praetorian

eBook

Continuous Threat Exposure Management (CTEM) and PCI DSS 4.0.1 Compliance

Leveraging CTEM to Meet the Latest PCI DSS Requirements

Get Started ›

Inside this eBook

Introduction

The Payment Card Industry (PCI) Data Security Standard (DSS) provides a baseline of technical and operational requirements to ensure organizations meet consistent data security measures. Release in June 2024, the DSS v4.0.1 contains twelve high-level categories of security controls, each with a set of accompanying requirements.

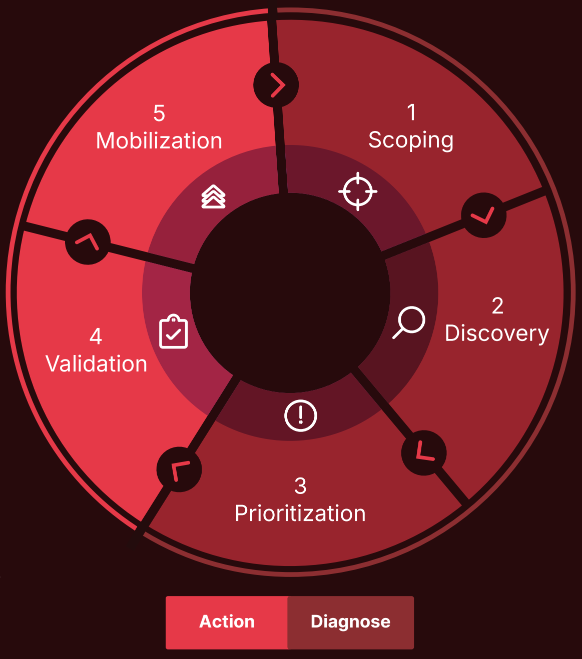
Continuous Threat Exposure Management (CTEM) is an emerging security testing framework that offers a proactive approach to cybersecurity suited to modern enterprises. This eBook outlines how organizations looking to implement a CTEM program can meet DSS 4.0.1 requirements.

Before diving into the regulation, we first present a definition of CTEM: “A program that continuously detects and eliminates cyber risks by leveraging automated technology with scalable processes and engaging stakeholders across the organization”.

CTEM shifts focus away from point-in-time assessments and toward continuous testing. When implemented correctly, CTEM enables organizations to know with certainty if their defenses will protect them against emerging threats.

Gartner proposed a five-step cycle to describe an effective CTEM program. At a high level, this cycle includes the following phases:

1. **Scoping:** Determine what the testing program is responsible for.
2. **Discovery:** Detect risks in scoped assets.
3. **Prioritization:** Order detected risks by impact to the organization
4. **Validation:** Determine which detected risks pose a genuine threat.
5. **Mobilization:** Address valid risks and improve higher-level security posture.



While organizations do not need to follow Gartner's framework verbatim, it is a useful starting description of a continuous security program.

We recommend reading Continuous Threat Exposure Management: A Blueprint to Modern Cybersecurity Testing or further Gartner resources [1,2], before continuing.

We now discuss which DSS requirements CTEM can help organizations reach.

Key Requirements and CTEM Alignment

PCI DSS Requirement ID	Description	Can CTEM Help?
1	Install and Maintain Network Security Controls	✓
2	Apply Secure Configurations to All System Components	✓
5	Protect All Systems and Networks from Malicious Software	✓
6	Develop and Maintain Secure Systems and Software	✓
8	Identify Users and Authenticate Access to System Components	✓
10	Log and Monitor All Access to System Components and Cardholder Data	✓
11	Test Security of Systems and Networks Regularly	✓
12	Support Information Security with Organizational Policies and Programs	✓

[1] https://www.gartner.com/en/documents/4922031
[2] https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes

Requirement 1

Install and Maintain Network Security Controls

DSS Requirement 1 requires organizations to store all cardholder data in a restricted environment. Organizations must ensure their cardholder network is not publicly accessible to the internet or untrusted computer networks and control network access in and out of the environment.

Cardholder environments are perhaps the first assets organizations should scope for their CTEM program. To meet DSS Requirement 1, organizations should include test cases to probe the cardholder network from various untrusted locations and as various unauthorized users. The program should run these test cases regularly, notifying administrators immediately if it detects an unauthorized path into the cardholder network.

Requirement 2

Apply Secure Configurations to All System Components

DSS Requirement 2 specifies that organizations must have processes to securely configure and manage all systems and environments.

While managing and applying configuration changes is outside the scope of a cybersecurity testing program, CTEM can help organizations map out their systems and environments. During the Discovery phase, organizations continuously search for computer systems, cloud components, source code repositories, SaaS deployments, and other attack surfaces that provide an avenue into their environment. Recently, organizations have achieved this with Attack Surface Management solutions, which fit neatly into the CTEM framework.

Requirement 5

Protect All Systems and Networks from Malicious Software

This requirement ensures that organizations implement defensive controls that properly prevent the installation and spread of malware on all systems and networks.

CTEM can help organizations determine if their Requirement 5 controls are effective. During the Scoping phase, organizations

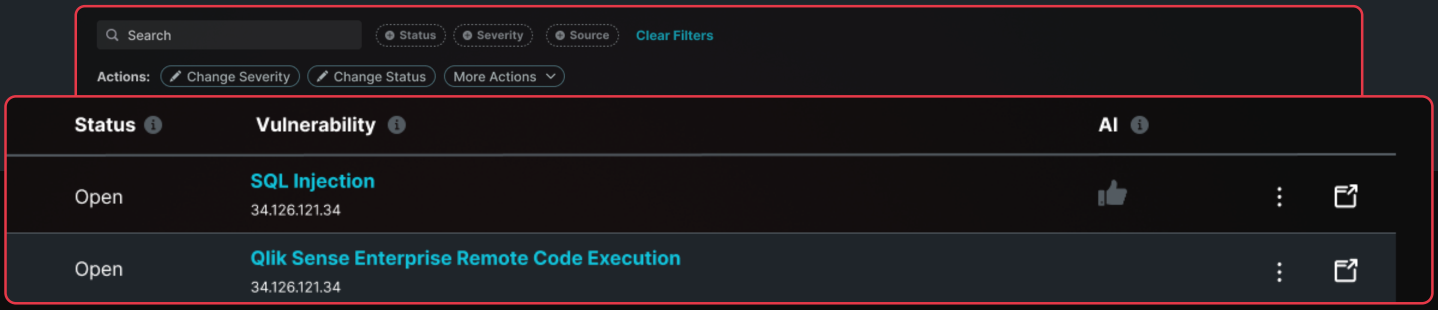
should include test cases for attack simulations that run various ransomware, rootkits, and other malware on a representative subset of endpoints. Including such test cases will enable organizations to test the controls specified in Requirement 5, giving them confidence in their efficacy.

Requirement 6

Develop and Maintain Secure Systems and Software

Developing and maintaining secure systems means that organizations must effectively identify and remediate known security vulnerabilities, design custom software securely, and protect public-facing web applications.

CTEM's primarily goal is to discovery and eliminate cyber risks. CTEM relies on vulnerability scanners, penetration tests, and other solutions to generate risk alerts. CTEM then builds prioritization and validation processes around these technologies to efficiently handle the alerts. To maintain DSS compliance, organizations simply need to direct this detection pipeline at all PCI-relevant systems.



Status	Vulnerability	AI
Open	SQL Injection 34.126.121.34	👍
Open	Qlik Sense Enterprise Remote Code Execution 34.126.121.34	

Requirement 8

Identify Users and Authenticate Access to System Components

Requirement 8 ensures authentication is enforced consistently throughout the organization. All sensitive applications must enforce traditional authentication and multi-factor authentication (MFA).

CTEM can help organizations to test their authentication mechanisms by simulating unauthenticated accesses to scoped assets. Organizations should include test cases that regularly attempt unauthenticated network requests to sensitive applications, logins with weak credentials, single-factor authentications (where MFA is implemented), and similar tests. Such a program will alert the organization as soon as a configuration occurs that results in an unauthenticated breach.

Requirement 10

Log and Monitor All Access to System Components and Cardholder Data

Requirement 10 dictates that compliant organizations must log and monitor all user actions in system components and on cardholder data. Organizations traditionally use a SIEM or similar solution to aggregate all logs and write rules to alert administrators when malicious or suspicious actions are detected.

CTEM ensures that such rules work properly. If an organization's first lines of defense fail, and a security breach occurs, the organization must have confidence that it can immediately detect and act on the breach. Therefore, when designing test cases, organizations must regularly simulate suspicious alerts. If a simulation runs and the accompanying alert fails to trigger, the organization must investigate to determine why.

Manual
Testing
CTEM
Automated
Testing

Requirement 11

Test Security of Systems and Networks Regularly

Requirement 11 ensures organizations regularly perform security assessments against their environments. This section primarily emphasis manual testing, such as penetration testing or red teaming exercises.

Manual testing has a large role to play in a CTEM program. Just because CTEM stresses continuous testing does not mean that all testing must be automated. Organizations should include manual assessments to cover test cases that are too complicated or difficult to automate, or to target especially high-priority assets. By including manual assessments in the scope of their CTEM programs, organizations will meet Requirement 11 items related to security assessments.

Requirement 12

Support Information Security with Organizational Policies and Programs

Among other things, Requirement 12 covers risk assessment and cybersecurity training. Organizations must regularly evaluate their environment of risk from novel cybersecurity threats and train their employees to handle security risks.

When performing scoping, organizations should include a threat modeling exercise to enumerate potential risks to the business. Organizations should use their threat model to inform asset and test case selection. To meet the training needs of this requirement, organizations must simulate risks against employees, particularly social engineering campaigns like phishing or vishing (voice-phishing).

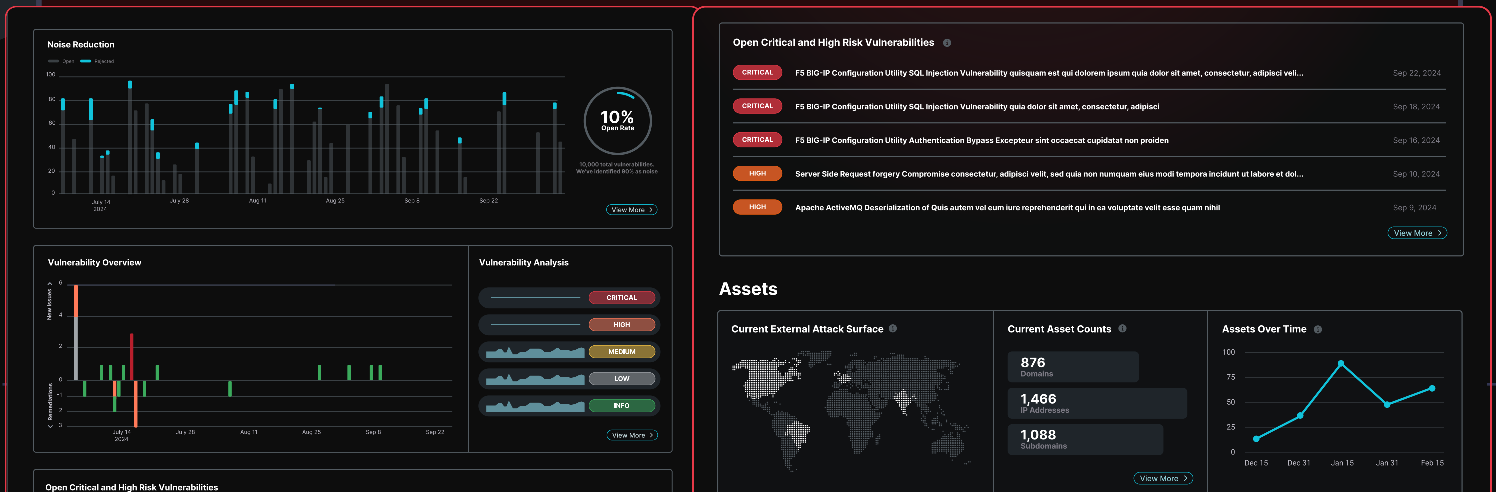
Conclusion

CTEM shifts focus away from point-in-time assessments and toward continuous testing. Additionally, it spreads the responsibilities of security posture across the broader organization to ensure alignment on security objectives throughout the business. By integrating CTEM into their cybersecurity strategy, organizations can effectively meet PCI DSS 4.0.1 requirements. This approach helps organizations stay ahead of evolving threats while meeting stringent regulatory standards.

CTEM with Praetorian Guard

If you believe your organization would benefit from a Continuous Threat Exposure Management program but aren't sure where to start, Praetorian's got you covered. Our Praetorian platform provides all the above technological capabilities out of the box, and our professional services can help with the rest.

Contact Praetorian | Start Free Trial



Noise Reduction

10% Open Rate

10,000 total vulnerabilities. We've identified 90% as noise

Vulnerability Overview

Vulnerability Analysis

Open Critical and High Risk Vulnerabilities

CRITICAL F5 BIG-IP Configuration Utility SQL Injection Vulnerability quisquam est qui dolorem ipsum quia dolor sit amet, consectetur, adipisci veli... Sep 22, 2024

CRITICAL F5 BIG-IP Configuration Utility SQL Injection Vulnerability quia dolor sit amet, consectetur, adipisci Sep 18, 2024

CRITICAL F5 BIG-IP Configuration Utility Authentication Bypass Excepteur sint occaecat cupidatat non proiden Sep 16, 2024

HIGH Server Side Request forgery Compromise consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dol... Sep 10, 2024

HIGH Apache ActiveMQ Deserialization of Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil Sep 9, 2024

Assets

Current External Attack Surface

Current Asset Counts

876 Domains

1,466 IP Addresses

1,088 Subdomains

Assets Over Time