praetorian

eBook

Continuous Threat Exposure Management (CTEM) and NYDFS Compliance

Leveraging CTEM to Meet Enhanced NYDFS Cybersecurity Requirements

Get Started ›

Copyright Praetorian Security. All Rights Reserved.

Inside this eBook

Introduction

Vulnerability Management (Section 500.5)

Risk Assessment (Section 500.9)

Asset Management (Section 500.13(a))

Training (Section 500.14(a)(3))

Conclusion

Introduction

The recent amendments to the New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR Part 500) introduced significant changes, particularly to vulnerability management, risk assessment, and incident response. This eBook explains how Continuous Threat Exposure Management (CTEM) can help organizations satisfy these enhanced requirements through a proactive and comprehensive approach to cybersecurity.

Before diving into the regulation, we first present a definition of CTEM: *"A process that continuously tests an organization's infrastructure for cyber risks, effectively triages and remediates these risks, and self-improves over time."*

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

1. **Scoping:** Decide which assets and entry points are in scope for testing.
2. **Discovery:** Map scoped assets to live systems and scan detected systems for risks.
3. **Prioritization:** Order detected risks by estimated impact on the organization.
4. **Validation:** Determine which risks pose a genuine threat to the organization.
5. **Mobilization:** Remediate valid risks and improve higher-level security posture.

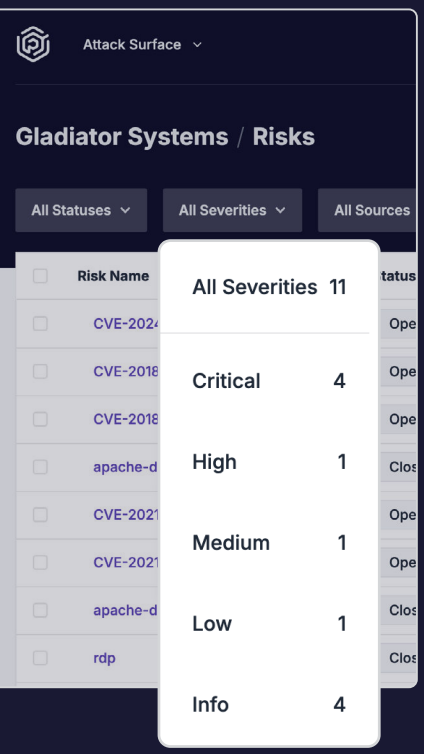
We recommend reading Gartner's CTEM resources[1,2], for more information.

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

Copyright Praetorian Security. All Rights Reserved.

While organizations do not necessarily need to follow Gartner's framework verbatim, the crucial element of CTEM is "continuous". It steps away from traditional point-in-time testing and instead relies on well-known technologies and techniques (such as attack surface management, vulnerability scanning, breach and attack simulation, cyber threat intelligence, and penetration testing) to ceaselessly hunt for gaps in defensive capabilities. When addressing a confirmed risk, a good CTEM program not only remediates the specific instance of the risk but also takes action to prevent the risk from recurring in the future. This allows organizations to improve security posture over time instead of merely keeping pace with vulnerability alerts.

Put simply, CTEM uses the most effective technologies at its disposal to continuously find risks and thoroughly address them. We now discuss how this program can meet NYDFS compliance.



Key Requirements and CTEM Alignment

Vulnerability Management (Section 500.5)

The NYDFS amendments require covered entities to implement robust vulnerability management policies and procedures. Key requirements include:

Annual Penetration Testing: Conduct penetration tests from both inside and outside the information systems' boundaries by a qualified internal or external party.

Automated Scans and Manual Reviews: Perform automated vulnerability scans of information systems regularly, supplemented by manual reviews for systems not covered by automated scans.

Prompt Alerts for New Security Vulnerabilities: Establish a process to monitor novel vulnerabilities and attack techniques.

Timely Remediation: All identified vulnerabilities must be remediated promptly, with prioritization based on the risk they pose to the entity.

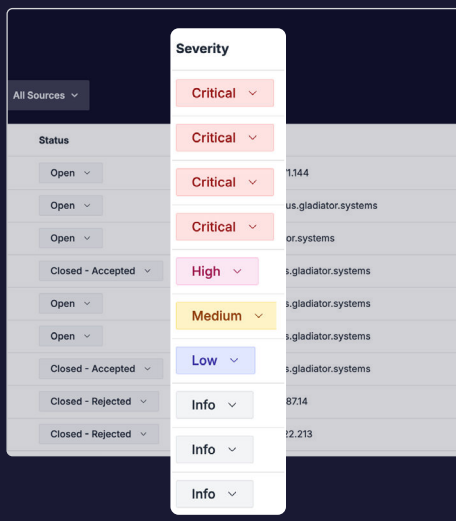
In an effective CTEM program, organizations move away from point-in-time assessments and toward continuous testing. Security professionals conduct regular testing against attack paths prioritized by impact. Because CTEM focuses manual efforts on a smaller set of higher-impact attacks, teams can afford to conduct frequent testing against the selected attacks.

Copyright Praetorian Security. All Rights Reserved.

To ensure that lower-impact attack paths do not remain unaddressed, CTEM programs rely on a pipeline of automated scanning tools to provide coverage over all assets in the organization. When the organization's threat intelligence learns about a new threat, the team builds a new capability to detect the threat and adds the capability to the pipeline.

Finally, CTEM mobilization ensures that identified risks are handled by the appropriate stakeholders for remediation and that stakeholders implement any higher-level recommendations. This improves the organization's security posture over time, allowing it to escape the scan-detect-patch cycle.

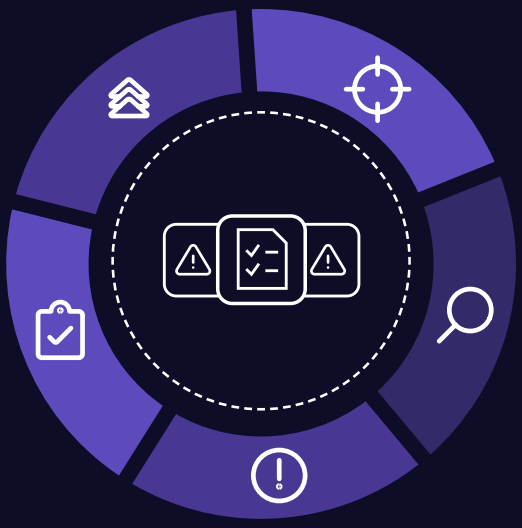
Collectively, these factors satisfy the requirements in Section 500.5.



Risk Assessment (Section 500.9)

Section 500.9 mandates that organizations periodically conduct risk assessments and update their risk assessment at least annually, or whenever significant changes in business or technology occur. The updated definition of risk assessment ensures organizations have a well-documented plan for evaluating exposure to cyber threats and an iteration cycle to build and improve on their plan. Specifically, Section 500.9 requires the risk assessment to include:

- Criteria to evaluate and categorize identified risks
- Criteria to assess each risk's impact to confidentiality, integrity, security, and availability of impact systems and data, taking into consideration any mitigating controls
- Requirements for mitigating or accepting identified risks.



Gartner's five-step cycle describes a continuous process. CTEM programs allow organizations to test their security controls and assess their risk constantly – not just quarterly or annually. In an effective CTEM program, security professionals conduct threat modeling exercises to determine the attack paths that pose the greatest greatest risk to their organization. The team uses the results of their risk assessments to direct security resources to the highest-risk areas of the organization.

Copyright Praetorian Security. All Rights Reserved.

Another important difference between CTEM and legacy security testing is mobilization. Effective mobilization doesn't just patch individual risks. Rather, mobilization consists of a process that facilitates the adoption of higher-level recommendations. This process should also record all findings in a central database, enabling organizations to take a data-driven approach to risk management and allocate future security resources accordingly. Mobilization is what empowers organizations to improve security posture over time, rather than merely react to immediate threats.

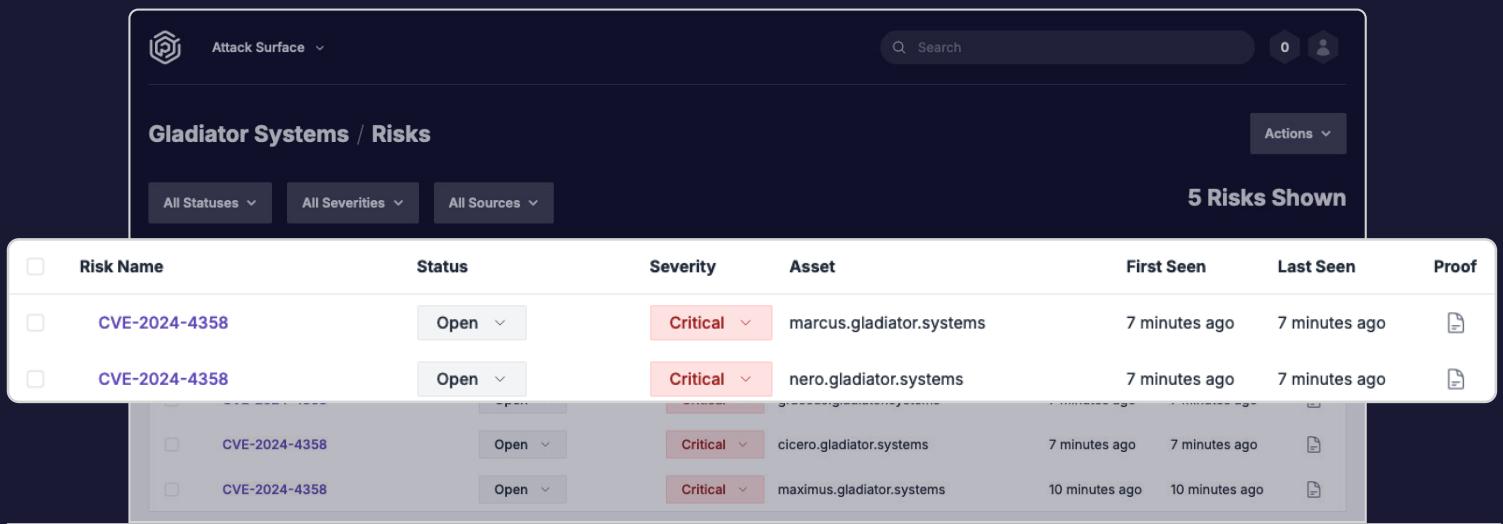
A well-architected CTEM program will satisfy NYDFS Section 500.9.

Asset Management (Section 500.13(a))

ASM solutions continuously monitor and map the organization's digital footprint, resulting in an accurate asset database that changes with the organization.

Covered entities must implement policies and procedures to maintain a complete and accurate asset management inventory of their information systems. This includes tracking key information such as asset owner, location, classification, support expiration date, and recovery time objectives, with regular updates and validations.

CTEM requires a robust asset discovery process, often powered by an attack surface management (ASM) solution, to continuously monitor and map the organization's digital footprint into a "living" database. Most ASM solutions use well-known techniques such as TLS mining, subdomain enumeration, WHOIS lookups, and port scanning to identify external-facing assets. Industry-leading ASM solutions also integrate with cloud providers, DNS management platforms, source code managers, and other third parties to identify additional assets in SaaS and cloud environments. The resulting inventory meets the above requirement.



Copyright Praetorian Security. All Rights Reserved.

Training (Section 500.14(a)(3))

The regulation specifies that security training must occur at least annually and include social engineering.

CTEM can include regular simulations for social engineering, internal breaches, and other real-time risks. Programs may achieve this with a traditional red team or with automated solutions. As a continuous process, the goal should be to constantly test employees against various cyber threats to build up their habitual resistance and awareness of cyber threats. This training ensures compliance with Section 500.14(a)(3) requirements and enhances the organization's overall security posture.

Conclusion

By integrating CTEM into their cybersecurity strategy, organizations can effectively meet the enhanced requirements of the NYDFS Cybersecurity Regulation. CTEM not only ensures compliance through continuous monitoring and proactive risk management but also enhances overall security resilience. This strategic approach helps organizations stay ahead of evolving threats while adhering to stringent regulatory standards.

CTEM with Chariot

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 Chariot platform provides all the above technological capabilities out of the box, and our professional services can help with the rest.

Contact Praetorian