PRAETORIAN

eBook

Continuous Threat Exposure Management (CTEM) and NIST SP 800-171 Compliance

Leveraging CTEM to Meet Enhanced NIST SP 800-171 Cybersecurity Requirements

Get Started ›

Inside this eBook

Introduction

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 provides enhanced security requirements for protecting Controlled Unclassified Information (CUI) in nonfederal systems and organizations. Continuous Threat Exposure Management (CTEM) offers a proactive approach to cybersecurity that aligns with NIST SP 800-171's advanced security practices. This eBook outlines how CTEM helps organizations satisfy these enhanced requirements through comprehensive vulnerability management, risk assessment, incident response, and more.

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:** 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.

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

Organizations move away from point-in-time assessments to continuous testing

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 NIST SP 800-171 compliance.

Key Requirements and CTEM Alignment

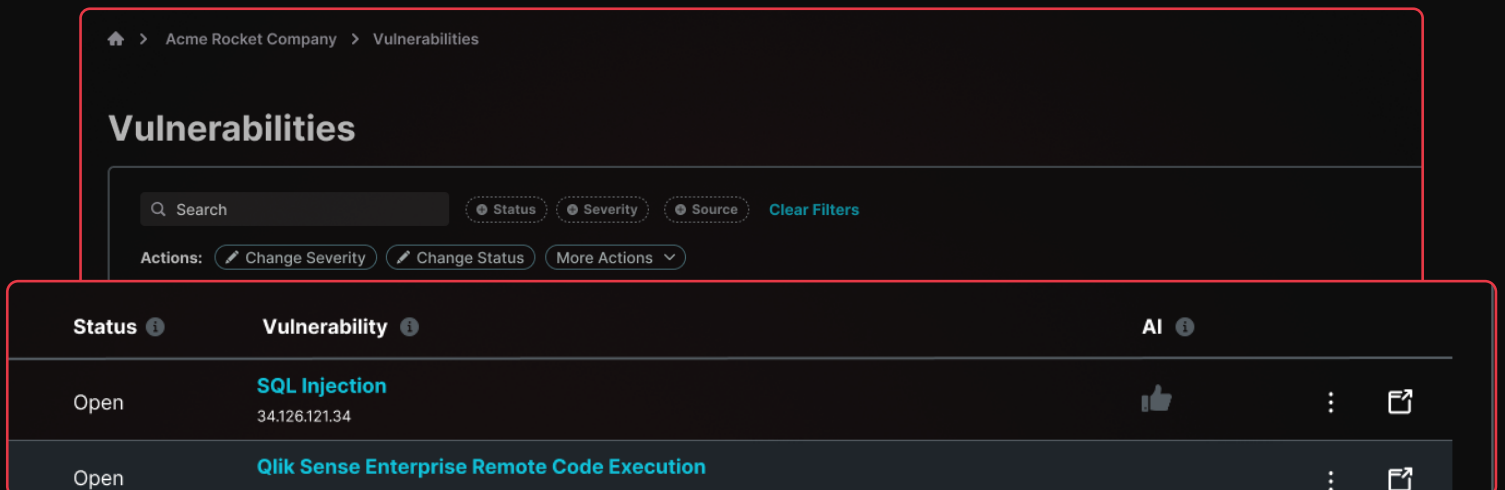
Vulnerability Management (SI-2, RA-5)

NIST SP 800-171 requires organizations to implement robust vulnerability management processes to detect, identify, and mitigate vulnerabilities:

Regular Vulnerability Assessments: Conduct regular automated and manual vulnerability assessments.

Timely Remediation: Prioritize and address vulnerabilities based on their risk to the organization.

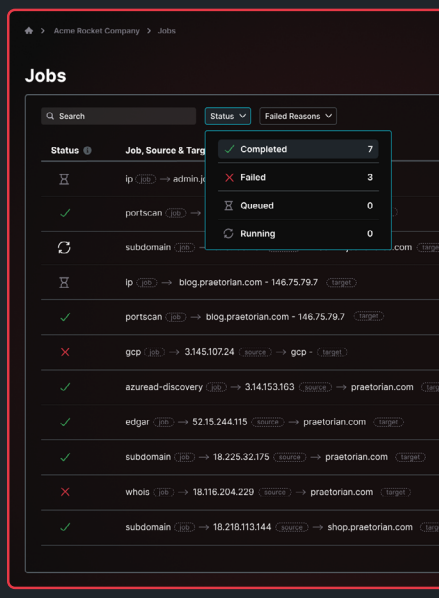
In an effective CTEM program, organizations move away from point-in-time assessments and toward continuous testing. Security professionals conduct regular testing against attack paths prioritized by impact. Because CTEM focuses manual efforts on a smaller set of higher-impact attacks, teams can afford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



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.

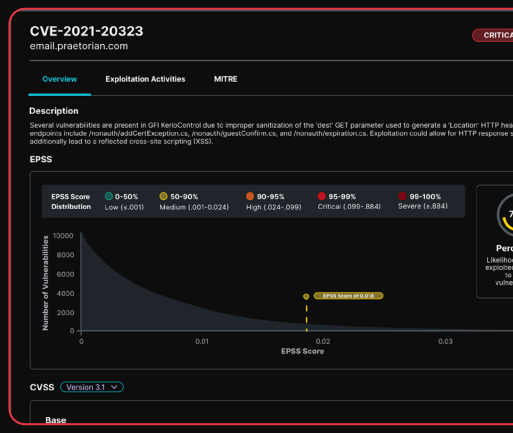
Collectively, these factors satisfy the SI-2 and RA-5 requirements.



Risk Assessment (RA-3)

RA-3 mandates periodic assessments to identify and prioritize cybersecurity risks to organizational assets, individuals, and data.

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 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.



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 NIST SP 800-171's RA-3 requirement.

Effective mobilization doesn't just patch individual risks... it facilitates the adoption of higher-level recommendations.

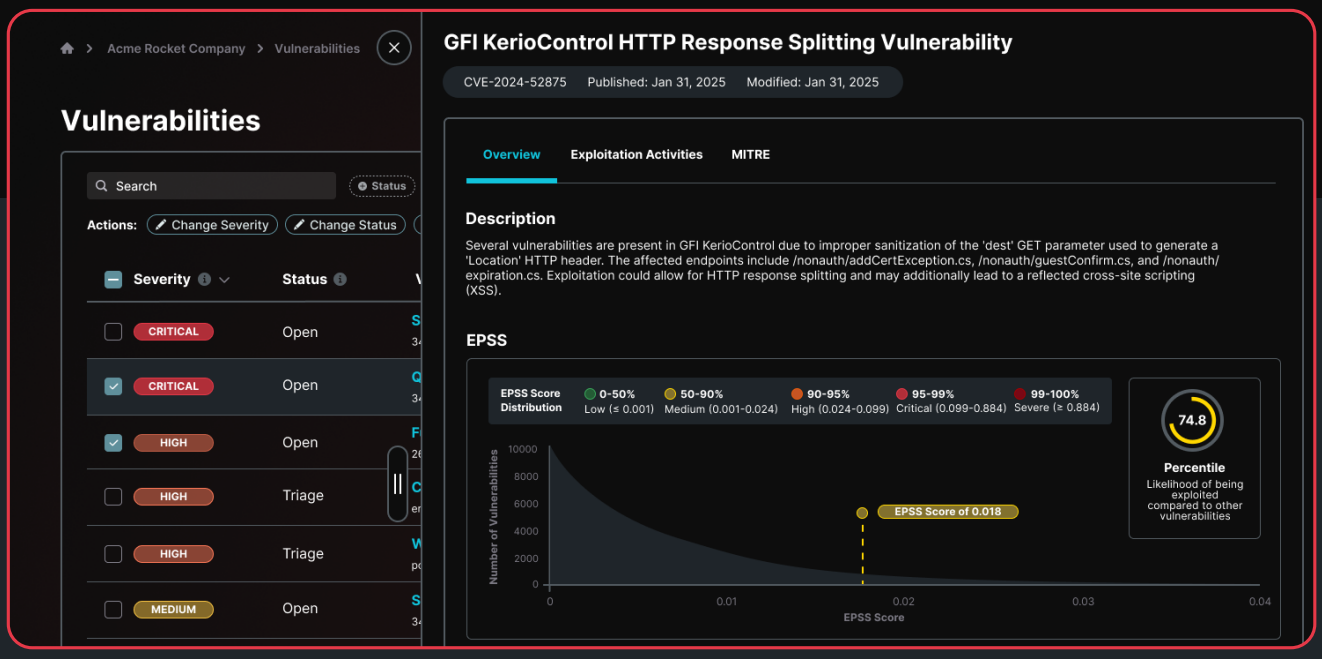
Asset Management and Monitoring (CM-8, CA-7)

Organizations must maintain a comprehensive and accurate asset inventory and continuously monitor their systems for security effectiveness.

Detailed Asset Inventory: Track organizational assets and key metadata, such as asset owner, location, and business classifications.

Continuous Monitoring: Implement continuous monitoring to ensure defensive controls remain effective.

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.



Training (AT-2, AT-3)

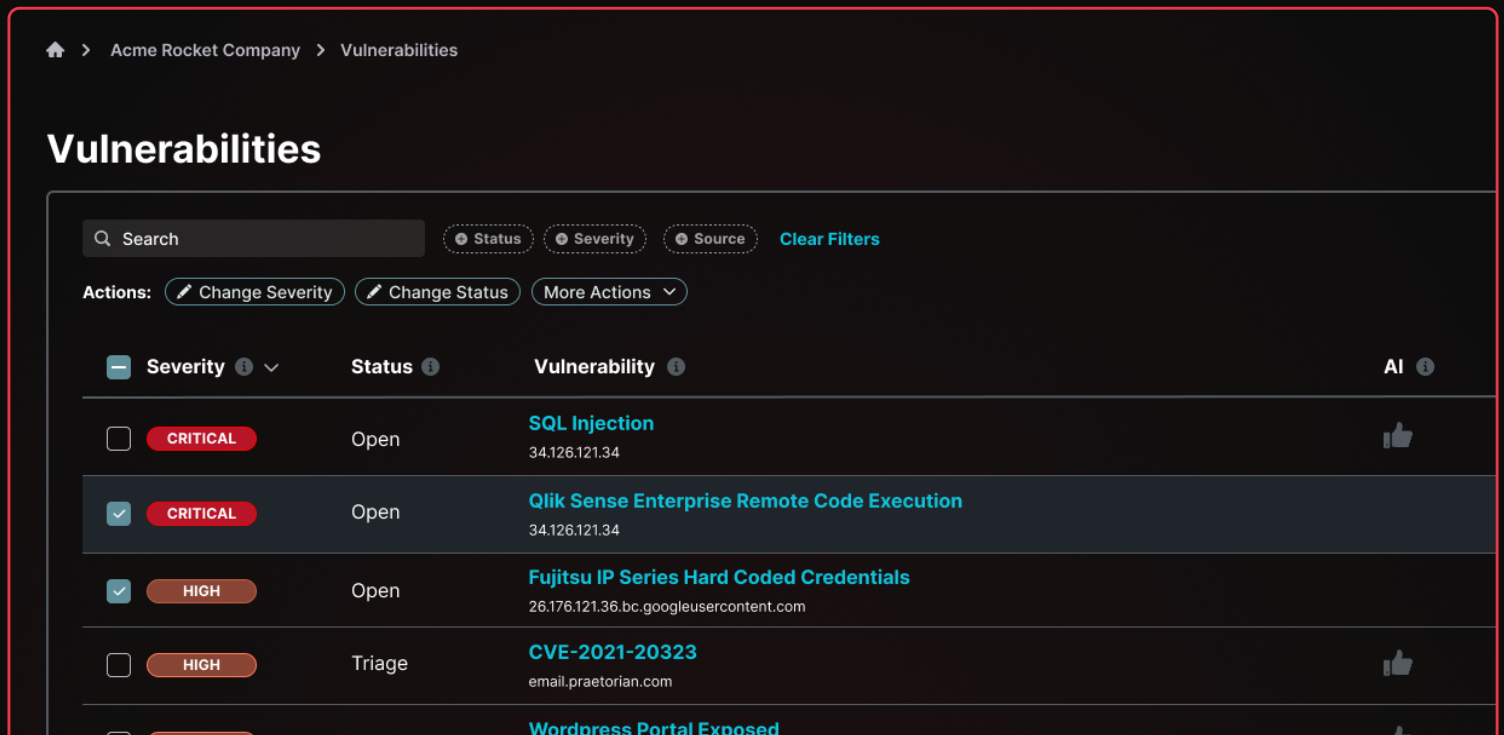
NIST SP 800-171 specifies the need for regular cybersecurity training, including role-specific training and exercises, to ensure that system administrators and users are aware of the security risks associated with their activities.

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 800-171 requirements and enhances the organization's overall security posture.

Incident Response and Business Continuity (IR-4, CP-4)

Organizations must develop and maintain capabilities to handle cyber incidents. This includes processes for preparation, detection, analysis, containment, recovery, and response. Furthermore, organizations must actively test their plans regularly to ensure their efficacy.

CTEM can help organizations meet 800-171 IR requirements by playing devil's advocate. A well-designed CTEM program allows an organization to constantly probe for weaknesses and test defenses, which includes simulating different types of attacks. As such, CTEM acts as a threat actor whose sole goal is to compromise your organization. Organizations use CTEM programs to test hypotheses about their incident response plans, compare different strategies or solutions, and iteratively improve their responses.



Conclusion

By integrating CTEM into their cybersecurity strategy, organizations can effectively meet the enhanced requirements of NIST SP 800-171. CTEM ensures compliance through continuous monitoring and proactive risk management, enhancing overall security resilience. This strategic approach helps organizations stay ahead of evolving threats while adhering to 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 Guard platform provides all the above technological capabilities out of the box, and our professional services can help with the rest.

Contact Praetorian