NetSPI

Proactive Defense

Mastering Continuous Threat Exposure Management (CTEM)

International Cyber Risk Summit 2025

Joe Evangelisto, CISO

July 11, 2025

Agenda

- Why CTEM? Why Now?
- Benefits
- Stages of CTEM
- CTEM in Action
- NetSPI's Role
- Wrap Up

The Evolving Threat Landscape

Current State of Vulnerability Management

CVEs Exploding:

- 22,254 CVEs *(mid-2024)*
  - 30% jump (2023)
  - 56% jump (2022).

Daily Vulnerabilities Surging:

- 115 CVEs disclosed daily

Vulnerability Attacks Soaring:

- 124% increase in Q3 2024 (vs. 2023)

Public-Facing Apps Exploited:

- 25% of attacks targeted public-facing app vulnerabilities.

Why Adopt CTEM?

Tangible Business & Security Benefits

Reduced Breach Risk	Improved Security ROI	Enhanced Cyber Resilience
Better Communication & Collaboration	Compliance Support	Business Enablement

By 2026, organizations prioritizing their security investments based on a continuous exposure management program will be three times less likely to suffer from a breach.

- Gartner

Think of CTEM as a continuous security health check — showing you where you're weak, before attackers find out.

What is Continuous Threat and Exposure Management (CTEM)?

KEY PRINCIPLES:

- Continuous vs. Periodic
- Business-Risk Focused
- Threat-Informed
- Exposure-Centric

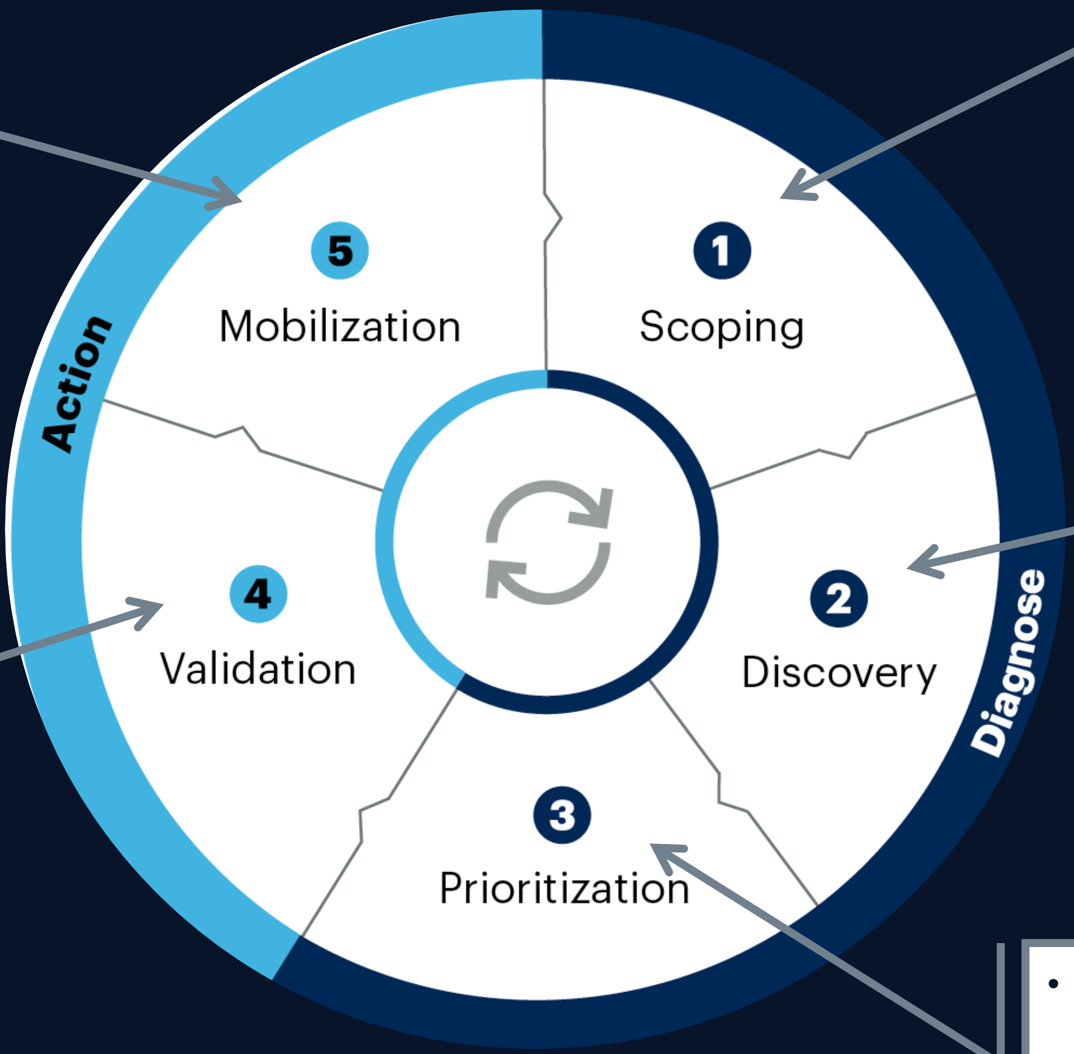
CORE DIFFERENTIATORS

- From Reactive to Proactive
- From Technical to Business
- From Static to Dynamic
- From Volume to Value

CTEM Framework

- Communicate **findings and actions**
- Assign **remediation Tasks**
- Integrate into **security operations**

- Identify **critical assets** and information.
- Understand potential **attack paths**
- Define **risk tolerance**.



- Catalog all **digital assets**.
- Uncover **vulnerabilities** and misconfigurations.
- Map asset **interconnections**.

- Test **security controls**.
- Verify **vulnerability resolution**.
- Measure **exposure reduction**.

- Assess **business impact** of exposures.
- Rank risks by **severity**.
- Focus on **highest impact threats**.

Practical Example

Traditional Vulnerability Management

M1: 847 Vulnerabilities Found

M2: Focus on 12 "Critical" CVEs

M3: Still patching Critical vulns

M4: Breach occurs via **CVSS 6.8 Vuln**

New scan finds 923 new vulnerabilities

❌ **45,000 customer records exposed**
❌ **$2.3M total breach cost**
❌ Vulnerability was "medium priority"

CTEM Approach

W1: Scoping & Discovery

Critical assets mapped, continuous monitoring deployed

W3: Prioritization

CVSS 6.8 API vuln flagged as **Priority**

- active exploits + customer data access

W4: Validation

Confirmed direct path to customer database

W5: Mobilization

Emergency patch + WAF rules deployed

NetSPI & CTEM

	DIAGNOSE			ACTION	
	SCOPING	DISCOVERY	PRIORITIZATION	VALIDATION	MOBILIZATION
PRODUCTS					
SERVICES					

DIAGNOSE

ACTION

SCOPING | DISCOVERY | PRIORITIZATION | VALIDATION | MOBILIZATION

PRODUCTS

Attack Surface Management (ASM)

EXTERNAL	INTERNAL / CYBER ASSET
EASM / EASM Plus	**CAASM**
Always-on external attack surface asset and vulnerability discovery and monitoring.	Real-time internal attack surface asset and vulnerability visibility and contextualization.
EXTERNAL ASSET DISCOVERY & INVENTORY	INTERNAL ASSET AND RISK
CONTINUOUS MONITORING & TESTING	CONTROLS COVERAGE
HUMAN VALIDATION (ZERO FALSE POSITIVES)	RISK BASED REMEDIATION

SERVICES

DIAGNOSE

ACTION

SCOPING | DISCOVERY | PRIORITIZATION | VALIDATION | MOBILIZATION

PRODUCTS

Attack Surface Management (ASM)

EXTERNAL

EASM / EASM Plus

Always-on external attack surface asset and vulnerability discovery and monitoring.

- EXTERNAL ASSET DISCOVERY & INVENTORY
- CONTINUOUS MONITORING & TESTING
- HUMAN VALIDATION (ZERO FALSE POSITIVES)

INTERNAL / CYBER ASSET

CAASM

Real-time internal attack surface asset and vulnerability visibility and contextualization.

- INTERNAL ASSET AND RISK
- CONTROLS COVERAGE
- RISK BASED REMEDIATION

Breach and Attack Simulation (BAS) as a Service

Validate security detection controls, improve cyber defense readiness, and demonstrate security ROI.

- EFFECTIVENESS OF BREACH DETECTION CAPABILITIES
- SECURITY COVERAGE VISIBILITY
- IMPROVE DETECTION CAPABILITIES

BREACH AND ATTACK SIMULATION PACKS

- MITRE ATT&CK
- AZURE CLOUD
- RANSOMWARE
- LINUX
- ESXI

SERVICES

DIAGNOSE

ACTION

SCOPING | DISCOVERY | PRIORITIZATION | VALIDATION | MOBILIZATION

PRODUCTS

Attack Surface Management (ASM)

EXTERNAL

EASM / EASM Plus

Always-on external attack surface asset and vulnerability discovery and monitoring.

- EXTERNAL ASSET DISCOVERY & INVENTORY
- CONTINUOUS MONITORING & TESTING
- HUMAN VALIDATION (ZERO FALSE POSITIVES)

INTERNAL / CYBER ASSET

CAASM

Real-time internal attack surface asset and vulnerability visibility and contextualization.

- INTERNAL ASSET AND RISK
- CONTROLS COVERAGE
- RISK BASED REMEDIATION

Breach and Attack Simulation (BAS) as a Service

Validate security detection controls, improve cyber defense readiness, and demonstrate security ROI.

- EFFECTIVENESS OF BREACH DETECTION CAPABILITIES
- SECURITY COVERAGE VISIBILITY
- IMPROVE DETECTION CAPABILITIES

BREACH AND ATTACK SIMULATION PACKS

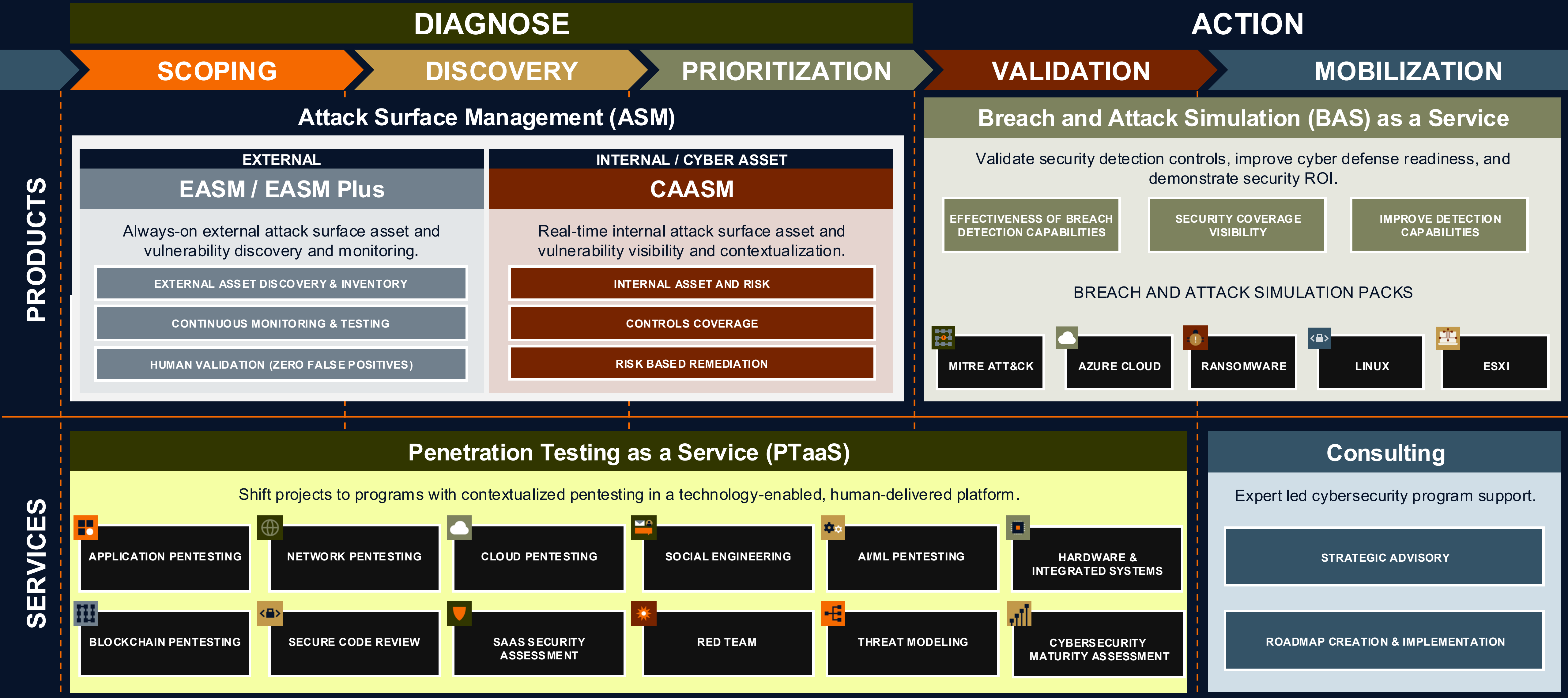
- MITRE ATT&CK
- AZURE CLOUD
- RANSOMWARE
- LINUX
- ESXI

SERVICES

Penetration Testing as a Service (PTaaS)

Shift projects to programs with contextualized pentesting in a technology-enabled, human-delivered platform.

- APPLICATION PENTESTING
- NETWORK PENTESTING
- CLOUD PENTESTING
- SOCIAL ENGINEERING
- AI/ML PENTESTING
- HARDWARE & INTEGRATED SYSTEMS
- BLOCKCHAIN PENTESTING
- SECURE CODE REVIEW
- SAAS SECURITY ASSESSMENT
- RED TEAM
- THREAT MODELING
- CYBERSECURITY MATURITY ASSESSMENT



DIAGNOSE
ACTION
SCOPING
DISCOVERY
PRIORITIZATION
VALIDATION
MOBILIZATION
PRODUCTS
Attack Surface Management (ASM)
EXTERNAL
EASM / EASM Plus
Always-on external attack surface asset and vulnerability discovery and monitoring.
EXTERNAL ASSET DISCOVERY & INVENTORY
CONTINUOUS MONITORING & TESTING
HUMAN VALIDATION (ZERO FALSE POSITIVES)
INTERNAL / CYBER ASSET
CAASM
Real-time internal attack surface asset and vulnerability visibility and contextualization.
INTERNAL ASSET AND RISK
CONTROLS COVERAGE
RISK BASED REMEDIATION
Breach and Attack Simulation (BAS) as a Service
Validate security detection controls, improve cyber defense readiness, and demonstrate security ROI.
EFFECTIVENESS OF BREACH DETECTION CAPABILITIES
SECURITY COVERAGE VISIBILITY
IMPROVE DETECTION CAPABILITIES
BREACH AND ATTACK SIMULATION PACKS
MITRE ATT&CK
AZURE CLOUD
RANSOMWARE
LINUX
ESXI
SERVICES
Penetration Testing as a Service (PTaaS)
Shift projects to programs with contextualized pentesting in a technology-enabled, human-delivered platform.
APPLICATION PENTESTING
NETWORK PENTESTING
CLOUD PENTESTING
SOCIAL ENGINEERING
AI/ML PENTESTING
HARDWARE & INTEGRATED SYSTEMS
BLOCKCHAIN PENTESTING
SECURE CODE REVIEW
SAAS SECURITY ASSESSMENT
RED TEAM
THREAT MODELING
CYBERSECURITY MATURITY ASSESSMENT
Consulting
Expert led cybersecurity program support.
STRATEGIC ADVISORY
ROADMAP CREATION & IMPLEMENTATION

Key Takeaways

CTEM is essential for modern cybersecurity resilience

Continuous beats periodic - always-on monitoring prevents blind spots

Business context over technical scores - protect what matters most

Prevention is cheaper than recovery - proactive defense delivers ROI

Call to ACTION:
Secure Your Future Proactively

- Assess your current security posture.
- Start the CTEM conversation in your organization.
- Identify one area where you can apply CTEM principles this quarter.
- Explore leveraging NetSPI to support your journey.

Want to learn more?

Get a free copy of

Continuous Threat Exposure Management For Dummies

NetSPI Special Edition