HORIZON3

Operationalize CTEM with NodeZero®

Turn the CTEM framework into a repeatable operating model

Continuous Threat Exposure Management (CTEM) is ultimately about one outcome: continuously reducing exposure.

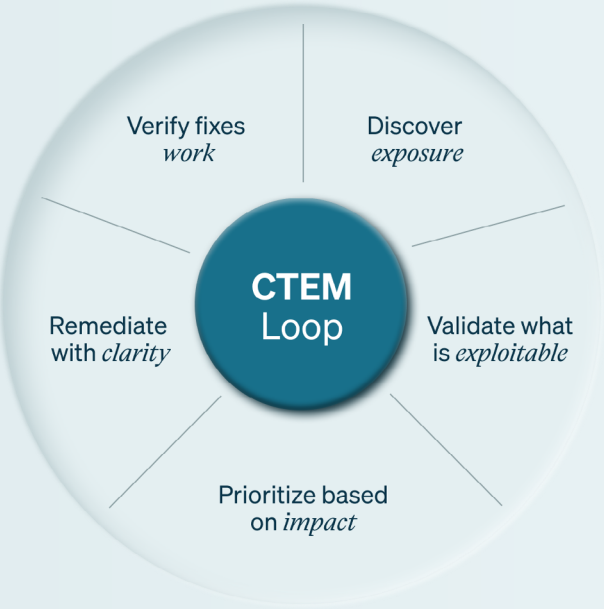
Gartner® defines CTEM through five stages:

Scoping → Discovery → Prioritization → Validation → Mobilization

These stages provide a framework for organizing a CTEM program. They are not five technology categories to fill.

Most organizations already have many of the people, processes, and technologies needed to manage exposure. Vulnerability scanners, EASM, CSPM, threat intelligence, risk scoring, ticketing systems, and remediation workflows provide visibility and support action.

What is often missing is a repeatable way to connect them, determine what attackers can actually exploit, focus remediation where it matters, and verify that the work reduced risk.



The Horizon3 CTEM Operating Loop

Turns the CTEM framework into repeatable action, with the NodeZero® Proactive Security Platform enabling teams to execute it at scale.

Move from visibility to measurable risk reduction

Discovery tells you where exposure may exist. Validation tells you what can actually be exploited. NodeZero safely attacks your environment to uncover exploitable vulnerabilities, misconfigurations, credential weaknesses, and attack paths, giving teams actionable exploit data at scale without disrupting production.

It chains weaknesses together to demonstrate how an attacker could move through the environment, what they could reach, and what they could achieve.

That evidence creates a bias for action. Instead of relying on severity scores, scan data, and assumptions alone, teams can prioritize based on demonstrated exploitability and impact, remediate with greater clarity, and retest to verify that fixes actually removed the risk. Identify what matters. Fix it. Prove it's fixed. Repeat.

See it in action

How NodeZero puts the CTEM Operating Loop into action

1. DISCOVER EXPOSURE

Build visibility across the environment

NodeZero discovers and enumerates assets across the infrastructure, from internal devices and endpoints to internet-facing assets, giving teams visibility into the systems and assets that make up their attack surface. Combined with exposure signals available to the security program, this establishes the coverage needed to determine what is actually exploitable.

Outcome: Build comprehensive visibility across the defined scope.

2. VALIDATE WHAT'S EXPLOITABLE

Replace assumptions with evidence

NodeZero safely tests those assets in production to determine what can actually be exploited, whether weaknesses can be chained together, how far an attacker can move, and what systems, privileges, or data become reachable. It also tests whether security controls are working as intended as attacks progress. Validation turns suspected exposure into evidence of what an attacker can actually do.

Outcome: Know what can be exploited and what an attacker can achieve.

3. PRIORITIZE BASED ON IMPACT

Focus remediation where it matters

Once exposures are validated, NodeZero helps teams prioritize based on what has been proven: the criticality of affected systems, access gained, ability to move laterally, and potential impact to data, operations, or customers.This helps shrink the backlog, giving security and IT teams evidence for what should be addressed first.

Outcome: Focus remediation on exposures proven to create the greatest impact.

4. REMEDIATE WITH CLARITY

Give teams the evidence to act

NodeZero provides evidence of successful exploitation, attack-path context, affected assets, and remediation guidance so teams understand what needs to be fixed and why it matters. This evidence helps inform remediation decisions, align teams around priorities, and give the right owners clear guidance on what needs to be done.

Outcome: Clear ownership and actionable remediation grounded in evidence.

5. VERIFY FIXES WORK

Prove the fix reduced risk

Closing a ticket does not mean the exposure has been eliminated. Instantly retest a single endpoint or the entire scope again with NodeZero to verify that proven weaknesses are no longer exploitable and the associated attack paths have been broken. Verification confirms that remediation changed the outcome, not simply that work was completed.

Outcome: Verified risk reduction instead of assumed remediation.

REPEAT

Environments change. New systems are deployed. Configurations drift. Identities change. New vulnerabilities emerge.

Run the loop on a regular cadence, after major changes, following critical vulnerability disclosures, or in response to incidents. The evidence gained from testing, remediation, and verification can also inform future scoping decisions, helping teams reassess priorities, controls, security investments, and where to focus next.

Continuously run the loop across your entire environment

The operating loop stays the same. What changes is where exposure originates and how attackers can move through the environment.

Attackers do not treat security domains as separate. They move across them wherever access allows. Continuously applying the Horizon3 CTEM Operating Loop across the attack surface helps teams understand exposure in the context of the paths an attacker can actually take.

External Attack Surface ⟷ **Internal Systems** ⟷ **Cloud and Identity** ⟷ **Web Apps** ⟷ **3rd-Party Connections**

Proven results in NodeZero customer environments

94

Attack paths eliminated at a key manufacturing site, removing all network-level compromise scenarios

16

Weaknesses remediated across four compromised hosts, closing the path to AWS compromise

4

Domain compromise paths identified and remediated during M&A due diligence

NodeZero helps you measure whether you're actually becoming more secure.

EXPLOITABLE WEAKNESSES AND ATTACK PATHS OVER TIME

See whether validated exposure is increasing or decreasing across recurring tests.

MEAN TIME TO REMEDIATE (MTTR)

Measure how quickly proven weaknesses move from discovery to remediation.

REMEDIATION AND VERIFICATION STATUS

Track what has been fixed and whether retesting confirmed the fix worked.

RECURRING AND SYSTEMIC WEAKNESSES

Identify issues such as credential reuse and misconfigurations that continue to create exposure across the environment.

EXPOSURE REDUCTION OVER TIME

Show whether remediation is reducing exploitable paths, blast radius, and high-impact exposure.

See NodeZero® *in action.*
horizon3.ai/schedule-demo