Infopercept
INVINSENSE

Buyer's Guide for a Comprehensive CTEM Program

Introduction to CTEM

Organizations today face an increasingly complex and relentless cybersecurity landscape.

Rapid expansion of digital infrastructures

Hybrid workforces

Multi-cloud environments

Constantly evolving threats

make it difficult for security teams to keep up. Traditional methods of vulnerability management have become insufficient, creating a widening remediation gap — the difference between the volume of exposures that need addressing and what security teams can realistically remediate.

As cybersecurity threats grow more complex and pervasive, organizations need more than reactive vulnerability management—they need strategic, continuous protection. Continuous Threat Exposure Management (CTEM) provides a framework that enables proactive risk mitigation by identifying, validating, prioritizing, and remediating exposures in a cyclical and continuous manner.

- Identifying
- Validating
- Prioritizing
- Remediating

As Gartner® puts it

"A continuous threat exposure management (CTEM) programme is an integrated, iterative approach to prioritizing potential treatments and continually refining security posture improvements".

(Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, October 11, 2023)

Developed from Gartner's insights and market best practices, CTEM spans five key stages: Scoping, Discovery, Prioritization, Validation, and Mobilization.

five key stages

- Scoping
- Discovery
- Mobilization
- Prioritization
- Validation

This model aligns cybersecurity activities with real business risk, ensuring the most impactful issues are resolved first.

CTEM programs shift focus from just tracking vulnerabilities to reducing the likelihood of successful cyberattacks. Traditional vulnerability tools alone cannot meet this demand, as they often lack business context, prioritization mechanisms, and real-time adaptability.

Pillars of an Effective CTEM Program

1

Visibility into All Attack Surfaces

Monitor IT, OT, IoT, Cloud, and hybrid environments to discover known and unknown exposures.

2

Prioritized Risk Context

Combine business-critical asset mapping with real-world exploitability to focus on what matters most.

3

Attack Path Mapping

Visualize how attackers can chain vulnerabilities and move laterally through your environment.

4

Validation through Simulations

Test security defenses against adversary behaviors and measure control effectiveness.

5

Actionable Remediation Plans

Provide precise, risk-based recommendations to eliminate high-impact exposures.

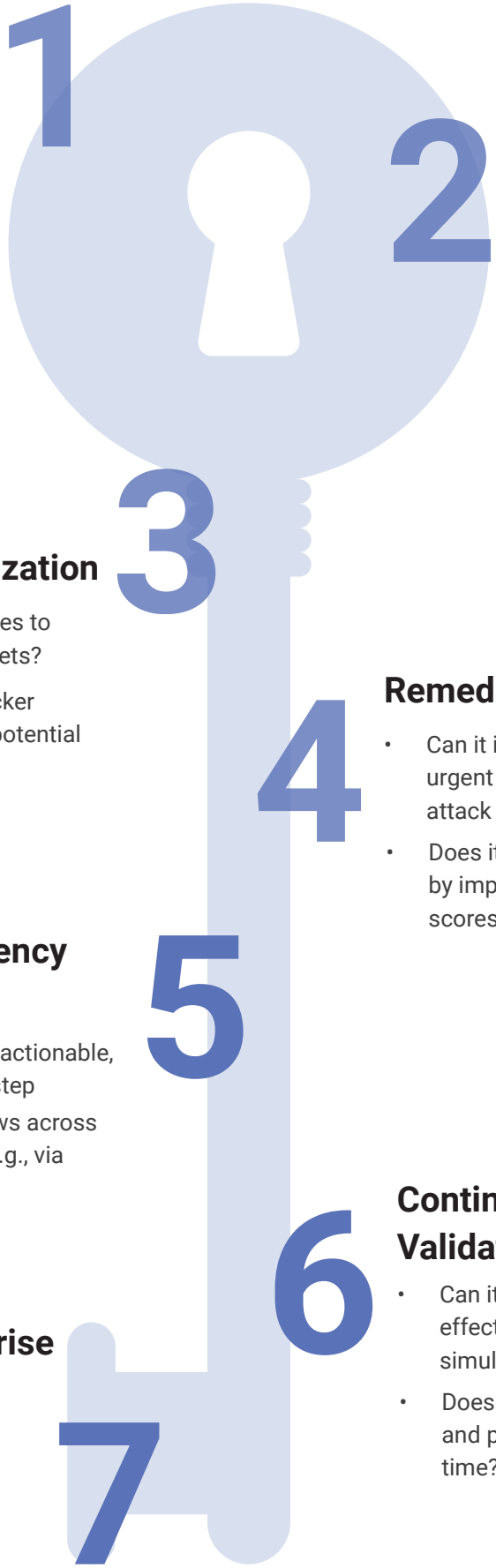
6

Continuous Improvement

Track trends, adapt to new threats, and refine the security posture over time.

Key Capabilities to Look for in a CTEM Provider

To achieve meaningful and measurable outcomes, organizations should evaluate CTEM platforms based on these core criteria:



1 Breadth of Exposure Detection

- Does it identify vulnerabilities, misconfigurations, identity gaps, and excessive privileges?
- Does it go beyond traditional scanning to uncover chained exposures?

2 Environmental Comprehensiveness

- Can it assess risks across cloud, on-prem, remote, containerized, and SaaS environments?
- Does it analyze assets both inside and outside your perimeter?

3 Risk Contextualization

- Does it map exposures to business-critical assets?
- Can it simulate attacker behavior and show potential lateral movement?

4 Remediation Prioritization

- Can it identify the most urgent fixes to block entire attack chains?
- Does it prioritize remediation by impact, not just severity scores?

5 Remediation Efficiency & Assistance

- Does it suggest precise, actionable, and realistic mitigation step
- Does it support workflows across security and IT teams (e.g., via ticketing integrations)?

6 Continuous Security Validation

- Can it validate control effectiveness through simulations?
- Does it track improvements and posture changes over time?

7 Scalability and Enterprise Readiness

- Is it built for large, distributed, hybrid environments?
- Does it deliver executive dashboards, KPIs, and posture trending?

Why Invinsense OXDR is Purpose-Built for CTEM

Invinsense OXDR, developed by Infopercept, is a unified exposure management platform that operationalizes CTEM through an integrated suite of modules designed to discover, validate, and remediate threats in real time.

Invinsense OXDR

Invinsense OXDR's Unique CTEM Capabilities

Exposure Assessment Platform (EAP)

Continuously monitors digital ecosystems — including IT, OT, IoT, and multi-cloud — to detect known and unknown exposures.

1. **Attack Surface Monitoring (ASM)**

   Identifies shadow IT, vulnerable assets, and misconfigurations across the full attack surface.

2. **Vulnerability Management (VM)**

   It brings all the vulnerabilities from external and internal ecosystem and gives one view for all.

Adversarial Exposure Validation (AEV)

Validates all exploitable exposures by simulating and automating red teaming and also attacking humans, processes and machines.

1. **Breach and Attack Simulation (BAS)**

   Simulates realistic threat scenarios and validates whether controls detect and stop them.

2. **Continuous Automated Red Teaming (CART)**

   Automatically emulates real adversary behavior across environments to expose high-risk attack paths.

AI-Powered Threat Intelligence

Incorporates dynamic threat intelligence to contextualize risks and prioritize what matters.

RedOps (Adversary Emulation)

Simulates stealthy attacks to validate detection, response, and mean time to detect (MTTD).

Remediation Orchestration

Integrates with IT ticketing systems (e.g., Jira) to provide step-by-step fixes and streamline workflows.

Posture Dashboards & Reporting

Delivers real-time insights, executive reporting, and security performance metrics.

What is Not a CTEM Program

To clearly understand what Continuous Threat Exposure Management (CTEM) entails, it's equally important to identify what it does not represent. CTEM is not simply a set of isolated security processes or tools, nor is it a one-time assessment activity. Below are common misconceptions:

Not Just a Technology Solution

While CTEM may leverage various tools (such as vulnerability scanners, attack surface management platforms, or security validation technologies), the program itself is not confined to these products. It is a comprehensive, risk-based operational approach involving people, processes, and technologies working in sync.

Not Merely a Compliance Checklist

Although CTEM can support regulatory and security framework compliance, its primary aim is to proactively uncover, assess, and reduce real-world risks—especially those that could be exploited by threat actors. It focuses on reducing exploitable exposure, not just ticking boxes.

Not a Static Process

Threat exposure management must evolve as threat landscapes change. CTEM is dynamic and iterative, adapting to emerging vulnerabilities, business shifts, and evolving attacker techniques.

Not Solely Owned by IT or Security Teams

CTEM is most effective when it involves cross-functional collaboration. Business leaders, IT, and security teams must align to ensure exposures that pose real risk to business outcomes are prioritized and addressed.

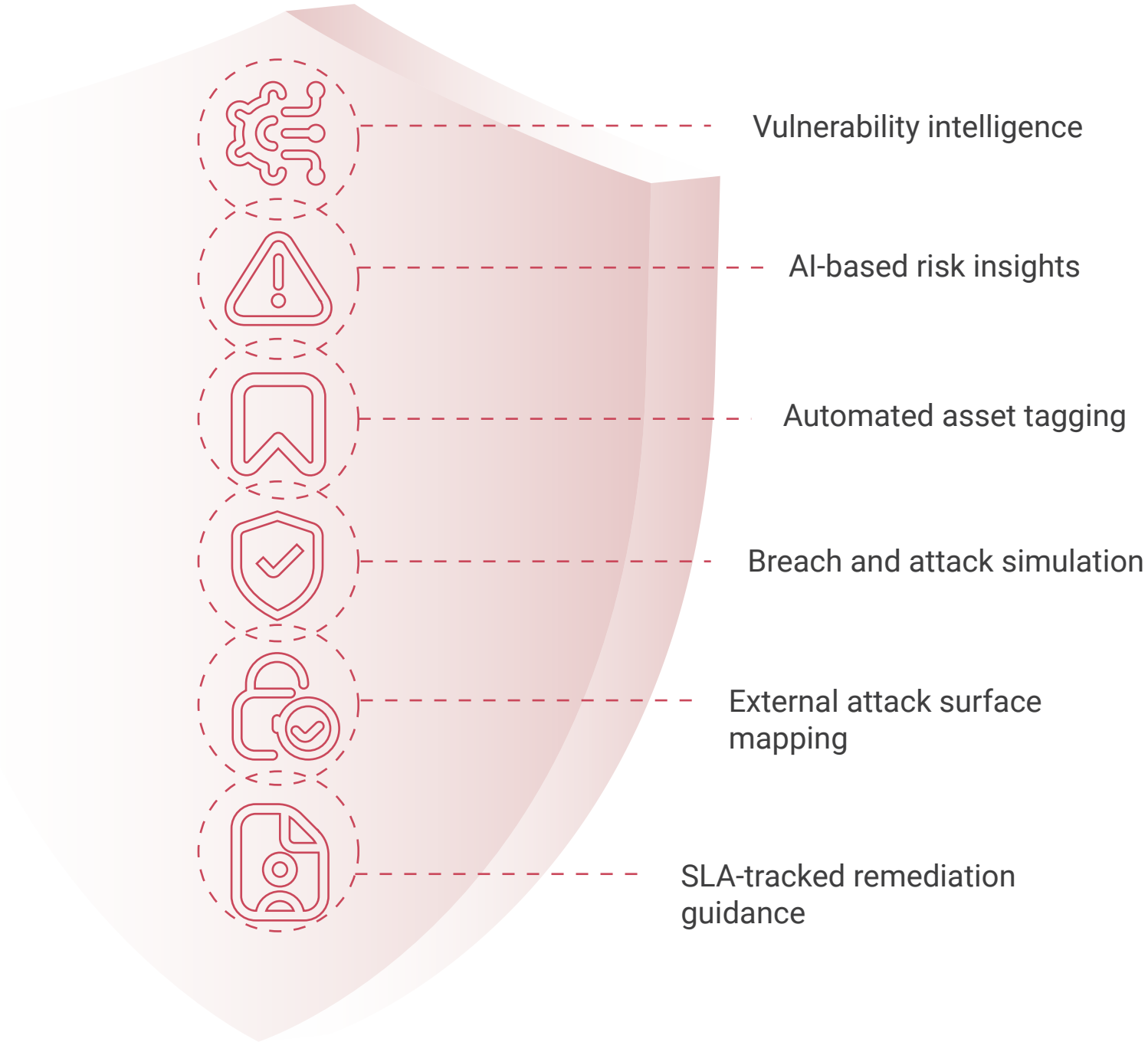
Not a One-Off Penetration Test or Red Team Exercise

CTEM goes beyond occasional testing or red teaming efforts. These methods may offer insights at a point in time, but CTEM requires consistent, ongoing exposure management integrated into operational workflows.

The Role of Invinsense OXDR in CTEM

Invinsense OXDR by Infopercept is a Platform-Led Managed Security framework that enables organizations to unify detection, response, and exposure management. Its modular yet integrated approach helps organizations operationalize CTEM effectively.

With capabilities including vulnerability intelligence, external attack surface mapping, automated asset tagging, breach and attack simulation, AI-based risk insights, and SLA-tracked remediation guidance, Invinsense OXDR is architected to empower every step of the CTEM cycle.



Unlike point solutions that address siloed concerns, Invinsense OXDR offers a unified, correlated view of exposures and threats, allowing organizations to mature their security posture while meeting compliance and executive reporting needs.

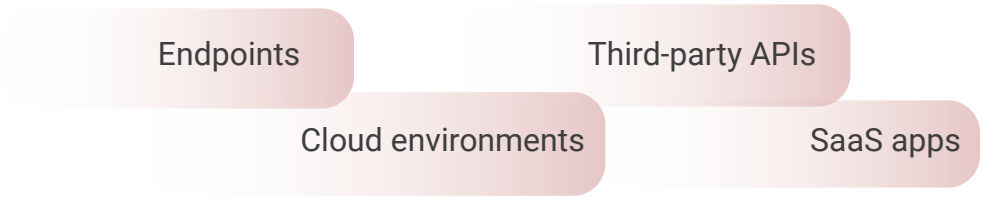
Mapping Invinsense OXDR to the 5 CTEM

Invinsense OXDR aligns tightly with Gartner's five CTEM stages, enabling security teams to continuously evaluate and improve their organization's exposure posture.

1.Scoping

Scoping defines the CTEM initiative's focus. Invinsense enables scoping through advanced asset aggregation, tagging, and contextual prioritization.

It collects metadata across endpoints, cloud environments, third-party APIs, and SaaS apps.



Business impact tagging and role-based criticality assessments help ensure focus on assets with the highest value and risk.

Its visibility into internal and external surfaces allows organizations to start with manageable pilots—like external assets or specific applications—before scaling CTEM efforts organization-wide.

2. Discovery

Discovery involves identifying exposures across the scoped asset set. Invinsense automates this through ASM and Vulnerability Management. The platform is integrated with EASM, vulnerability scanners, secrets managers, and configuration analyzers.

It identifies not just CVEs but also misconfigurations, leaked credentials, over-privileged identities, and misaligned access policies.

This stage also integrates intelligence from cloud security posture, supply chain partners, and custom threat feeds. Invinsense goes beyond internal findings and integrates attacker-view intelligence for complete exposure mapping.

3. Prioritization

Risk-based prioritization is central to CTEM. Invinsense applies EPSS, CVSS, and exploit intelligence to quantify the urgency of exposures.

However, it extends beyond severity scores by factoring in lateral movement potential, asset importance, availability of compensating controls, and real-time exploitability.

- Lateral movement potential
- Asset importance
- Availability of compensating controls
- Real-time exploitability

Invinsense generates dynamic attack path graphs to visualize the impact of remediation actions, enabling teams to identify choke points—where one fix mitigates multiple risks—and avoid wasting resources on low-impact patches.

4. Validation

Validation confirms whether exposures can be exploited and how defenses would react. Invinsense integrates with breach and attack simulation (BAS) and continuous and automated red teaming (CART) platforms, red teaming tools, and pentesting modules to emulate adversarial behavior. These techniques help simulate end-to-end attacks and assess exposure chains, including credential abuse, misconfigured policies, and privilege escalation.

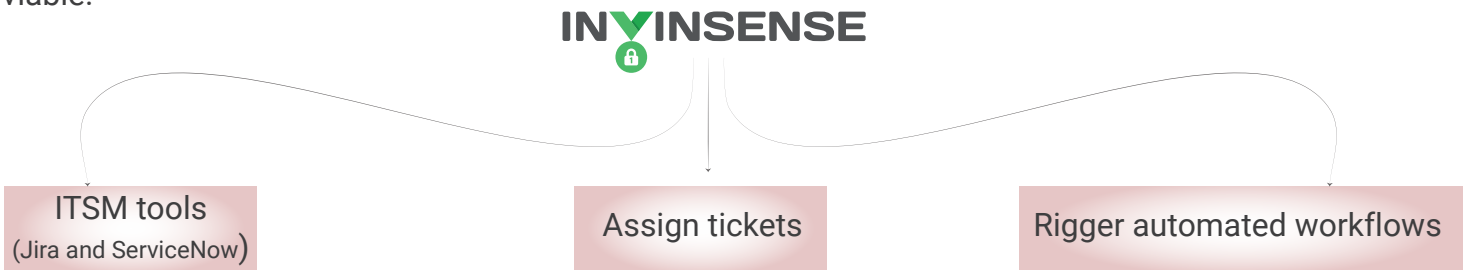
INVINSENSE

- Breach and attack simulation (BAS)
- Continuous and automated red teaming (CART) platforms
- Red teaming tools
- Pentesting modules

This phase also evaluates how security controls and teams respond, thus testing not just technology but also process maturity. Invinsense helps quantify effectiveness and reduce false sense of security.

5. Mobilization

Mobilization ensures CTEM outcomes are operationalized. Invinsense integrates with ITSM tools like Jira and ServiceNow to track remediation SLAs, assign tickets, and trigger automated workflows. Its AI assistant suggests feasible remediation actions and fallback mitigations when a full fix is not viable.



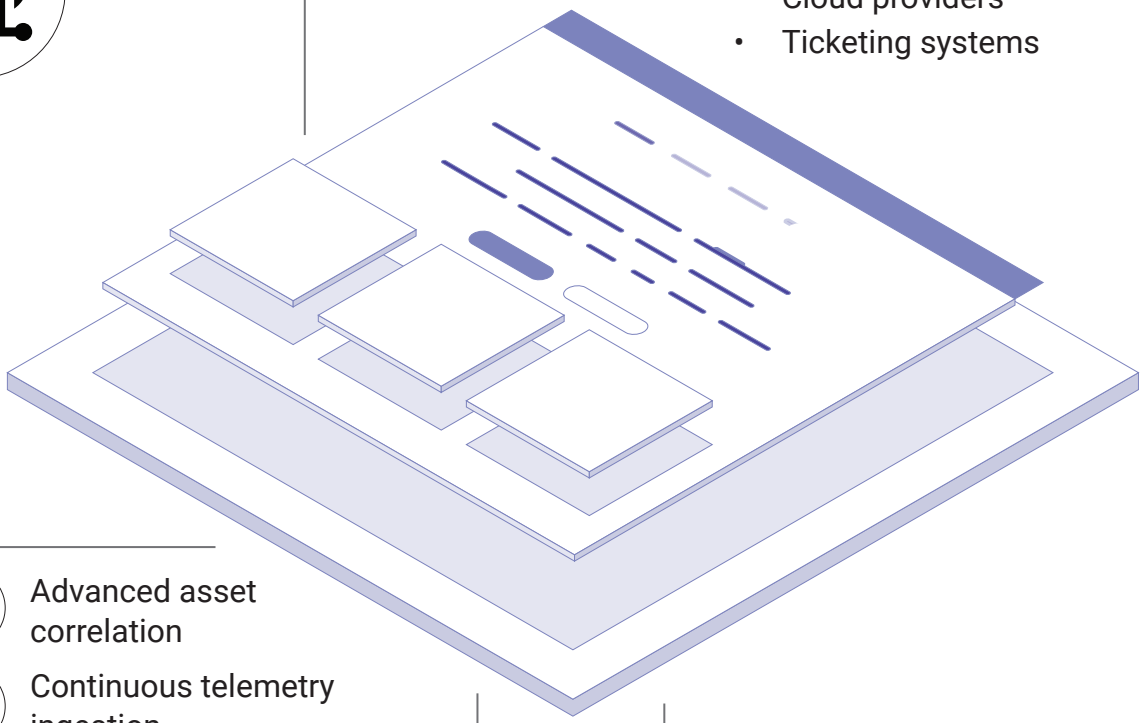
By tracking the life cycle of remediations and offering dashboards aligned with executive KPIs, Invinsense supports cross-functional alignment between security, infrastructure, and business units.

Architecture Overview

Invinsense OXDR offers a modular, API-first architecture designed to seamlessly integrate with existing enterprise tools, cloud environments, and security ecosystems.

It supports bi-directional integrations with

- SIEMs,
- Vulnerability scanners
- BAS tools,
- IAM platforms
- Cloud providers
- Ticketing systems

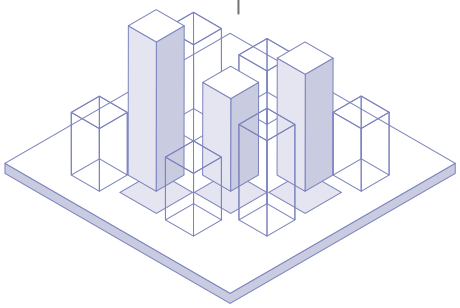


The architecture supports

- Advanced asset correlation
- Continuous telemetry ingestion
- Risk scoring engines
- AI-based remediation guidance

Components include

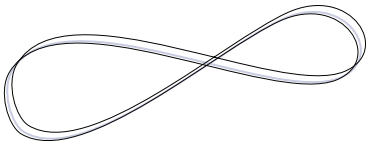
- The Core Intelligence Engine
- Risk Prioritization Service
- Threat Intelligence Gateway
- Exposure Graph Processor
- Compliance Reporting Hub



OXDR leverages XDR-native capabilities to pull threat telemetry directly into the CTEM workflow, facilitating real-time validation and enabling rapid incident-driven reprioritization.

Operationalizing CTEM with Invinsense

Operationalizing CTEM with Invinsense means building a continuous feedback loop between detection, exposure analysis, and remediation.



Security teams use dashboards that visualize exposure trends, SLA breaches, remediation bottlenecks, and business asset risk shifts.

Key CTEM KPIs tracked within Invinsense include:

- Mean Time to Remediate (MTTR)
- Exposure to Critical Assets Ratio
- Posture Improvement Index
- Control Coverage Gaps

Executive views help CISOs align security investments with board-level risk objectives.

The platform also supports automated compliance mapping, enabling organizations to assess posture against ISO 27001, NIST CSF, CIS Benchmarks, and sector-specific regulations.

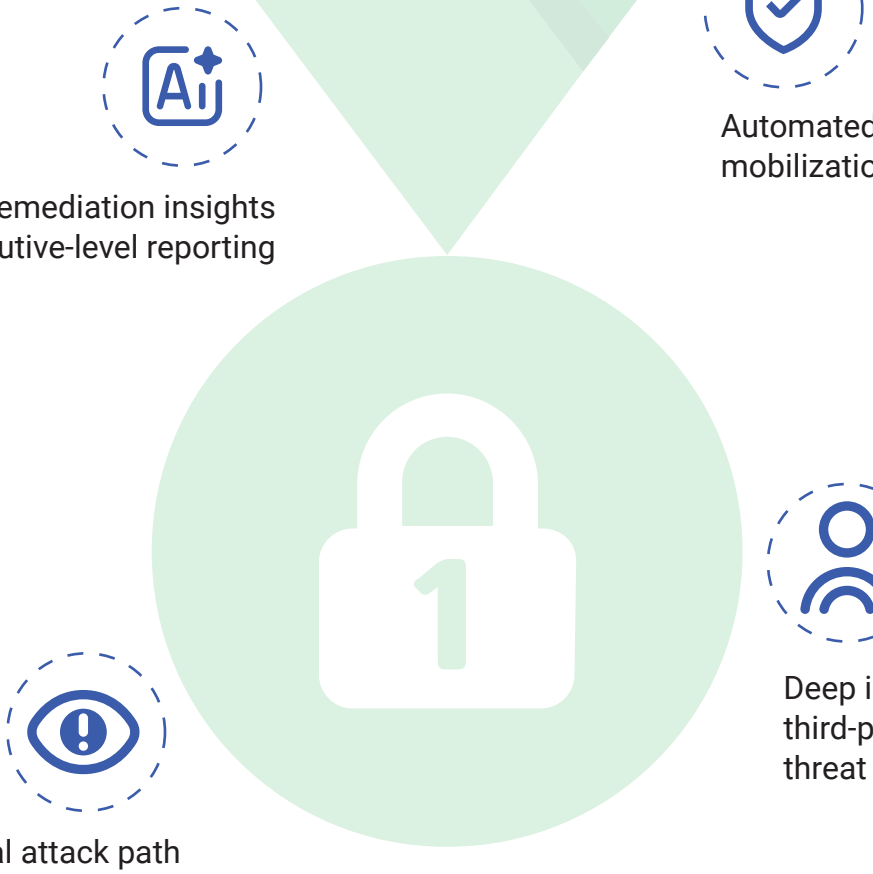
Why Choose Invinsense for CTEM

Invinsense stands out in the CTEM landscape due to its comprehensive, platform-led approach. Key differentiators include:

Unified platform spanning risk discovery to remediation

AI-driven remediation insights and executive-level reporting

Automated, SLA-driven mobilization support



Contextual attack path visualization and business asset risk alignment

Deep integration with third-party tools and threat intelligence feeds

These capabilities make Invinsense OXDR uniquely positioned to deliver CTEM outcomes faster, more accurately, and more sustainably than traditional fragmented toolsets.

Conclusion

CTEM is no longer optional in an era of increasing threat velocity and regulatory scrutiny. Organizations must evolve from reactive patching and vulnerability enumeration to strategic exposure management.

Invinsense OXDR empowers organizations to implement, operate, and mature a CTEM program that aligns with business risk, improves security posture, and supports measurable resilience gains. With built-in integrations, dynamic prioritization, and intelligent mobilization, Invinsense enables security teams to focus on what truly matters—preventing attacks that matter most.

Infopercept

INVINSENSE

Office Address

3rd floor, Optionz Complex
Opp. Hotel Regenta,CG Road,
Navrangpura, Ahmedabad -
380009, Gujarat, INDIA

Contact Detail

www.infopercept.com

sos@infopercept.com

+91 9898857117