SANS | CYBERSECURITY LEADERSHIP

Understanding Continuous Threat Exposure Management (CTEM)

Jonathan Risto

2025-03-12

Agenda

- What is Continuous Threat Exposure Management?
- What are the main components of CTEM
- Difference between CTEM and traditional VM
- Why an organization should consider CTEM
- 5 things organizations can do to start to move to CTEM
- 5 CTEM challenges
- 5 Best practices for CTEM adoption
- Q&A

Who Am I?

- Course Co-Author – LDR516
- Started teaching with SANS 13+ years ago
  - I have taught SEC504, 560, 580, 566, FOR408 and 508, LDR516
- Member of the Faculty Research Committee at SANS.edu
  - Help students in their master's program complete their research paper, and grade the paper and presentation they have to do
  - STI Alumni – Master's in Information Security Management (MSISM)
- Day job
  - Technical Director, Cyber Posture Management
- Enjoy spending time with my kids and being outdoors

What is Continuous Threat Exposure Management???

- Continuous Threat Exposure Management (CTEM) is not a tool.
  - You cannot go out and buy CTEM in-a-box.
- It is an ongoing, risk-based approach to identifying, prioritizing, and mitigating security exposures across an organization.
- It goes beyond traditional vulnerability management by continuously evaluating risks like misconfigurations, identity weaknesses, and real-world attack paths.
- CTEM ensures security teams focus on the most critical threats, rather than just fixing every vulnerability.

What Are The Main Parts Of The CTEM Process?

- Scoping
  - Defines the security areas and assets to evaluate (e.g., cloud environments, on-prem infrastructure, applications).
  - Identifies business-critical systems, high-value assets, and known threat actors targeting the organization's industry.
  - Aligns CTEM goals with business risk and security priorities.
- Discovery
  - Continuously identifies security exposures across all assets, including vulnerabilities, misconfigurations, identity weaknesses, and shadow IT.
  - Uses asset discovery tools, external attack surface management (EASM), and active scanning methods.

What Are The Main Parts Of The CTEM Process? (2)

- Prioritization
  - Assesses and ranks security exposures based on exploitability, business impact, and adversary behavior.
  - Incorporates frameworks like EPSS (Exploit Prediction Scoring System) and SSVC (Stakeholder-Specific Vulnerability Categorization) to determine risk levels.
  - Considers attack path analysis to understand how an attacker could exploit multiple weaknesses in a kill chain.
- Validation
  - Tests the effectiveness of security controls using penetration testing, breach-and-attack simulations, and red teaming.
  - Validates whether prioritized exposures are truly exploitable under real-world conditions.
  - Helps security teams focus on practical, high-impact remediation efforts rather than hypothetical risks.
- Mobilization
  - Translates risk findings into actionable mitigation and remediation efforts.
  - Engages IT, security, and business teams to resolve prioritized issues.
  - Establishes feedback loops to refine and improve the CTEM process over time.

Differences Between CTEM and Traditional Vulnerability Management

Traditional Vulnerability Management	Continuous Threat Exposure Management (CTEM)
Focuses mainly on known software vulnerabilities (CVEs).	Evaluates all types of exposures, including misconfigurations, identity weaknesses, and attack paths.
Relies on periodic scanning (e.g., monthly or quarterly).	Continuous assessment of security risks.
Uses static scoring methods (e.g., CVSS).	Incorporates threat intelligence (e.g., EPSS, SSVC, attack path analysis).
Prioritization is based mostly on severity scores.	Prioritization is based on real-world exploitability and business impact.
Remediation is often handled in silos, with IT fixing vulnerabilities without security validation.	Involves cross-functional teams, including security, IT, and business units, for more strategic remediation.
Often lacks validation—fixes are applied without verifying their effectiveness.	Uses red teaming, breach simulations, and attack path analysis to validate threats and fixes.

Why Should An Organization Consider CTEM?

- Better risk-based prioritization
  - CTEM ensures security teams focus on exposures that pose real threats, not just theoretical vulnerabilities.
- Aligns security with business risk
  - CTEM ensures security priorities align with business-critical functions, reducing operational friction and improving decision-making.
- Continuous security improvement
  - Instead of periodic assessments, CTEM continuously refines an organization's security posture.
- Addresses modern attack techniques
  - Adversaries don't just exploit CVEs; they abuse misconfigurations, identity gaps, and weak security controls. CTEM accounts for these.
- Enhances validation
  - Organizations often patch vulnerabilities without knowing if attackers could exploit them. CTEM integrates validation techniques to verify security effectiveness.

What Are The 5 Things Organizations Can Do To Start To Move To The CTEM Model?

- Map the Attack Surface
  - Use attack surface management (ASM) tools to discover known and unknown assets, including cloud environments, SaaS applications, and on-prem infrastructure.
  - Identify security gaps beyond traditional vulnerabilities, such as misconfigurations and excessive privileges.
- Adopt Threat-Informed Prioritization
  - Move beyond CVSS and incorporate EPSS, SSVC, and threat intelligence feeds to understand real-world exploitability.
  - Consider business context when prioritizing exposures—an internet-facing asset with a known exploit should take priority over a low-risk internal system.
- Implement Continuous Testing and Validation
  - Leverage red teaming, penetration testing, and breach simulation to validate which vulnerabilities and weaknesses are most critical.
  - Adopt automated testing tools to ensure continuous validation of security controls.
- Establish a Cross-Functional Security Program
  - Break down silos between vulnerability management, security operations, and IT teams.
  - Define clear workflows for assessing, prioritizing, and remediating exposures.
- Shift from a Reactive to a Continuous Approach
  - Move from scheduled scans to continuous security assessments using cloud-native security tools, ASM solutions, and endpoint monitoring.
  - Implement real-time dashboards to track security posture and risk trends.

5 CTEM Challenges

- Cultural Resistance
  - Many security teams are used to the traditional vulnerability management approach. Moving to a continuous, risk-based model requires a mindset shift.
  - IT teams may resist new remediation workflows that prioritize risks differently than before.
- Tooling and Integration Gaps
  - Organizations often rely on vulnerability scanners that aren't designed for real-time exposure management.
  - Security teams may need to integrate new technologies, such as ASM, breach simulation, and attack path mapping tools.
- Data Overload
  - CTEM produces a large volume of data, including exposure reports, validation results, and risk assessments.
  - Without proper automation and analytics, teams may struggle to focus on the most important security issues.

More of the 5 CTEM Challenges

- Cross-Team Collaboration
  - CTEM requires cooperation between security, IT, DevOps, and business teams.
  - Without clear communication and ownership, remediation efforts may stall.
- Measuring Success
  - Traditional vulnerability management has clear KPIs (e.g., number of vulnerabilities fixed).
  - CTEM requires new metrics that measure security posture improvements over time, such as exposure reduction and attack path mitigation.

5 Best Practices for CTEM Adoption

- Focus on quick wins first
  - Start small, e.g., implement CTEM for high-risk assets first (e.g., external-facing cloud environments).
  - Use threat intelligence and attack paths to justify risk-based prioritization to leadership.
- Automate as much as possible
  - Use automation for attack surface discovery, risk scoring, and remediation workflows.
  - Implement API integrations between vulnerability management, SOAR, and ASM tools for seamless security operations.
- Make security validation a habit
  - Run continuous security tests, rather than waiting for annual red team engagements.
  - Validate whether security controls actually mitigate real-world threats.
- Communicate in business terms
  - Use business impact scoring to gain leadership buy-in.
  - Replace security jargon with clear risk reduction metrics that align with business goals.
- Continuously evolve
  - CTEM is a continuous process—adapt to evolving attack techniques and business risks.
  - Regularly review and refine CTEM workflows based on feedback and security incidents.

Summary

- Proactive & Continuous – Moves beyond periodic scans to continuously assess security risks.
- Risk-Based Prioritization – Focuses on real-world threats and attack paths, not just CVSS scores.
- Expands Beyond CVEs – Includes misconfigurations, identity weaknesses, and cloud exposures.
- Threat-Informed Decisions – Uses intelligence like EPSS, SSVC, and attack simulations to guide remediation.
- Cross-Team Collaboration – Requires alignment between Security, IT, DevOps, and Business teams.
- Key Takeaway:
- CTEM modernizes vulnerability management by focusing on continuous risk reduction, ensuring security teams address what truly matters to prevent real-world attacks.

SANS | GIAC CERTIFICATIONS

FORMULA FOR **OPERATIONAL CYBERSECURITY EXECUTIVES**

516 **VULNERABILITIES**
Building and Leading a Vulnerability Management Program

566 **CONTROLS**
Implementing and Auditing Security Frameworks and Controls

551 **SECURITY OPERATIONS**
Building and Leading a Security Operations Center

sans.org/cybersecurity-leadership/triads

SANS CYBERSECURITY LEADERSHIP

Building and Leading Vulnerability Management Programs

sans.org/ldr516

Developing World Class Cyber Security Leaders

Online

OnDemand

Anytime

with Jonathan Risto

Live Online & In Person

SANS 2025 - Orlando

Apr 13 - 17

with Jonathan Risto

Live Online

SANS Cyber Security Mountain

March 31 – Apr 4

with Jonathan Risto

SANS | CYBERSECURITY LEADERSHIP

Thank You - Questions?

Jonathan Risto

www.linkedin.com/in/jonathanristo

Jonathan@zenzizensec.com