CYCOGNITO

TECHNOLOGY CHECKLIST

Demystifying Continuous Threat Exposure Management (CTEM)

Ensure your EASM platform meets the needs of your exposure management program

Continuous Threat Exposure Management (CTEM) is a risk reduction strategy designed to unify traditional silos of visibility, risk assessment, issue prioritization, and validation. With CTEM, exposed systems are continuously identified and comprehensively tested, allowing teams to make informed decisions and take prompt action.

External attack surface management (EASM) technology is a foundational element of CTEM, providing coverage for the most common and difficult-to-manage attack vector.[1]

Gartner states, "By 2026, organizations prioritizing their security investments, based on a continuous threat exposure management program, will realize a two-third reduction in breaches." The right EASM paves the way for achieving this goal.

Exposure Management

Exposure management is a modern risk management program that supersedes legacy vulnerability management programs.

When evaluating technologies for use within your CTEM program, ensure that your success criteria aren't developed with workflows that lack coverage, accuracy and frequency of insight required.

Choosing an EASM requires evaluating a broad range of capabilities prior to committing to a proof of value (PoV). As an example, Gartner's 2024 Strategic Roadmap for Managing Threat Exposure report lists two requirements that align directly with EASM:

- What are the most critical and exposed IT systems and enterprise IT subscriptions in relation to those business processes? Are all of those systems visible, and where are those systems?
- Who are the system and service management owners of such IT systems and enterprise IT subscriptions, and who can effect change on those?

Implementing an EASM that does not meet these requirements would directly impact the success of the exposure management program.

CTEM Technology Checklist

This checklist will help you ask the right questions when shortlisting an EASM technology for inclusion in your exposure management program.

Scoping

This phase involves the identification of infrastructure segments tied to your parent organization.

Requirement	EASM Purchase Guidance
☐ Automatically build a model of organizational business relationships as it relates to the parent company, including acquired companies, subsidiaries, and joint ventures	*Ensure the EASM provides fully automated organizational reconnaissance globally. Evidence collection for each decision streamlines all CTEM scopes.* *Tools that require manual input to maintain pace with changes do not have the level of sophistication needed for CTEM.*
☐ Automatically discover new organizations and changes to existing organizations	
☐ Provide a clearly defined discovery path for all discovered organizations	
☐ Does not require input or seed information to identify business structure	

Discovery

This phase involves discovery and testing of all exposed assets.

ASSET DISCOVERY

Requirement	EASM Purchase Guidance
☐ Automatically discover exposed assets across all organizational business segments	*Ensure the EASM provides fully automated asset discovery across the entire organization. Discovery evidence and confidence scores are critical for this phase of CTEM.* *Tools that only search for assets within pre-configured IP ranges cannot scale to enterprise requirements.*
☐ Provide the discovery path for all discovered assets (for example, where the asset resides in relationship to the business structure)	
☐ Show asset relationships with each other	
☐ Provide multiple asset discovery options, including high-frequency (daily/weekly/bi-weekly/monthly/etc)	

Discovery *(Continued)*

ASSET ATTRIBUTION

Requirement	EASM Purchase Guidance
☐ Automatically determine asset attribution	*Ensure the EASM automatically capturescontext to speed remediation and CTEM mobilization.* *Performed manually, attribution can take 5-10 hours per asset.[2] Tools that do not support automation will be difficult to build into a CTEM program.*
☐ Provide confidence score and supporting evidence about the relation of the asset to the organization	

ASSET CLASSIFICATION

Requirement	EASM Purchase Guidance
☐ Automatically classify all assets based on business context	*Ensure the EASM provides business context that enables accurate remediation prioritization.* *Tools that focus on running services alone lack the information needed to make effective decisions.*
☐ Determine the criticality of the asset to the organization	
☐ Identify web applications and their key components	
☐ Identify cloud assets and their key components	

RISK DETECTION

Requirement	EASM Purchase Guidance
☐ Automatically identify risk across all exposed assets	*Ensure the EASM continuously assesses risk across all external assets with active testing (including DAST for web apps).* *Tools that rely solely on passive scanning (also known as banner grabbing) for both asset discovery and risk detection create high false positives and gaps. Passive scanning cannot identify complex risks or verify remediation.*
☐ Provide risk detection at the pace of exposure (daily/weekly/bi-weekly/monthly/etc)	
☐ Captures evidence of risk per asset and makes it available to users	

Prioritization

This phase involves exposures ranked based on risk and asset information.

Requirement	EASM Purchase Guidance
✓ Provide risk-based prioritization through business context and exploit availability/weaponization obtained through threat intelligence	*Ensure the EASM includes prioritization data based on current threat intelligence and business context to understand the true risk to your organization.* *Tools that rely solely on CVSS information for risk prioritization do not align with the organization's business requirements.*
✓ Include vulnerability research to augment prioritization	
✓ Rank exposures based on impact on business	
✓ Rank exposures based on issue severity	
✓ Rank exposures based on asset discoverability	
✓ Rank exposures based on asset attractiveness	
✓ Identify critical attack vectors	

Validation

This phase includes an assessment of the likelihood of attacker success, verifies identified risk and estimates business impact.

Requirement	EASM Purchase Guidance
✓ Validates risk detection using active security testing engines	*Ensure the EASM automatically assigns issue prioritization ranking based on validated active test and threat intelligence information.* *Tools that do not actively test for vulnerabilities will lead to high false positives and wasted efforts.*
✓ Tests web applications using dynamic application security testing, or DAST	
✓ Detects data exposure and classifies data sensitivity	
✓ Collects evidence for all test results and makes evidence available through the console and API	
✓ Validates remediation efforts through active security testing	

Mobilization

This phase involves sharing exposure information and evidence to responsible teams.

Requirement	EASM Purchase Guidance
✓ Provides trackable remediation planning per organization and per environment within the organization	*Ensure the EASM automatically provides issue context that includes exploit availability, attacker interest, exploitation tools, remediation effort and remediation instructions.* *Tools that require further investigation for remediation guidance cannot scale to enterprise requirements.*
✓ Provides testing instructions to simplify validation	
✓ Provides metrics to show improvement in risk posture over time	
✓ Provides metrics showing remediation trends over time	
✓ Includes workflow automation and communication integration via API to deliver exposure information	

Mapping CyCognito EASM to CTEM Technology Capabilities

The CyCognito platform aligns with the five phases of CTEM; scoping, discovery, prioritization, validation and mobilization.

CTEM		CyCognito EASM Phase
Phase	**Capability**	
Scoping	• Organizational mapping • Identify security initiatives, build scopes	**Discovery & Contextualization**
Discovery	• Asset discovery - Known IP ranges/segments • Asset discovery - New IP ranges/segments • Asset classification • Asset attribution • Risk assessment - Passive scanning	
Prioritization	• Exposure ranking/Issue prioritization • Threat intelligence	**Prioritization**
Validation	• Risk assessment - Active security testing • Risk assessment - Application testing (DAST)	**Security Testing**
	• Likelihood of attacker success • Evidence collection • Remediation validation	**Remediation**
Mobilization	• Remediation instructions	
	• Workflow automation/integration • Alerting	**Integration & Automation**

Find Out How CyCognito Accelerates Exposure Management Programs

CyCognito is a cloud-native software-as-a-service that was built to meet the external risk requirements of the largest and most complex organizations. To find out more about our external attack surface management (EASM) platform and how CyCognito aligns with your exposure management program, please contact us at info@cycognito.com or www.cycognito.com.

1. 83% of breaches involve external actors. Source: Verizon Data Breach Intelligence Report, 2023
2. Source: Communication with enterprise CyCognito customers, 2023

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit **cycognito.com**.

CYCOGNITO