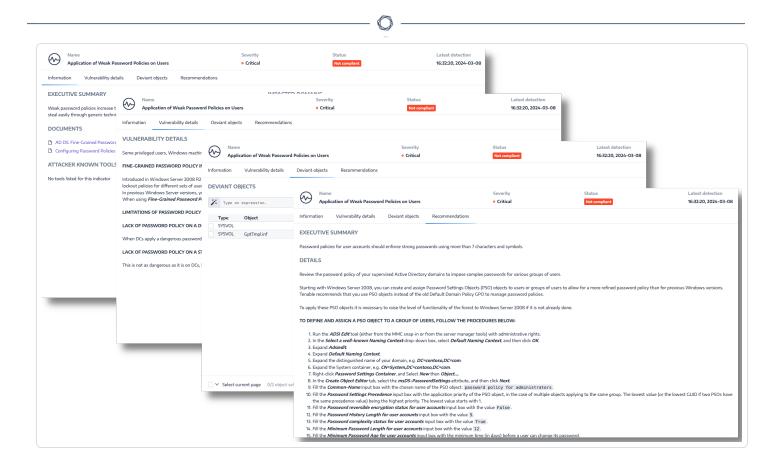
Tenable Identity Exposure measures security maturity of the AD infrastructure through Indicators of Exposure assigning severity levels to the flow of events that are being monitored and analyzed. Alerts are triggered when security regressions are detected. To view these indicators select the Indicators of Exposure icon from the navigation pane. All Indicators of Exposure can be displayed by toggling the Show all indicators to Yes, or a keyword can be typed into the search pane. In the following example indicators based on the keyword "password" are displayed.

 \bigcirc

Ind				()
	cators of Exposure			
h	A password			X Show all indicators
	Critical			*
	Application of Weak Password Policies on Users Some password policies applied on specific user accounts		_	
	are not strong enough and can lead to credentials theft.			
	▲ tenable.ad.local Complexity 🕥			
1	High			
	Potential Clear-Text Password	Account with Possible Empty Password	Detection of Password Weaknesses	
	Checks for objects containing potential clear-text passwords in attributes readable by domain users.	Identifies user accounts that allow empty passwords.	Verifies for weaknesses in passwords that may heighten the vulnerability of Active Directory accounts.	
	▲ tenable.ad.local Complexity 🔊	▲ tenable.ad.local Complexity 🕥	▲ tenable.ad.local Complexity の	
	Medium			
Į				
	Reversible Passwords Verifies that the option to store passwords in a reversible format does not get enabled.	Accounts With Never Expiring Passwords Checks for accounts with the DONT_EXPIRE_PASSWORD property flag in the userAccount Control attribute that allows indefinite use of the same password, bypassing password renewal policies.		
	▲ tenable.ad.local Complexity 🕥	▲ tenable.ad.local Complexity (

Selecting a result presents a series of details allowing the analyst to view:

- **Information** Which provides an executive summary, including known attack tools, affected domains, and relevant documentation.
- **Vulnerability Details** More in-depth information about the misconfiguration.
- **Deviant Objects** This information highlights misconfigurations in AD that may contribute to broader attacks.
- **Recommendations** Provides guidance on effective configuration strategies to minimize the attack surface.



Control Objective 5: Regularly Monitor and Test Networks

This includes monitoring all systems/network access and regularly testing systems security and processes. This control objectives covers the following PCI DSS requirements:

Requirement 10: Log and monitor all access to system components and cardholder data.

Requirement 11: Test security of systems and networks regularly.

PCI Requirements Under This Objective Supported by Tenable

Requirement 10: Log and monitor all access to system components and cardholder data

Audit logs are required which capture all individual user access to cardholder data. PCI DSS requirements highlight the criticality of having a process or system that links user access to system components accessed. Log mechanisms which record relevant events are an important component in detecting unauthorized access and potential breaches. Systems should have synchronized clocks to ensure that log entries are consistent and accurately reflect the timing of events.

By keeping logs and monitoring them, organizations not only meet regulatory compliance, they can quickly identify and respond to potential security incidents and breaches. In the event of a data breach, logs provide a crucial understanding of what happened, how the breach may have happened, and the impact of the breach. While Tenable does not directly collect and store system logs, there are several checks that assist organizations with this requirement.

The Regularly Monitor and Test Networks widget within the PCI-DSSv4.0 Audit Summary dashboard covers topics within PCI requirement 10 and 11.

	FAILED	PASSED	WARNING	SKIPPED
10.2.2	168	98	1	0
10.3.3	34	3	0	0
10.6.3	13	0	0	0
10.6.2	13	0	0	0
10.6.1	13	0	0	0
10.6	13	0	0	0
10.3.2	9	8	2	8

Both of these requirements cover tracking and monitoring all access to network resources and cardholder data, and the regular testing of security systems and processes. This widget provides details on each of the compliance controls for the compliance family group being referenced. The compliance control reference number is followed by a count, and compliance result for the compliance control. The specific controls being referenced are: 10.2.2 | 10.6.2 | 11.5.2 | 10.2.1 | 10.6.1 | 10.2.1.7 | 10.2.1.5 | 10.3.2 | 10.2.1.2 | 10.4.1.1 | 10.6.3 | 10.2.1.4 | 10.6 | 10.5.1 | 10.2.1.1 | 10.2.1.3 | 10.3.3 | 10.2.1.6

Requirement 11: Test Security of Systems and Networks Regularly

PCI DSS requires that vulnerabilities are identified and assigned a risk ranking based on industry best practices and consideration of potential impact. Continuous vulnerability scanning is essential for maintaining a robust security posture, adapting to changes, ensuring compliance, and effectively managing and mitigating risks.

Tenable assigns an Asset Criticality Rating (ACR) to each asset based on indicators of business value and criticality. ACR is based on several key metrics such as business purpose, asset type,

location, connectivity, capabilities, and third-party data. An ACR score is a range from 0-10. Low scores are not considered to be business critical, and high scores represent the organizations most critical, and have a greater business impact if compromised. Organizations that are also Tenable Lumin customers have the ability to adjust the default Tenable ACR value to more accurately reflect organizational risk.

Not all vulnerabilities pose the same risk. By combining ACR and VPR, prioritization efforts focus on the most critical vulnerabilities first.

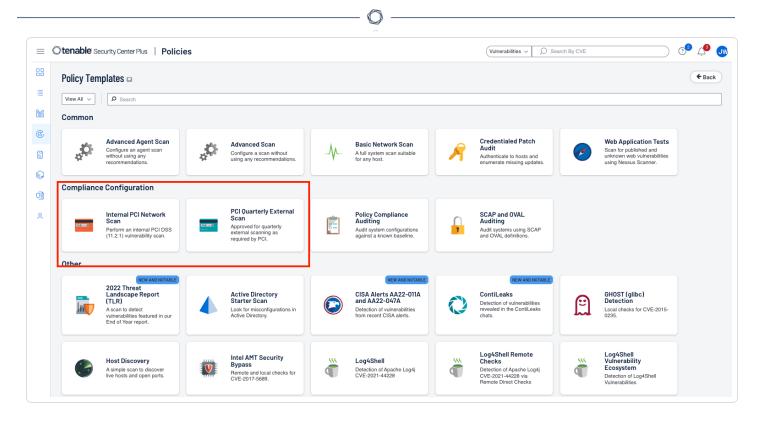
Organizations may also utilize CVSS and Severity ratings for risk prioritization. For more information on prioritization of vulnerabilities <u>reference this document</u>.

For additional scanning under Requirement 11 organizations should utilize the pre-configured Nessus scan templates, available in Nessus, Tenable Security Center, and Tenable Vulnerability Management. These PCI scan templates allow organizations to get started quickly, with minimal configuration, however they can not be edited. When these scans are completed they can be submitted to Tenable's ASV Engineers for review. To maintain a set continuous scanning schedule, Nessus scans can be easily automated to run at specific times/days.

More information on this process can be found here: <u>Submitting Scans for PCI ASV Validation</u>.

As a PCI Approved Scanning Vendor (ASV), Tenable offers two built-in scan policies designed for PCI scanning: 'PCI Quarterly External Scan' and 'Internal PCI Network Scan'. While only the 'PCI Quarterly External' policy is valid for official attestation, both policies can be used anytime for organizational scanning purposes. For official attestation, the PCI ASV add-on is required. The two policies differ in terms of settings and plugins included- the 'External' policy is designed for an 'outside-in' perspective of the target vector and therefore only executes remote checks, while the 'Internal' policy is better suited for scanning various connected devices within an organization's network.

Mandatory Requirement: PCI Requirement 11.3.1 requires that vulnerability scans be conducted at least once every three months, and that high risk and critical vulnerabilities are resolved. Rescans are to be conducted to verify that any identified high risk and critical vulnerabilities have been resolved. Tenable's PCI Scan policies assist organizations in meeting this requirement.



As the official External policy is approved and designed specifically in accordance with the specifications set forth by the PCI Security Standards Council, there is little customization possible with it- users are limited to adjusting the scan's performance settings to allow for proper analysis per the network's capabilities. No other customization to the External policy is permitted. The Internal policy, however, allows users to control the scan's Discovery, Assessment, Report, and Advanced settings, although plugins are not modifiable. Additionally, the Internal policy allows for the input of credentials to enable the local checks included in the scan's configuration.

A comparison between the two policies (default settings)

Setting	Internal	External
Use fast network discovery	enabled	disabled
Override firewall detection (for TCP port scanner)	automatic	soft
Credentialed access (local checks possible)	yes	no
Only use NTMLv2	yes	no
Paranoia level (Override normal accuracy)	normal	high

	<u></u>	
Perform thorough tests (slow)	disabled	enabled
CGI scanning	disabled	disabled
Only use credentials provided by the user	enabled	disabled
Elevate privileges	disabled	enabled
Test default accounts (slow)	disabled	enabled
Check for PCI DSS compliance	yes	yes
Enable Web Application tests	no	yes
Max simultaneous hosts per scan	30	20
Network timeout	5	15
Port scan range	default	1-65535

While the policies differ in terms of their various settings, the main idea for the external scan is that the policy demonstrates the publicly-visible attack vector currently present in the environment. The policy is meant to show what an attacker may be able to leverage from the external perspective, with the understanding that they would not be privy to valid authentication methods.

The settings that tend to make the biggest difference in the outcome of the two policies are the ability to authenticate with the Internal PCI policy and the increased paranoia in the External PCI policy. Use of credentials for the internal scan policy is preferred. Valid credentials allow the Internal policy to utilize a variety of local plugins, including the enumeration of missing patches. The increased paranoia of the External policy may result in some plugins reporting a vulnerability with lower confidence that would otherwise not be reported. Another key difference between the Internal and External PCI policies is how the port scanners operate. Especially if the Internal policy is provided with target credentials, the port scanner can enumerate the services running on the data plane, whereas the External policy will enumerate exposed ports, and can potentially enumerate the services running on the control plane.

Tenable Web App Scanning

Tenable Web Application Scanning contains a built-in PCI scan template. The PCI ASV Scan is a scan that assesses web applications for compliance with Payment Card Industry Data Security Standards (PCI DSS) for Tenable PCI ASV. (This scan also allows you to view and edit the Request

Redirect Limit. The default value for this limit is 3.) This scan template helps organizations who are using web servers or APIs meet the requirements for PCI 11.3.2.

Ø

© tenable Web App Scanning ©		
ŵ		
Scans > Scan Template:	Create Scan Template 🗆 🛛 🗙	Create Scan Template
Scan Served Filters v En	Creater Scan Templac Creater Scan Templac Creater Scan Creater Scan Templac Creater Scan Creater Scan Templac Creater Scan Creater Scan Creater Scan Templac Creater Scan Templac Creater Scan Templac	Create Scan Template
	Cancel Save Template	

Control Objective 6: Maintain an Information Security Policy

This includes maintaining a policy that addresses information security policies and procedures. PCI DSS Requirement 12 resides within this control objective. Requirement 12 ensures that organizations handling cardholder data have clear security policies in place, which are communicated, enforced, and updated on a regular basis. In addition to the establishing, publishing and maintaining of security policies, other Items that are evaluated in this requirement are employee training and awareness, are information security responsibilities.

By enforcing these requirements organizations ensure that security policies are in place but also actively maintained, communicated, and followed, reducing the risk of security incidents.

This control objectives covers the following PCI DSS requirements:

Requirement 12: Support information security with organizational policies and programs.

PCI Requirement 12.5.1 mandates that organizations have an inventory of system components that are in scope for PCI DSS. Maintaining a current list of all systems enables organizations to define which assets are in scope for PCI DSS. Recommended methods of maintaining the inventory list include databases, files, or inventory management tools.

PCI Requirements Under This Objective Supported by Tenable

As listed in PCI Requirement 12.5.1, a good practice is to keep an inventory of all assets. Those systems that are in scope for PCI DSS should be clearly identifiable among those assets.

Tenable products allow assets that have been identified to be tagged. Organizations can use tags to label assets, policies, credentials, or queries with a custom descriptor to improve filtering and object management. For example, you could add a tag named PCI DSS to label all of the assets that are in scope for PCI. Tenable Attack Surface Management continuously maps the Internet and discovers connections to your Internet-facing assets, whether internal or external to your networks, allowing organizations to discover unauthorized or unknown devices.

For more information regarding tagging assets reference these documents:

- Tenable Security Center
- Tenable Vulnerability Management
- Tenable Attack Surface Management

References

- PCI Security Standards Council
- <u>PCI DSS Prioritized Approach to PCI Compliance</u>
- PCI DSS v4.0 Quick Reference Guide
- PCI DSS Summary of Changes from v4.0 to 4.0.1
- PCI DSS Summary of Changes from PCI DSS v3.2.1 to 4.0

O