



# ADDRESSING PCI DSS WITH TENABLE.IO

#### PCI COMPLIANCE

Because payment card information is one of the most appealing theft targets for attackers, protecting payment card transactions and cardholder data (CHD) is critical. A breach of cardholder data affects the entire payment card ecosystem. Merchants, processors, acquirers, issuers and service providers lose credibility – and in turn lose business – and are also subject to financial liabilities. More importantly, customers may lose trust in merchants or financial institutions.

# INTERNAL VULNERABILITY SCANNING

PCI DSS 6.1 requires you to establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk rating to newly discovered vulnerabilities. Additionally, PCI DSS 11.2.1 requires you to perform quarterly internal vulnerability scans.

Tenable.io Vulnerability Management is continually updated with the latest vulnerability information and quickly scans your cardholder data environment for known vulnerabilities. Tenable.io VM uses CVSS scoring to rate vulnerability risk so you can identify those that are "high-risk" and prioritize remediation accordingly. Additionally, it can re-scan your environment to help you confirm vulnerabilities were resolved per your policy.

Trical and High Exploit	table Vunerabilities										
968 Explored by Milliagre		370 Nerrotely Explorable and LD	w Complexity	308 Locally Exploitable and Low Com	skety	374 Explored to	y Franciscon		1081	Wable and High Co	implexy
future Threats: Not Yet	Exploitable Vulnera	icitties.		10	verability Age	Managing S	iLAs				
	CARADUSTY POSISION	INTERNET POLICIES AND THE DAYS AGO	ENVELTY PUBLISHED IN Th 193 GRITIAGO	NAME AND ADDRESS AND ADDRESS ADDRE		in-1075.	61-98 (MPS	n-witers	0.004/5	011005	17245
Road of Galogie Septem				1126	Critical Physics	1007	-	-			
Improve Septer.		-		1942	libellari Los		-	844 162	(H) (H)		
							Scan Cr	werage			
								-		ast 90 Days	
17ĸ	1.00000	1.5ĸ	List? bys	2.2ĸ	3995 64	iesti		456		5% Authentic 19% Unauther	



# EXTERNAL VULNERABILITY SCANNING

PCI DSS 11.2.2 requires that an Approved Scanning Vendor (ASV) performs quarterly external vulnerability scans.

Tenable.io PCI ASV, an add-on to Tenable.io VM, streamlines the quarterly external vulnerability scan submission and dispute resolution process. With pre-configured scan templates and an efficient process, you can quickly run scans, submit attestation requests and resolve disputes.

Videostilios	PCI ASV Attestation Requests						
<ul> <li>Assets</li> <li>Health &amp; Datus</li> </ul>	Remediation (5) ASV Review 4 Atventation	e 10					
E PCIASV &	C Naria	Durier	Assets	Falues	Last Modified -		
	🗇 gap scar 3	koolum@po-twit.com	3 63	65 (5)	Today at 1:11 PM		
<ul> <li>My Dashboarth</li> <li>Exploitable by Mel</li> </ul>	GAP POI Som	Hasher@psi-bed.com	3 63	01.071	June 22 al 1.12 PM		
	📋 AK - Scar20	chear#pci-text.com	2.63	38 (28)	June 22 at 9-34 AM	11	
	😄 PO 1687	covillamo@pointest.com	36	65 (62)	Today at 10:49 AM		
	Main's PCI scan	musicmavv@pci-tast.com	2.65	45 (40)	June 22 at 9:29 AM		
	O Nell	cavillams@pci-text.com	36	85 (64)	June 22 at 6:52 AM		
	Server 1 POI Scan	Nuclear@pci-text.com	16	20 (77)	June 21 at 9:17 PM	17	
	D PO Text 8	sawliana@pci test.com	3.63	44,000	June 20 at 12:49 PM		
	💠 PO TEST	cexillians@ccitest.com	2 63	A7 (47)	June 20 at 12:40 PM		
	PO Set 2	cavillame@pci-test.com	36	41 (41)	June 20 at 12-69 PM		
	POIDSON	cexilitians@pci-text.com	3 45	45 (61)	June 20 at 12:48 PM		
	Stan Importing 2		° 63	0.03	NA		
	Scan importing 3		0.03	0.00	NA		



#### **KEY BENEFITS**

- Security, not just compliance PCI compliance is critical, but realistically, it probably is not your entire job. More likely, it is only one of your many challenges. You have plenty of other servers, endpoints, and network devices to protect – not to mention cloud assets and possible operational technology assets. Tenable's PCI solution is part of the Tenable.io cyber exposure platform that helps you secure all of your assets, including those in scope for PCI.
- **Operations made easy** You need to focus on security, not on administering security tools. Tenable.io, a cloud-based solution, lightens your load. It is maintained by Tenable, and it comes with our 99.9% uptime Service Level Agreement.
- Future Growth Do not get stuck at a dead end with a solution that won't grow with you.
   Tenable.io supports modern assets, such as cloud, mobile, containers, and operational technology. It also will support your needs for scalability and integrating with your other security tools.

COPYRIGHT 2018 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE, TENABLE.IO, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.





### **CONFIGURATION COMPLIANCE**

PCI DSS 2.2 requires that you develop configuration standards for all system components. Cardholder Data Environment system components may include in-scope servers, endpoints, firewalls, routers, and databases. The configuration standards for Cardholder Data Environment components may be based on industry-accepted hardening standards, such as Center for Internet Security (CIS) benchmarks.

Tenable.io<sup>™</sup> Vulnerability Management includes configuration audit policies for all popular versions of servers, endpoints, firewalls, routers, and databases so you can audit configuration standard compliance. For example, you can determine if anti-virus is installed and set to be active on boot, if only necessary services and protocols are enabled, and if all system clocks are using time-synchronization technology.

nable 🚳	Warrabily Management - Emblement Scame Reports Serings	New Jointur Advector	Construction of the Constr	٠
No france in the	Office - CIS. Compliance Scan - Windows 10		Audit Topi	6ert 1
Alden Test	Audio II Versitation + Audio III Hony II			O Nov Detail
	(Line Color			_
Policies E Target Orman	131	23		
	NGD	aatest	NUED	
	Nare -		family	Cove
	CEL-42073-TLSV-T78ETL2_LLB The Enterced Mitigation Equations Toolist (EMET) upter	m-vole Data Execution Preventor (SRP) must be enabled and configured to at least Application Opt Out ZPVIC Target	L. SCAP Winters Compliance Checks	-1
	CEL-42187-5.52-77905-2_via The Totacced Mitigation Experience Taskit (DMT) symmetry	T. SCAP Writtees Compliance Decks	1	
	CCE-42238-6.0V-7793542,vie/The Interced Mitigation Experience Tools8 (IMRT) Deliv	SCAP Western Compliance Decks	1	
	CCE-42228-8:dV-7792362_vule The Enhanced Mitigation Expension Toolist (SHET) Deliv	5048 Westses Compliance Deoks	1	
	CCL 42970-4:07-7EDB(C_ruleThe built-in administrator account result be remained 2PM	SCAP Writisks Compliance Dipola	1	
	CCE 400% 5-07 TELESC, we The built in guest scould must be revened DPVS Targe	SCAR Western Compliance Checks	1	
	COF-48015-3-69-68003-1_vale/Windows 10 must be configured to acath Digest Access	SCAP Writtens Compliance Checks	1	
	CG-48005-3-07-49005-1, use Windows 10 must be configured to avail Digest Access	Other Object Access Sorris auconses DP445 Target Windows 32	SCAP Winters Campliance Checks	1
	CCI-50123-8-02-48305-1, use Windows 10 must be configured to audit Direct Access	File Share sustained.DPMS Target Windows 10	SCAP Weatows Compliance Checks	1
	• LEE-SELES-IN-SV-BETELS_V-METHODORE 10 must be composed to suit Object Access	SCAF Wintows Compliance Checks	11	
	N-17812/1_value/wes must be prevented from changing installation options.09MI Targ	at Wednes 18	SCAP Western Compliance Decks	11
	SV-775251_valeThe Illindone Installer Always install with situated privileges must be di	1CAP Weddes Compliance Deels	- 11	
	19-7782312 sub-Automatically storing in the last interaction spar after a solary-extrated	netert must be dealtied CPMS Terest Windows 10	SCAF Windows Constitution Checks	

Scan web applications in your cardholder data environment

#### WEB APPLICATION SCANNING

If your cardholder data environment includes public-facing web applications, PCI DSS 6.6 requires you to address new threats and vulnerabilities to ensure these applications are protected against known attacks.

Tenable.io Web Application Scanning delivers safe and automated vulnerability scanning for your in-scope web applications. It helps you identify and address the specific vulnerability types included in Requirement 6.5 so you can rapidly assess your web applications without heavy manual effort. Tenable.io Web Application Scanning provides high detection rates with minimal false positives, ensuring you understand the true risks in your web applications.

For More Information: Please visit tenable.com Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact

nable 🎯 🕠	Web Applications - Dashboarth Scene Prep	orts Settings New Interface		🛛 🌲 Ted Gay (
Valueshilles	Web Applications			Last 30 Gays 👻
Assets     Web Applications	By Plugin By Application			
Wy Dechboards	0		61	
Dashboard Templates				
Deputive Summary	DETCK	HER	NEEM	1211
Exploitable by Mal	VALNESHBLIPES OVER THE		CHANGE TOP LO 2017	
Exploitable Frame.	-		New .	Count
Nezzuring Volkera			di-Interior	
Mitgation Summary	-		A2-Boker Authentication	1
Outstanding Reme			AD-Sensitive Data Exposure	18
Prioritize-Assets Security-Managem			July 3344, External Erst Ken (2018)	
Spectre & Weltdown			45-Broken Access Control	83
When thilling by C.	20		A6-Security Misconfiguration	63
Vulnerability Mana	-		A7-Cross-Site Scripting (155)	11
Vulnerability Mana.			All-Insecure Deservation	•
Web Services	-		AB-Using Components with Known Vulnerabilities	0
M WHO SERVER			ALD-braufficient Logging & Monitoring	
			4	
	TOTAL RUSSING 34			TOTAL COUNT 48
	Sev - Name		Family -	Count
	Cross-Site Scripting (HSS) in HTML tag		Cross Site Scripting	1
	Cross Site Scripting (155)		Cress Site Scripting	1
	Cross-Site Scripting (HSS) in path		Cross Site Scripting	6
	DOM-based Cross-Site Scripting (ISS)		Cross Site Scripting	2
	<ul> <li>Cross-Site Scripting (555) in event tag of HTML element</li> </ul>		Cross Site Scripting	

Identify misconfigurations with compliance scans

# TENABLE.IO – A MODERN VULNERABILITY PLATFORM

Built on the leading Nessus® technology, Tenable.io™ brings clarity to your security and compliance posture through a fresh, asset-based approach that accurately tracks your resources and vulnerabilities, while accommodating dynamic assets like cloud and containers. Tenable.io maximizes visibility and insight and effectively prioritizes your vulnerabilities, while seamlessly integrating into your environment.

The platform includes unlimited Nessus data sensors for active and agent-based scanning and passive traffic listening. In addition, Tenable.io includes an API and SDK for those who want to automate the sharing of Tenable.io capabilities and vulnerability data, or build on the Tenable.io platform. Built on the Tenable.io platform are a growing number of applications that solve today's toughest security challenges, including vulnerability management, container security and web application scanning – making it easy to start with one application and upgrade to others as requirements grow. This combination of applications, data sensors and automation provides maximum coverage and continuous visibility into assets and vulnerabilities – so you can take better-informed action to protect what matters most.

#### TRAINING

Tenable offers training for those who are new to using Tenable.io and want the knowledge and skills to maximize use of the product, as well as advanced topics for seasoned users. Courses are available on-demand via www.Tenable.com

COPYRIGHT 2018 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE, TENABLE.IO, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS. 2