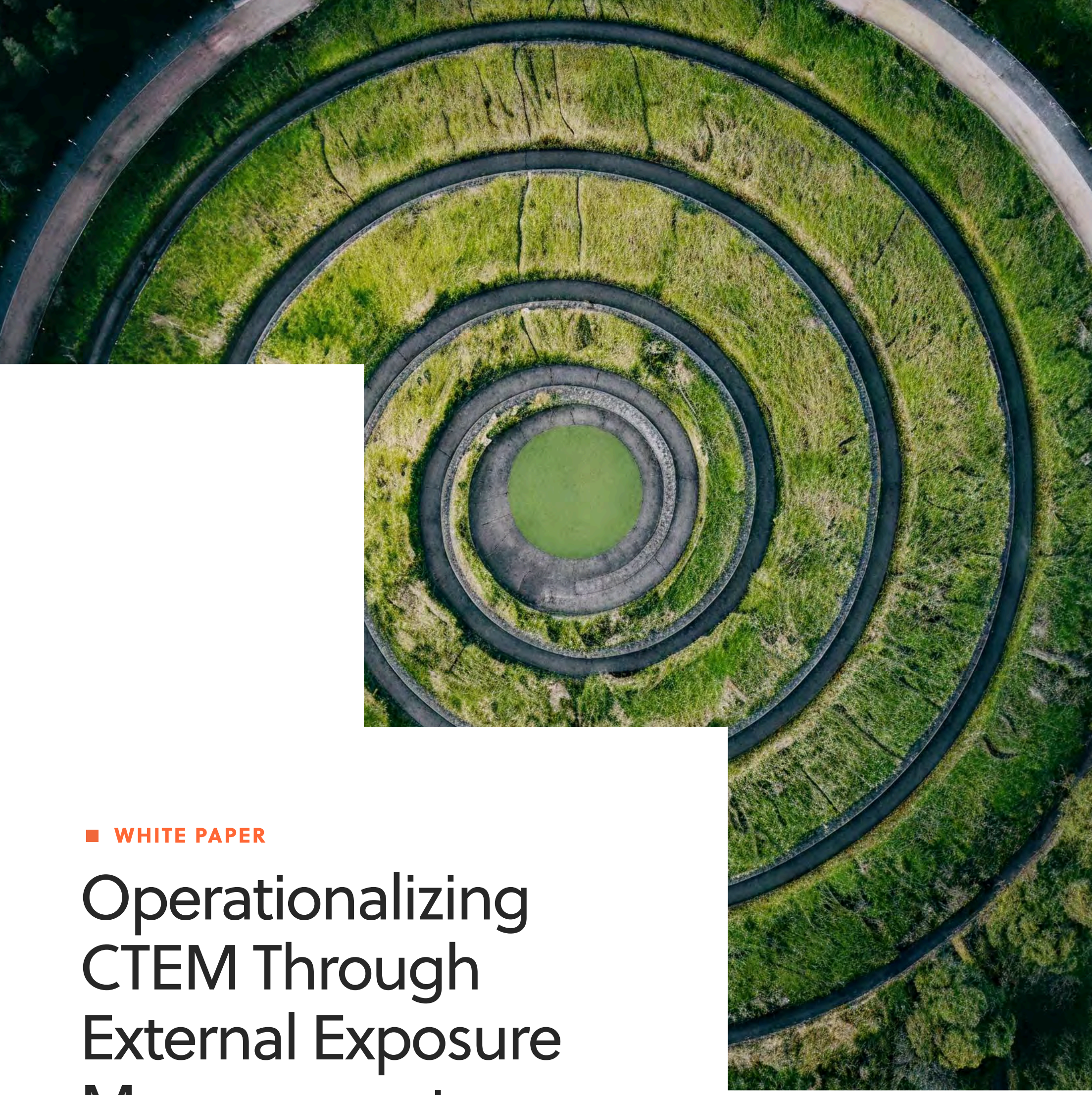

WHITE PAPER

Operationalizing CTEM Through External Exposure Management

From Vulnerability Chasing to Exposure Management

CYCOGNITO

Introduction

For years, organizations have measured security progress by the number of vulnerabilities identified and patched. The assumption was simple: more findings meant better coverage and lower risk.

Over time, the flaws became clear. Vulnerability programs produced growing volumes of findings while becoming less effective, creating large backlogs with little connection to attacker behavior or material business impact.

Teams grew busier, but not safer.

In 2022, Gartner introduced Continuous Threat Exposure Management (CTEM), recognizing that vulnerability-centric, tool-driven programs do not reduce exposure at scale.

CTEM defines a continuous lifecycle to identify, prioritize, validate, and mobilize. It shifts teams toward evidence-based decisions, reducing false urgency and focusing effort on attacker-relevant issues.

The goal is to prioritize impact over volume, cutting friction and wasted effort. Fewer issues are escalated, remediation becomes more targeted, and validation runs continuously instead of in bursts, to ensure ongoing resilience.

CTEM adoption is now moving from framework to practice. This paper covers the practical mechanics: impact on security KPIs, key technical requirements and practical ways to operationalize CTEM through external exposure management.

New to CTEM?

If you're new to CTEM and want to learn more about the basics download our Understanding Continuous Threat Exposure Management whitepaper.

Get The Whitepaper →

How CTEM Refocuses Security KPIs

One way to understand what CTEM changes is to look at how it reshapes the reporting conversation with leadership and the board. In traditional vulnerability management, security KPIs are largely volume and throughput based: total open CVEs, percentage patched, backlog size, etc.

These metrics are easier to produce, but they fluctuate with scan cadence and patch cycles, making them noisy and difficult to interpret.

CTEM shifts the reporting conversation from vulnerability counts to a smaller set of urgent issues and assets, by emphasizing resilience and prioritized action based on validated findings. KPIs then reflect efficiency and focus, tying security work to broader business objectives.

Here are a few examples of KPIs that illustrate this shift:

Urgent Issues Requiring Action

- **What changed:**
  Counting focuses on urgent issues requiring immediate action, rather than problems suited to ongoing security hygiene improvements.
- **Win looks like:**
  Reducing the number of issues to a few hundred validated, truly critical items across tens to low hundreds of critical assets.

Team Hours Spent On Remediation

- **What changed:**
  Measurement centers on the time engineering and operations teams spend on urgent remediation work.
- **Win looks like:**
  A significant (60–80%+) reduction in engineering and operations hours consumed by emergent remediation.

Ongoing Testing Coverage Of Critical Assets

- **What changed:**
  Coverage is defined by adherence to a testing cadence SLA (e.g., every 30–60 days) for a subset of critical assets, rather than point-in-time, broad red teaming and pentesting initiatives.
- **Win looks like:**
  Continuous compliance with the testing SLAs across the critical asset set.

CTEM and External Exposure Management

> "Attack surface assessment, delivered via external attack surface management tools, helps organizations understand visibility and reachability, but must be combined with prioritization, validation and mobilization."
>
> **Gartner,**
> **Reference Architecture Brief: Exposure Management**

Exposure starts with what attackers can discover and reach. That's why CTEM depends on managing the external attack surface.

Organizations establishing a CTEM program typically begin from one of three starting points:

- **Add external exposure management to an existing program:**
  Many organizations already run internal vulnerability or risk programs. They add external exposure management to close blind spots and prioritize based on attacker reachability.
- **Extend an existing external capability:**
  Some already have external discovery or scanning, but need to move beyond detection. To support CTEM, these organizations need to add validation, decision-ready prioritization, and workflows that drive remediation.

- **Start CTEM from scratch:**
  Organizations without established exposure management often begin with external exposure management, then layer in internal context and remediation workflows over time.

CyCognito supports all three scenarios by providing external exposure management and integrating it with internal context and remediation workflows.

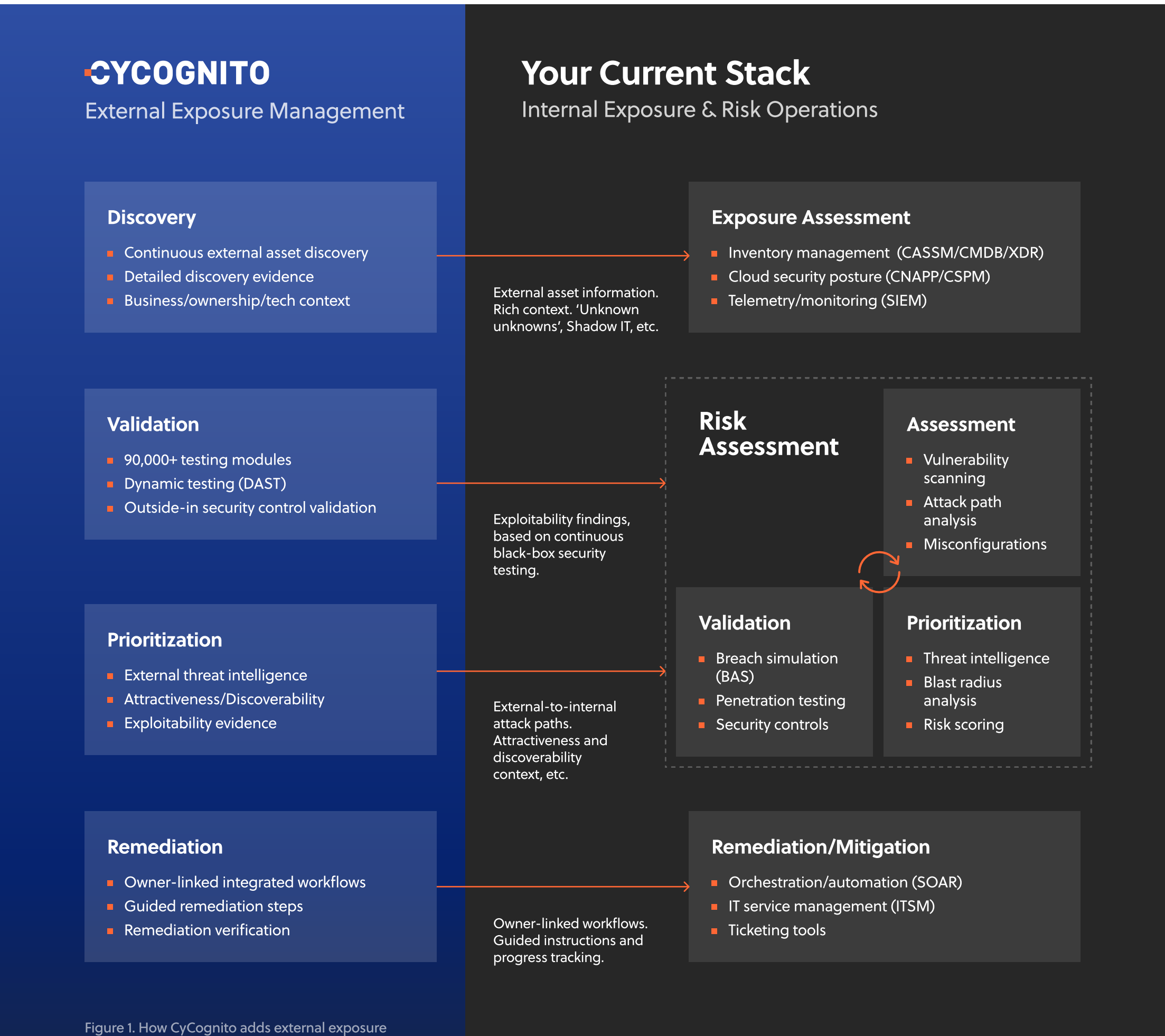

Figure 1. How CyCognito adds external exposure management to your CTEM technology stack

As the diagram shows, CyCognito continuously discovers externally reachable assets and validates which exposures are actually exploitable, producing contextual insights, validation evidence, and remediation guidance.

With outside-in grounding, CyCognito connects external reachability and exploitability to internal ownership and remediation so CTEM decisions follow real attacker paths instead of theoretical risk.

Through integrations, findings flow into existing asset inventory, risk assessment, and remediation systems, adding the context needed to drive prioritization and action.

Operationalize CTEM with CyCognito

■ SCOPING

"What are we focusing on, and why?"

> "Using a defined scope in a CTEM process means organizations do not have to tackle all exposures at once, but can start with what is most critical to the business."
>
> **Gartner,**
> **Strategic Roadmap for Continuous Threat Exposure Management**

Scoping sets the boundaries for continuous exposure management by determining where the CTEM program will focus and why. The decision is shaped by factors such as business priorities, compliance obligations, characteristics of asset inventory, the organization's risk profile and tolerance.

When this scope includes externally reachable exposure, CyCognito provides the visibility and validation needed to support CTEM execution, as outlined below.

DISCOVERY

"What is actually exposed right now?"

> "Discovery tools should prioritize external attack surface assessment, as it provides visibility into attacker-reachable assets."
>
> **Gartner,**
> **Use Continuous Threat Exposure Management to Reduce Cyberattacks**

Discovery continuously identifies externally reachable assets and exposure conditions, establishing a current view of what attackers can see.

Challenges to address

Attackers start with reconnaissance. They start by mapping what is reachable from the outside: exposed services, forgotten assets, shadow IT, etc. Next, they look for what is exploitable and could lead to meaningful compromise.

Most discovery approaches stop short of this. Some rely on seeded approaches that miss critical exposures. Others do not tie findings to validated exploitability, threat intelligence or deeper business relevance.

KEY REQUIREMENTS	CYCOGNITO APPROACH
Discover And Attribute Externally Reachable Assets	▪ Seedless discovery across on-prem, cloud, SaaS, and third-party environments ▪ Correlation of discovered assets to organizational structure, including subsidiaries and partners ▪ Continuous, daily monitoring of externally reachable assets and exposure conditions
Identify Risk Conditions Beyond CVEs	▪ Detection of exploitable conditions such as weak or missing authentication, exposed sensitive data, and misconfigurations ▪ Enrichment of findings with blast radius and security controls context ▪ Holistic view of attack paths via integrations with platforms (e.g., Armis, Axonius, and Wiz)
Produce Evidence-Backed Findings	▪ Provision of a detailed 'chain of discovery' evidence for each detected asset

PRIORITIZATION

"What should we fix first and why?"

> "Contextualized and reprioritized exposure risk data should be used as a new source of truth, rather than raw vulnerability scores."
>
> **Gartner,**
> **Reference Architecture Brief: Exposure Management**

Effective prioritization is not only about identifying what matters most, but also about establishing which issues do not require immediate action.

In practice, CTEM allows teams to distinguish between issues that demand urgent response and those that can be handled through standard hygiene, such as patching cycles or infrastructure refreshes.

This creates permission to "ignore things safely", without losing confidence that meaningful risks are being addressed.

Challenges to address

Prioritization remains vulnerability-centric in practice. Most tools still surface and score vulnerabilities as the primary signal, generating large volumes of alerts that look critical on paper but lack context about reachability, runtime relevance, or attacker behavior.

Without a way to narrow focus, teams escalate too many issues, eroding confidence, making reporting noisy and unreliable.

KEY REQUIREMENTS	CYCOGNITO APPROACH
Align Exposure Prioritization With Business Context	▪ Mapping of exposed assets to organizational structure and underlying infrastructure ▪ Association of exposures with business-critical services and potential attack paths
Incorporate Attacker Behavior And Threat Intelligence	▪ Incorporation of attacker behavior signals and external threat intelligence ▪ Evaluation based on reachability, attractiveness and ease of discovery ▪ Priority adjustment based on observed exploitation evidence in the wild

VALIDATION

"Can this actually be exploited?"

> "Validation works as a filter to prove which discovered exposures could actually impact the organization."
>
> **Gartner,**
> **Strategic Roadmap for Continuous Threat Exposure Management**

Validation confirms whether identified exposure can actually be exploited. In CTEM, validation turns exposure from a hypothesis into a decision by using active testing aligned with real attacker behavior.

Challenges to address

Validation does not scale in most environments. Organizations rely on point-in-time testing methods that provide depth in limited scope but cannot sustain continuous coverage across fast-changing attack surfaces.

Without ongoing validation, teams make remediation decisions without proof of exploitability, leading to effort spent on low-impact issues.

KEY REQUIREMENTS	CYCOGNITO APPROACH
Continuously And Safely Validate Exploitability As Conditions Change	▪ Active security testing using non-disruptive techniques, aligned with real attacker methods ▪ Ongoing revalidation as assets, configurations, risk profiles and exposure conditions change
Validate Exploitability Across A Broad Range Of Conditions And Controls	▪ Execution of 90,000+ security tests (including DAST) across 30+ categories, covering OWASP weaknesses, data exposure, abandoned assets, authentication bypass risk, etc. ▪ Validation of security control effectiveness (including WAF, encryption, and access controls)

KEY REQUIREMENTS	CYCOGNITO APPROACH
Produce Concrete, Actionable Validation Evidence	▪ Enriched scoring combining validated exploitability with attacker interest signals and potential impact ▪ Detailed technical findings with supporting artifacts, including exploit tooling, for self-verification

MOBILIZATION

"Who should fix it?"

> "Mobilization is the process of engaging teams outside of security to remediate exposures based on business risk."
>
> **Gartner,**
> **Mobilize Threat Exposure Management to Accelerate Remediation**

When mobilization works, teams stop getting hammered by repeated escalations for issues that lack context, proof, or clear ownership.

Validated evidence, risk-based urgency, ownership-linked routing, and clear remediation guidance reduce back-and-forth.

This, and the ability to continuously track open issues, means that when a problem is escalated, it gets attention.

Challenges to address

Mobilization stalls when findings lack clear ownership, proof, or actionable guidance.

Repeated escalations and manual handoffs create friction between security and delivery teams, slowing remediation and increasing operational fatigue.

KEY REQUIREMENTS	CYCOGNITO APPROACH
Deliver Exposure-Specific Remediation Guidance And Evidence	▪ Detailed technical findings with supporting artifacts, including exploit tooling for self-verification ▪ Remediation guidance tailored to each issue, with clear step-by-step instructions.
Assign Ownership To The Correct Teams And Systems	▪ Owner-linked logic that maps issues to responsible teams and systems ▪ Integration with ITSM, ticketing, and DevOps tools to deliver findings into the right hands
Track Progress And Confirm Exposure Reduction	▪ Remediation planning and progress visibility across teams, prioritized by severity and business impact ▪ Follow-up validation to confirm whether exploitable conditions have been reduced

The Right Partner for Your CTEM Journey

You can't buy CTEM or implement it with a single tool. CTEM is a framework, and results come from how consistently organizations execute discovery, prioritization, validation, and mobilization.

CyCognito helps operationalize CTEM by grounding decisions in what attackers can actually discover and exploit. This outside-in perspective, combined with continuous always-on validation and clear attribution, enables security teams to focus on the exposures that truly matter while safely deprioritizing the rest.

By reducing noise, clarifying ownership, and providing proof-backed findings, CyCognito supports CTEM programs that interrupt less, prioritize better, and maintain credibility with engineering and business teams.

The outcome is a security program that reduces exposure without becoming the team that cries wolf.

To learn more and see what that looks like in your environment, schedule time with a CyCognito expert using this link.

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 RULE YOUR RISK

SCHEDULE A DEMO →