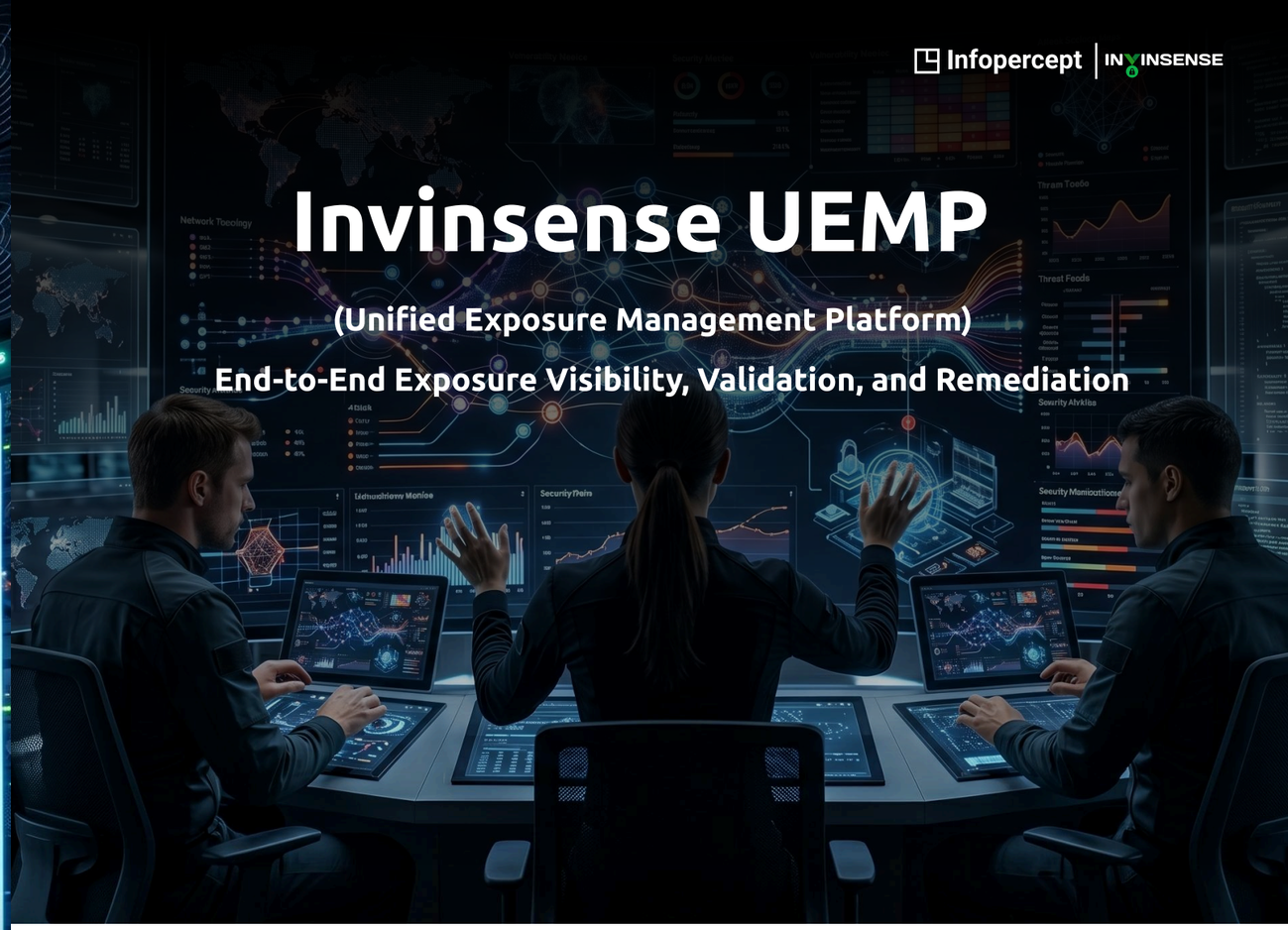
Infopercept | INVINSENSE

Invinsense UEMP

(Unified Exposure Management Platform)

End-to-End Exposure Visibility, Validation, and Remediation



Overview

Invinsense UEMP is a comprehensive, AI-driven Unified Exposure Management Platform designed to provide continuous visibility, prioritization, and validation of exposures across external, internal, identity, application, and human attack surfaces.
It integrates Shift-Left security, External Attack Surface Management (EASM), Adversarial Exposure Validation (AEV), CSPM, phishing simulations, and runtime security into a single, unified platform—while leveraging both native and existing customer tools.

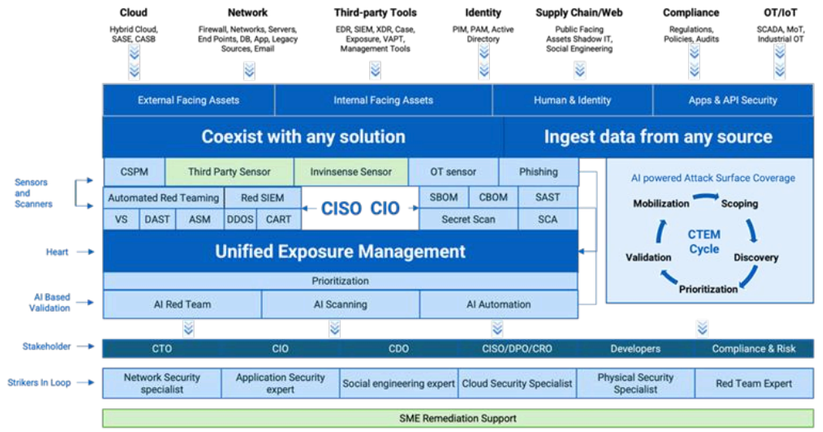
Problem Statement

Organizations today face fragmented exposure visibility due to:

- Multiple tools across AppSec, Cloud, Infra, Identity, and Red Teaming
- Lack of correlation between vulnerabilities, threats, and real exploitability
- Limited validation of whether exposures are actually exploitable
- Siloed teams (Developers, Security, Red Team, Awareness teams)

Result: Unprioritized risks, inefficient remediation, and unclear security posture

Invinsense - Unified Exposure Management Platform



Infopercept

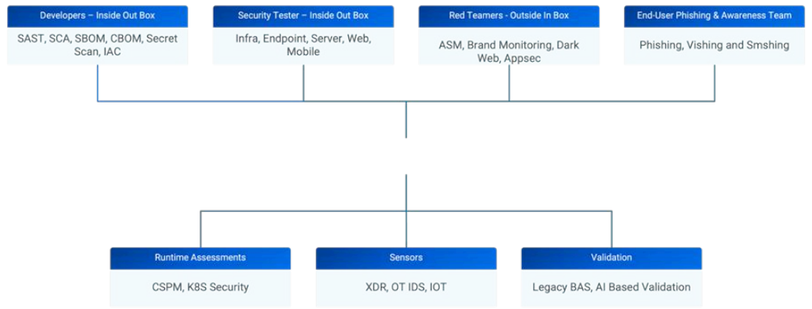
Office Address

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

Contact Detail

www.infopercept.com
sos@infopercept.com
+91 9898857117

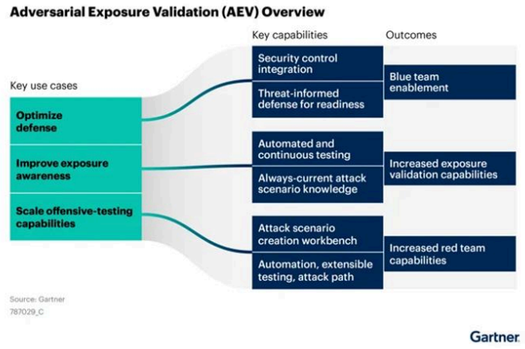
Teams required to support the remediation program - Extended Team



Remediation activities will be supported by specialized teams, with resource allocation determined by the vulnerability volume, severity levels, and the defined scope of the engagement.

2

Figure 1: AEV Market Use Cases



Solution Approach

Unified Exposure Coverage (Inside-Out + Outside-In)

1. Covers all major attack surfaces:
   - External Facing Assets – ASM, Brand Monitoring, Dark Web
   - Internal Assets – Infra, Endpoints, Servers, OT
   - Human & Identity – Phishing, Vishing, Smishing, IAM risks

Shift-Left to Runtime Security

1. Developers (Shift Left):
   - SAST, SCA, SBOM, CBOM, Secrets, IaC scanning
2. Security Testing:
   - Infra, Web, Mobile, Endpoint validation
3. Runtime & Cloud:
   - CSPM, K8s Security
4. Sensors:
   - XDR, OT IDS, IoT monitoring

Adversarial Exposure Validation (AEV)

1. Continuous validation using:
   - Automated Red Teaming
   - AI-driven attack simulations
   - Breach & Attack Simulation (BAS)
2. Aligns with CTEM (Continuous Threat Exposure Management) lifecycle:
   - Discovery → Prioritization → Validation → Mobilization

Unified Exposure Correlation & Prioritization

1. Central engine for:
   - Exposure aggregation across tools
   - Risk-based prioritization
2. Powered by:
   - AI Red Teaming
   - AI Scanning
   - AI Automation
3. Provides context-aware risk scoring

Coexist with Existing Tools (No Vendor Lock-in)

1. Integrates with:
   - Existing scanners, SIEMs, XDRs, and AppSec tools
2. Supports:
   - Third-party sensors + Invinsense-native engines
3. Protects existing investments while enhancing visibility

Flexible Scanning & Validation Engines

1.Supports multiple scanning approaches:
   - Vulnerability Scanners (VA, DAST, SAST)
   - ASM & External Scanners
   - Red Teaming tools
   - Custom & third-party integrations
2. Enables plug-and-play security testing ecosystem

AI-Driven Exposure Lifecycle Management

1. AI-powered capabilities:
   - Attack surface discovery
   - Intelligent prioritization
   - Automated validation
   - Guided remediation
2. Moves towards Autonomous Exposure Management

Remediation & Stakeholder Alignment

1. Aligns across:
   - CISO, CIO, CTO, CDO
   - Developers & DevSecOps
   - Compliance & Risk teams
2. Supported by:
   - SME remediation experts
   - Domain specialists (Network, AppSec, Cloud, Social Engineering, Red Team)

Key Capabilities

Unified Exposure Management Across All Attack Surfaces	Shift-Left + Runtime + External Security in One Platform	Adversarial Exposure Validation (AEV) with AI & BAS	CTEM-Aligned Continuous Security Lifecycle
AI-Powered Prioritization & Validation	Coexistence with Existing Tools (No Vendor Lock-in)	Flexible Scanning Engines (Native + Third-Party)	End-to-End Remediation Support with SMEs

Value Proposition

Complete Visibility Across internal, external, human, and application layers	**Risk-Based Prioritization** Focus on what truly matters	**Validated Security Posture:** Test real-world exploitability
Tool Consolidation Unify multiple exposure and testing tools	**Faster Remediation** Coordinated workflows across teams	**Future-Ready Security** AI-driven and CTEM-aligned