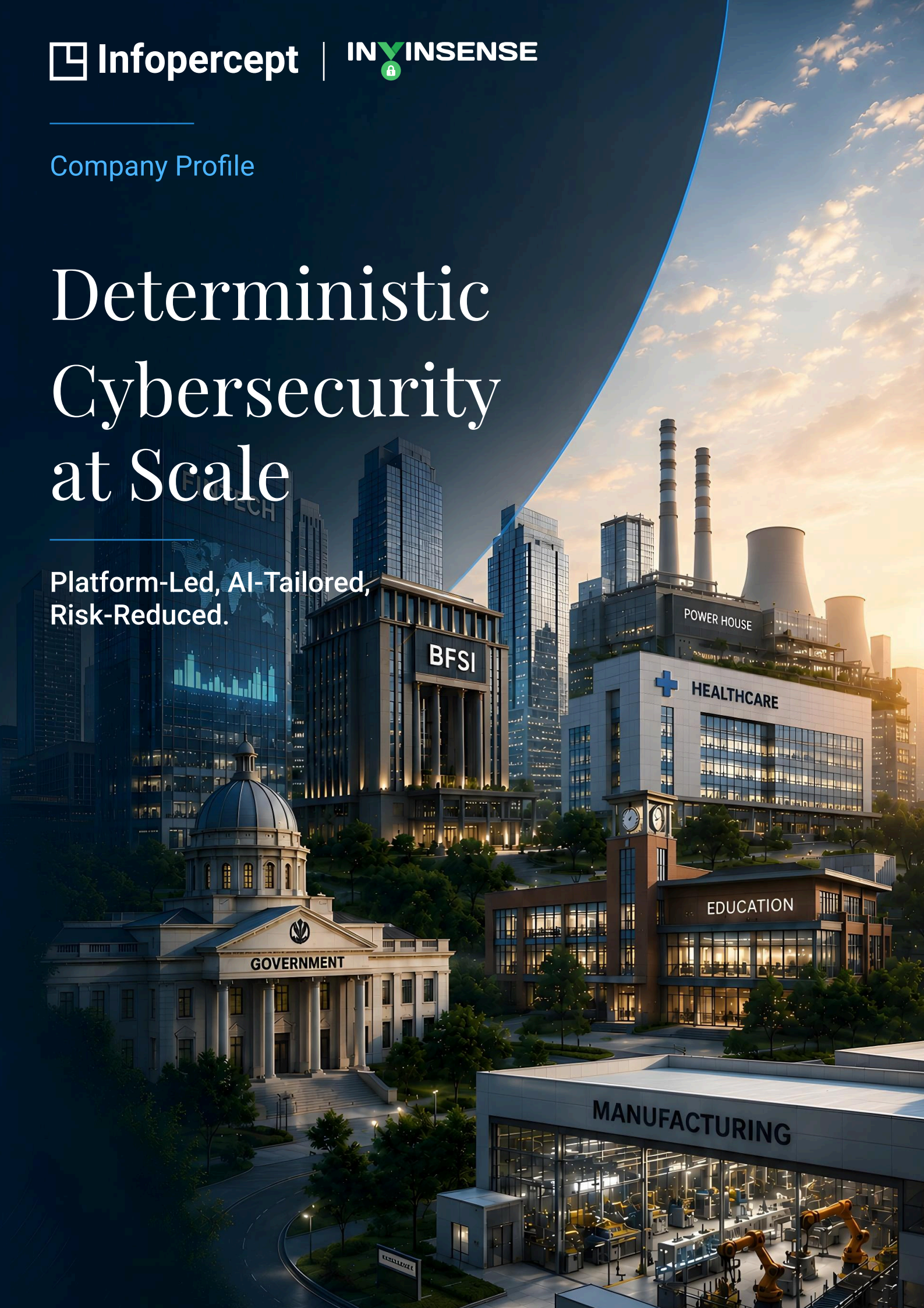
Infopercept | INSENSE

Company Profile

Deterministic Cybersecurity at Scale

Platform-Led, AI-Tailored, Risk-Reduced.



Company Overview

Infopercept is a global, platform-led managed cybersecurity services company that helps organizations reduce real cyber risk — not just deploy more security tools.

Most enterprises already spend heavily on cybersecurity — SIEMs, EDRs, vulnerability scanners, cloud security tools, and GRC platforms — yet still struggle with breaches, fraud, downtime, and audit stress. The problem is not intent or investment.

The problem is fragmentation.

Infopercept was built to fix the economics, execution, and outcomes of cybersecurity by consolidating detection, exposure management, and compliance into a single operating model powered by its proprietary Invinsense platform — with **Regiment AI at its core.**

Regiment AI enables a **controlled and deterministic use of AI**, ensuring cybersecurity decisions are intelligently distributed between **humans, automation, and AI** across offensive, defensive, and compliance functions.

Where traditional security creates dashboards and alerts, Infopercept delivers something boards actually care about:

Risk that is visibly, predictably, and measurably going down.

Company at a Glance

Global

- **Founded** : India (Global-first Cybersecurity Platform)
- **Presence** : US, Middle East
- **Footprint** : Middle East, Southeast Asia, Africa, UK

Core Platform

INVINSENSE

Operating Mode

Coverage

- IT
- Cloud
- OT
- AI
- APIs
- Data
- Identity
- Applications

Primary Buyers

- CISOs & CIOs
- CTOs
- CDOs
- Risk & Compliance Leaders

Partnerships

- Strategic partnerships with global technology vendors and regional distributors
- AWS marketplace, Global ISV and cloud ecosystem integrations

Mission

To unify offensive, defensive, and compliance cybersecurity to reduce real cyber risk.

Vision

To make cybersecurity simple, reliable, and outcome-driven for every organization.

Approach

Data first. Automation where repeatable. AI in a controlled manner.

Leadership & Culture

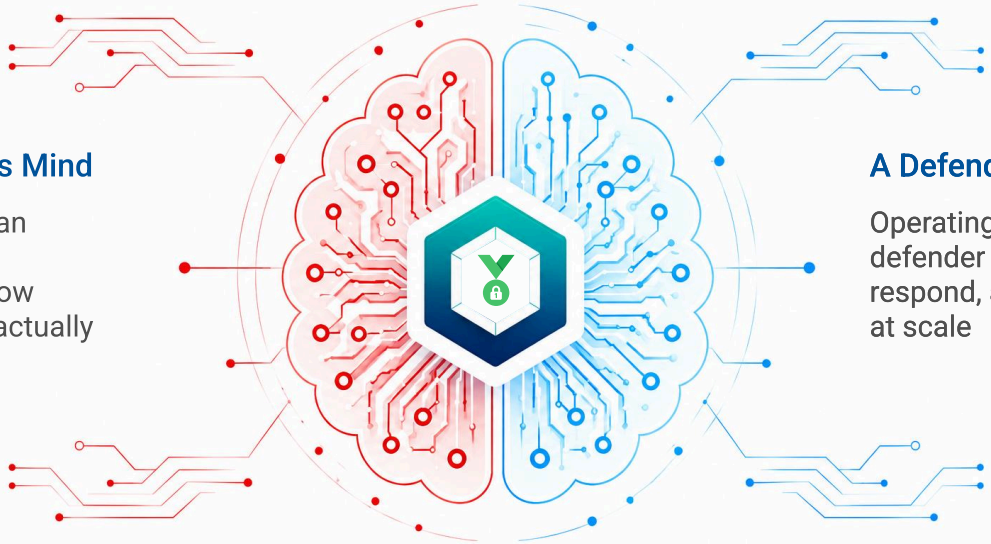
Infopercept thrives on a culture of **accountability, clarity, focus and adaptability**, aligning its teams with a shared mission to protect clients and innovate relentlessly.

The leadership combines deep cybersecurity experience with a forward-thinking approach that anticipates threats rather than merely reacting to them.

The Infopercept Philosophy

"Cybersecurity with an attacker's mind and a defender's brain."

Infopercept believes effective cybersecurity requires:



An Attacker's Mind

Thinking like an adversary to understand how systems will actually be breached

A Defender's Brain

Operating like a defender to detect, respond, and recover at scale

A Regulator's Governance

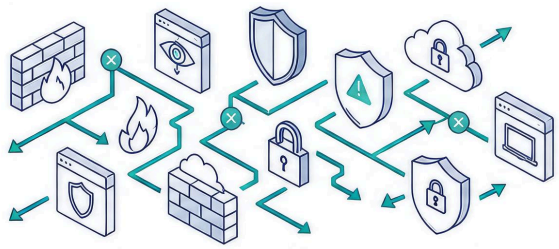
Governing like a regulator to ensure compliance, auditability, and trust

"This philosophy drives entire platform including modules, service, and decision across the company."

The Reality Organizations Face Today

Across industries, Infopercept sees the same structural problems:

Tool Sprawl Without Risk Clarity



- 15-43 security tools deployed
- Each tool works in isolation
- No unified view of “what actually puts the business at risk”

Results : High spend; Low confidence

Too Much Noise, Too Little Context

- Thousands of alerts
- CVSS scores without business relevance
- Security teams chasing symptoms, not attack paths

Results : Alert fatigue; Delayed response.

Annual Security Is Failing Continuous Attacks

- Audits, VAPT, and compliance done once or twice a year
- Attackers operate continuously

Results : Controls look good on paper, fail in practice; Remediation is the ever growing no ownership problem.

Cybersecurity Is Hard to Defend in the Boardroom

- CISOs forced to explain cyber risk in technical language
- Boards think in terms of money, downtime, and regulation

Results : Budget friction and credibility gaps; Regulators are equally tough to handle

How Infopercept Addresses These Challenges

Infopercept replaces fragmented security with a **single, measurable cybersecurity operating model.**

Customers can say

Instead of:

“We have many tools and alerts”

“Our attack surface reduced by

86%

This year and we were able to remediate critical exposures”

This shift is enabled by Invinsense.

Infopercept Security Operations Model - SWAS

Software With A Service (SWAS)

Infopercept delivers cybersecurity as a continuous program, not a one-time deployment:

Detect » Validate » Fix » Verify » Repeat

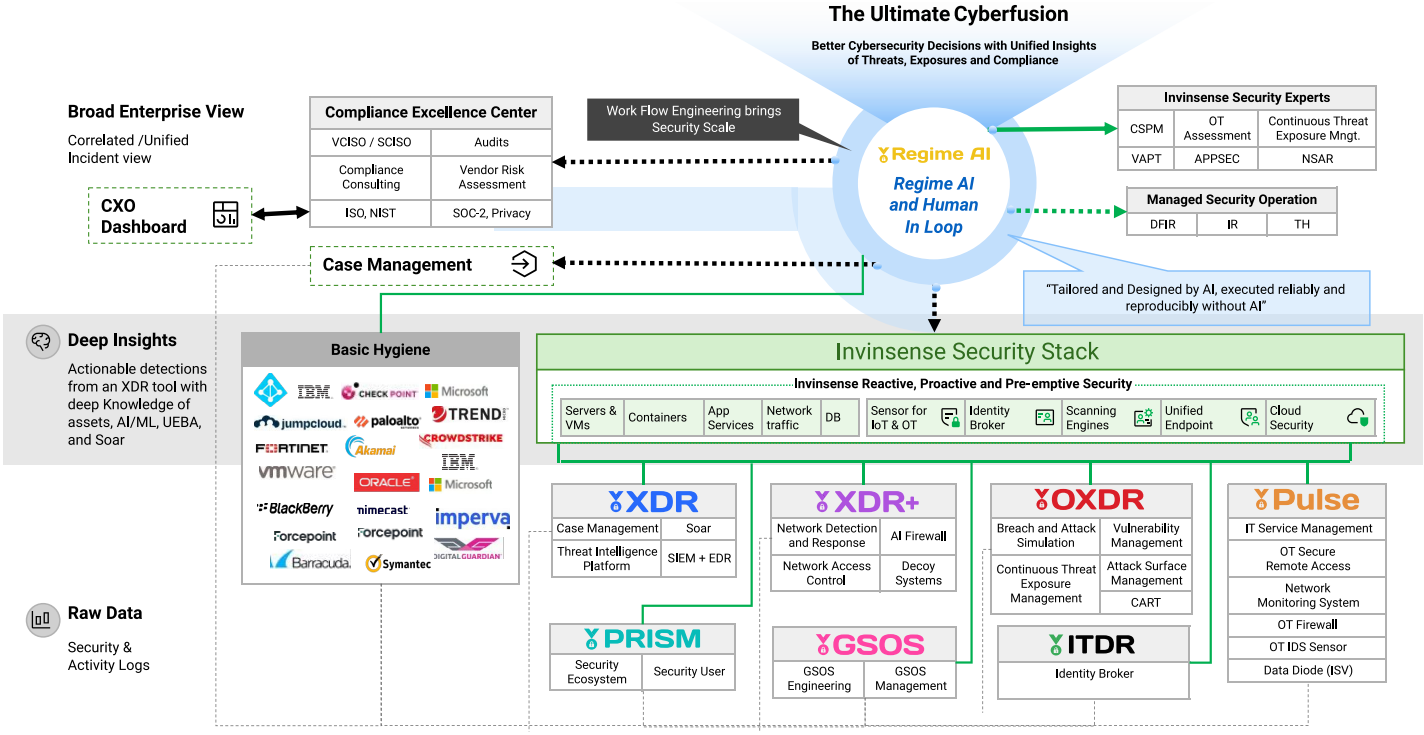
This operating model combines:

Platform Intelligence (Invinsense)	Manage Detect and Response (MDR)	Continuous validation (CTEM)	Continuous Compliance	24×7 expert-led execution (Managed Services)

Security becomes **repeatable, provable, and resilient** — not dependent on individuals or heroics.

The Invinsense Platform

Invinsense is a unified cybersecurity operating system that consolidates 25+ capabilities into a single platform — enabling data-driven, repeatable automation, and controlled AI-led security outcomes.



1. Unified Asset Lake: The Foundation of Context

What it Enables from existing sources

Complete Visibility
See all assets, identities, applications, and infrastructure in one place from existing investments

Context-Rich Intelligence
Understand relationships, dependencies, and integration with exposure sensors

Single Source of Truth
Eliminate data silos across offensive, defensive, and compliance functions

Business Outcomes

Reduced Blind Spots
Nothing critical is missed or unmanaged

Faster Response
Teams act quickly with full context

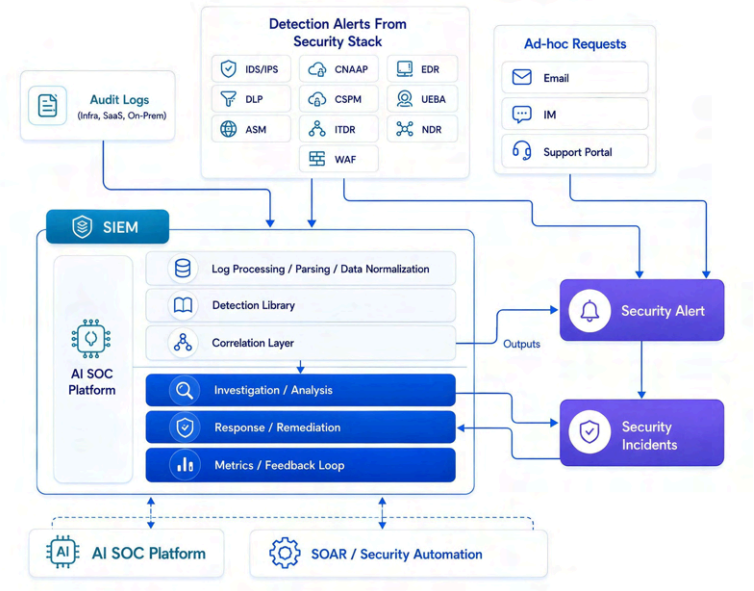
Accurate Risk Prioritization
Focus on what actually reduces risk

Improved Compliance Readiness
Consistent, audit-ready data across controls

Measurable Risk Reduction
Security efforts directly impact real risk

2. Invinsense Security Lake

Next-Gen SIEM + MDR +Security Data Lake in One Unified Platform



Outcome

- Invinsense Security Lake with OCSF converter
- Agentic AI for prioritization and reporting
- Invinsense LLM Gateway for AI access control & cost governance
- Extensible workflows for custom remediation

40–60% ↑ (MTTD) faster detection

55–70% ↑ (MTTR) faster response

Reduced downtime, fraud, and breach impact

Detect and respond before damage occurs

SIEM, SOAR, EDR, UEBA, NDR, Deception, AI Firewall, Threat Intelligence, Case Management

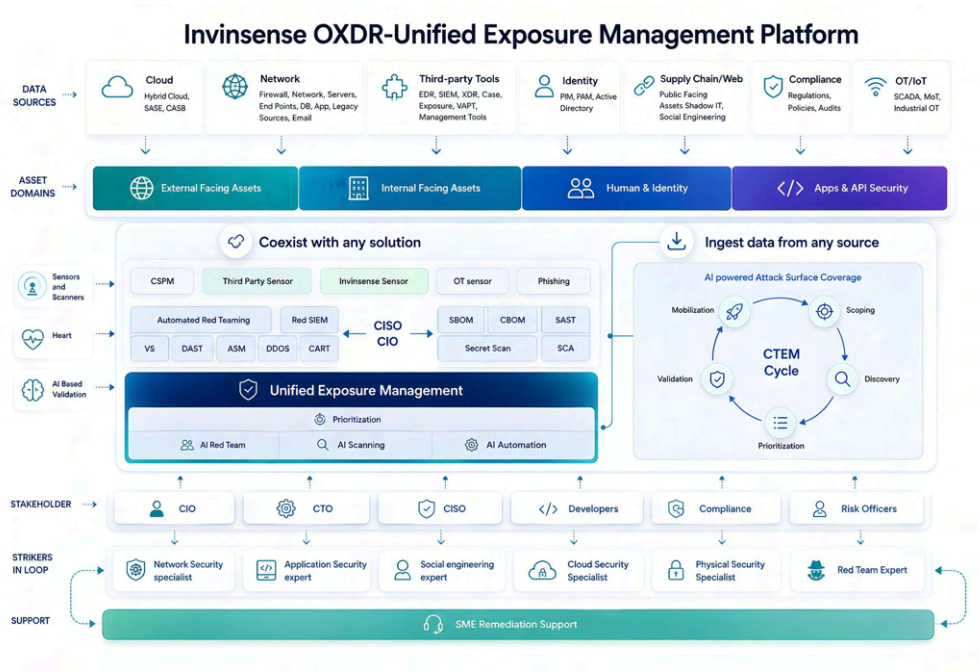
MITRE ATT&CK–mapped detections

Adaptable Workflows

Agentic AI-driven correlation and attack narration

24×7 Real MDR operations

3. Invinsense OXDR – Continuous Threat Exposure Management (CTEM)



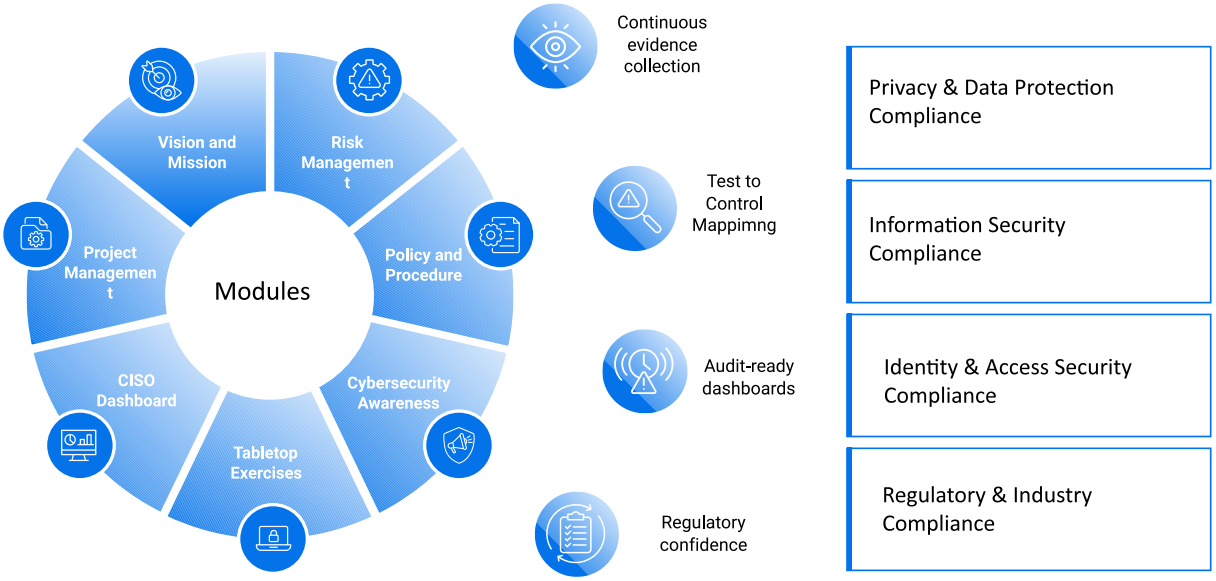
Prevent attacks by removing paths attackers actually use

- Unified Exposure Management
- Attack Surface Management
- Breach & Attack Simulation
- Continuous Automated Red Teaming
- Business-context exposure scoring
- Remediation

Measured Outcomes

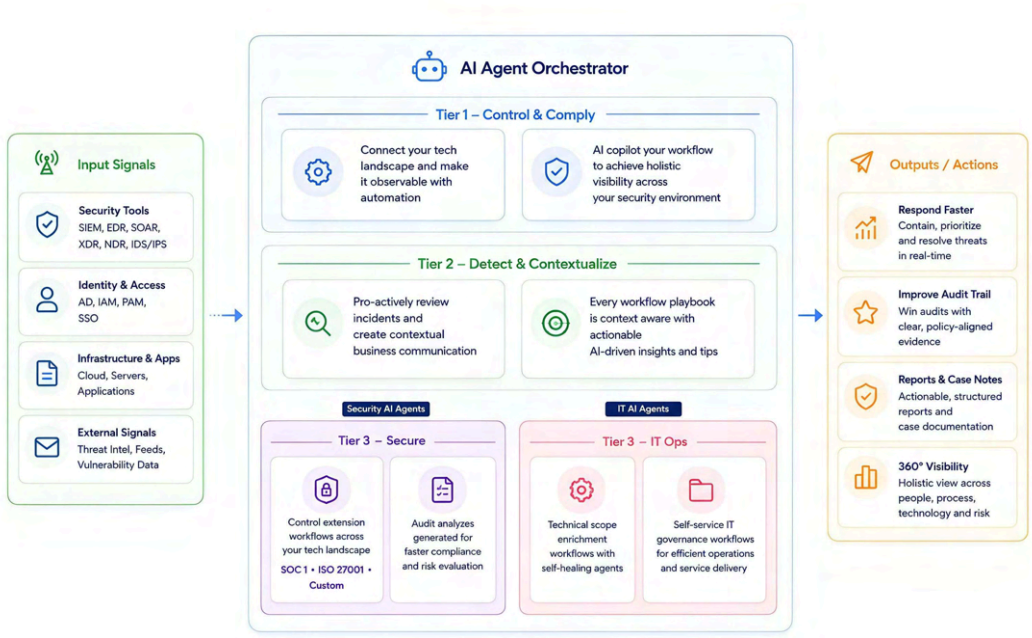
- ~76% average reduction in exploitable exposures in 3 CTEM cycles
- Attack surface reduced and critical vulnerabilities remediated, not just vulnerabilities listed

4. Invinsense GSOS – Governance, Risk & Compliance



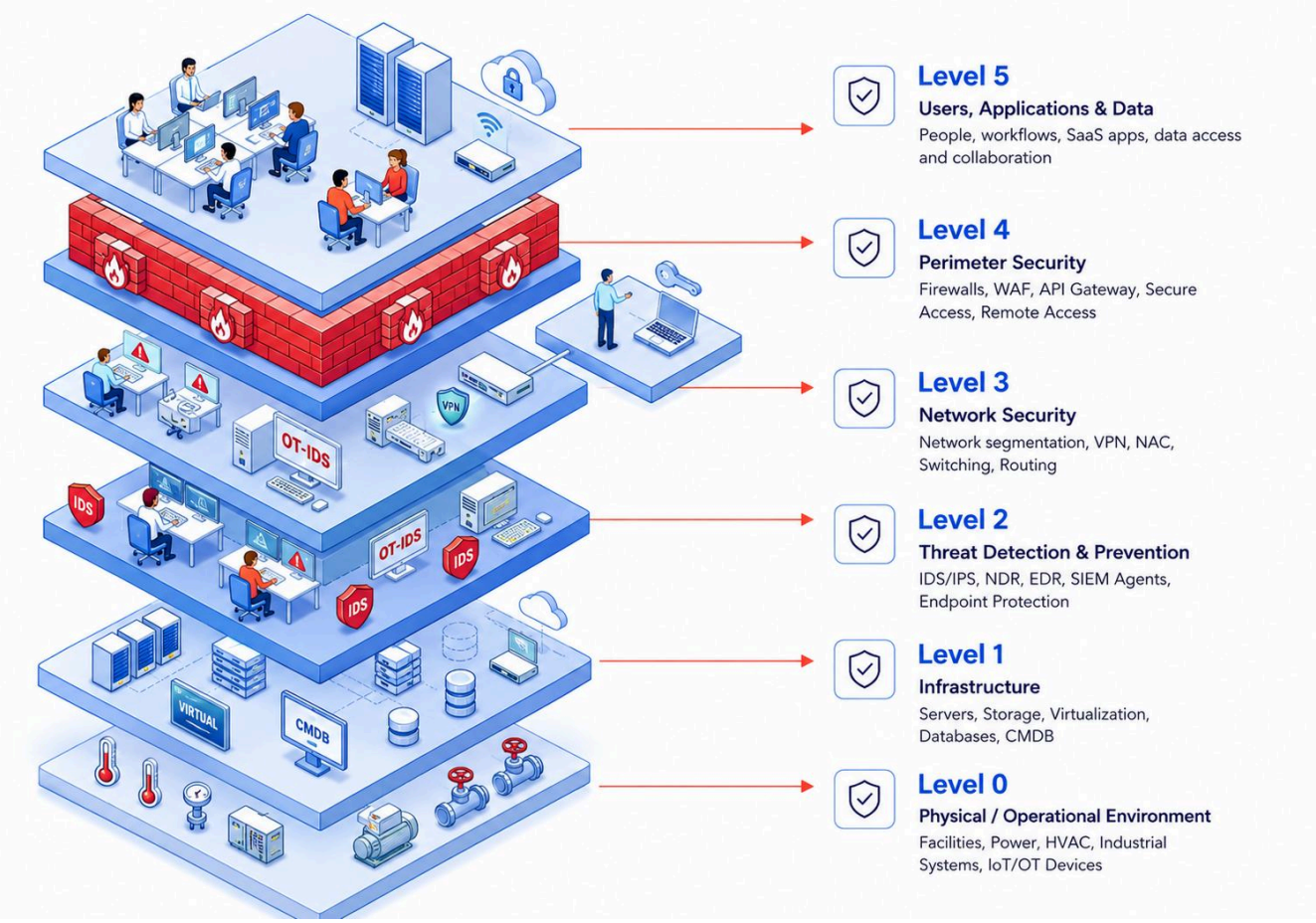
Compliance as a byproduct of security, not a fire drill	Outcome
• Continuous control validation • Automated evidence collection • Control mapping • Regulator-ready reporting (RBI, SEBI, IRDAI, SAMA, ISO, HIPAA, DPDPA, GDPR etc.)	• Lower audit effort • Faster regulatory response • Stronger legal defensibility

5. Regiment AI: Controlled Intelligence. Deterministic Execution. Measurable Outcomes



Benefits	Outcome
Focused Use of AI Applied only where it adds value, eliminating unnecessary noise **Context-Aware Decision-Making** Combines detection, exposure, and compliance for better prioritization **Structured, Actionable Intelligence** No raw or inconsistent outputs, only validated insights **Deterministic Execution** Policy-driven, predefined workflows ensure consistency **Clear Operating Model** Defined roles for humans, automation, and AI **Full Auditability** Every decision and action is traceable and compliant	**Faster, More Accurate Decisions** Reduced false positives and better focus on real threats **Reduced Alert Fatigue** Less noise, more meaningful actions **Predictable Security Operations** Consistent and reliable execution every time **Lower Operational Risk** Controlled AI and structured automation minimize errors **Audit & Compliance Readiness** Fully explainable and verifiable actions **Board-Level Confidence** Clear, measurable, and accountable security outcomes **Real, Measurable Risk Reduction** Security efforts directly reduce cyber risk

6. Unified OT Security Stack: Key Benefits & Outcomes



Benefits

End-to-End OT Visibility
Monitor networks, assets, and activities across the entire OT environment

Integrated Protection Layers
Firewall, access control, detection, deception, and monitoring working as one system

Secure Remote Access
Controlled, monitored, and policy-driven access to critical OT systems

Early Threat Detection
IDS and deception identify threats before they impact operations

Centralized Intelligence (OT SIEM)
Correlates events across all layers for better decision-making

Reduced Complexity
One unified platform instead of multiple disconnected tools

Outcome

Reduced Risk of Disruption
Minimized chances of production downtime or operational impact

Faster Threat Detection & Response
Early signals and correlated insights enable quick action

Improved Operational Continuity
Stable and secure industrial operations

Lower Attack Surface
Controlled access and layered defenses reduce exposure

Audit & Compliance Readiness
Centralized logs and controls support regulatory requirements

Cost Efficiency
Reduced tool sprawl and simplified operations

Measurable Risk Reduction in OT Environment
Security directly improves reliability and safety

Infopercept Real MDR Services

Managed Detection & Response

- 24×7 monitoring and triage
- Automated containment and response
- Industry-specific playbooks

Managed Risk & CTEM (OXDR)

- Continuous exposure discovery, validation, remediation & verification
- Board-visible risk reduction metrics

Managed Compliance & GRC (GSOS)

- Continuous compliance visibility
- Audit readiness by design

Incident Response & Digital Forensics

- Rapid containment
- Root cause analysis
- Business recovery support

Industries We Serve – Proven in Real Attacks

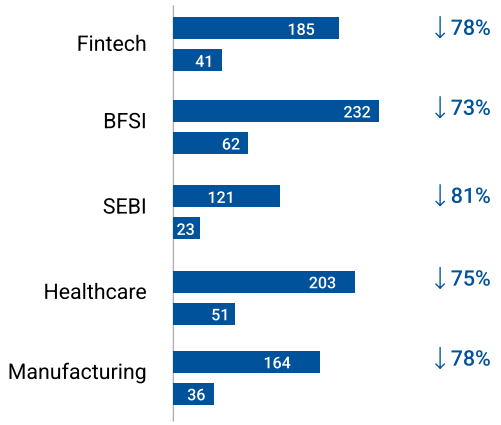
(Derived from attacks combated + CTEM cycles)

BFSI	Fintech & Neo-Banking	SEBI / Capital Markets	Healthcare	Manufacturing & OT
73%	78%	81%	75%	78%
CTEM: 232 → 62 exposures (↓73%)	**CTEM:** 185 → 41 exposures (↓78%)	**CTEM:** 121 → 23 exposures (↓81%)	**CTEM:** 203 → 51 exposures (↓75%)	**CTEM:** 164 → 36 exposures (↓78%)
Threats: Application & API Threats, BEC, ransomware pivots, cloud data theft	**Threats:** ATO, API abuse, silent fraud, Application & API Threats	**Threats:** Trading manipulation, research theft	**Threats:** Ransomware, vendor misuse, PHI theft	**Threats:** IT–OT ransomware pivots
Outcome: Core banking protected; fraud blocked pre-execution	**Outcome:** 90% fraud reduction; zero financial loss	**Outcome:** Market integrity preserved	**Outcome:** 15,000+ records protected; zero downtime	**Outcome:** Production continuity maintained

Visual Summary – CTEM Heatmap (Board View)

Exposure Reduction Across 3 CTEM Cycles

CTEM Exposure Reduction (Cycle 1 vs Cycle 3)



Board Interpretation:

- Attack surface is shrinking
- Risk is measurably trending down
- Controls are working

Visual Summary – Cross-Industry Attack Heatmap

CTEM Exposure Reduction (Cycle 1 vs Cycle 3)

	Fintech	BFSI	SEBI	Healthcare	Manufacture
Identity / ATO	🔴	🔴	🔴	🟠	🟡
API Abuse	🔴	🔴	🔴	🟠	🟠
Data Exfiltration	🔴	🔴	🔴	🔴	🟠
Cloud Misconfig	🔴	🔴	🟠	🟠	🟠
Lateral Movement	🟠	🔴	🟠	🟠	🔴
OT Exposure	🟡	🟡	🟡	🟡	🔴

Key Insight

- Identity + APIs are the new perimeter across all industries.

Infopercept Security Teams

Infopercept operates as an extension of the customer's security team — not a tool vendor.

Infopercept operates as an extension of the customer's security team — not a tool vendor.

By the Numbers

25 security capabilities in one platform

500+ MITRE ATT&CK–mapped detections

25 subject-matter experts

INSENSE Platform

Risk Reduction	Operational Velocity	Financial Efficiency
76% average exposure reduction in 12 months	**40–60%** Faster Detection **55–70%** Faster Response	**40–60%** lower total cybersecurity spend **5×–10×** return on security investment (ROSI)

The Infopercept Difference

Others manage alerts.
Infopercept manages cyber risk.

The Status Quo	The Infopercept Standard
❌ Tool-first	Platform-first, not tool-first
❌ Others manage alerts	Offensive + Defensive Security + Compliance unified
❌ Periodic Pen Testing	Continuous validation through CTEM
❌ Rip-and-replace mandates	No rip-and-replace — complements existing investments
❌ Hyper-technical jargon	Cybersecurity explained in business language

The Infopercept Promise

Infopercept does not promise perfect security.

It promises:

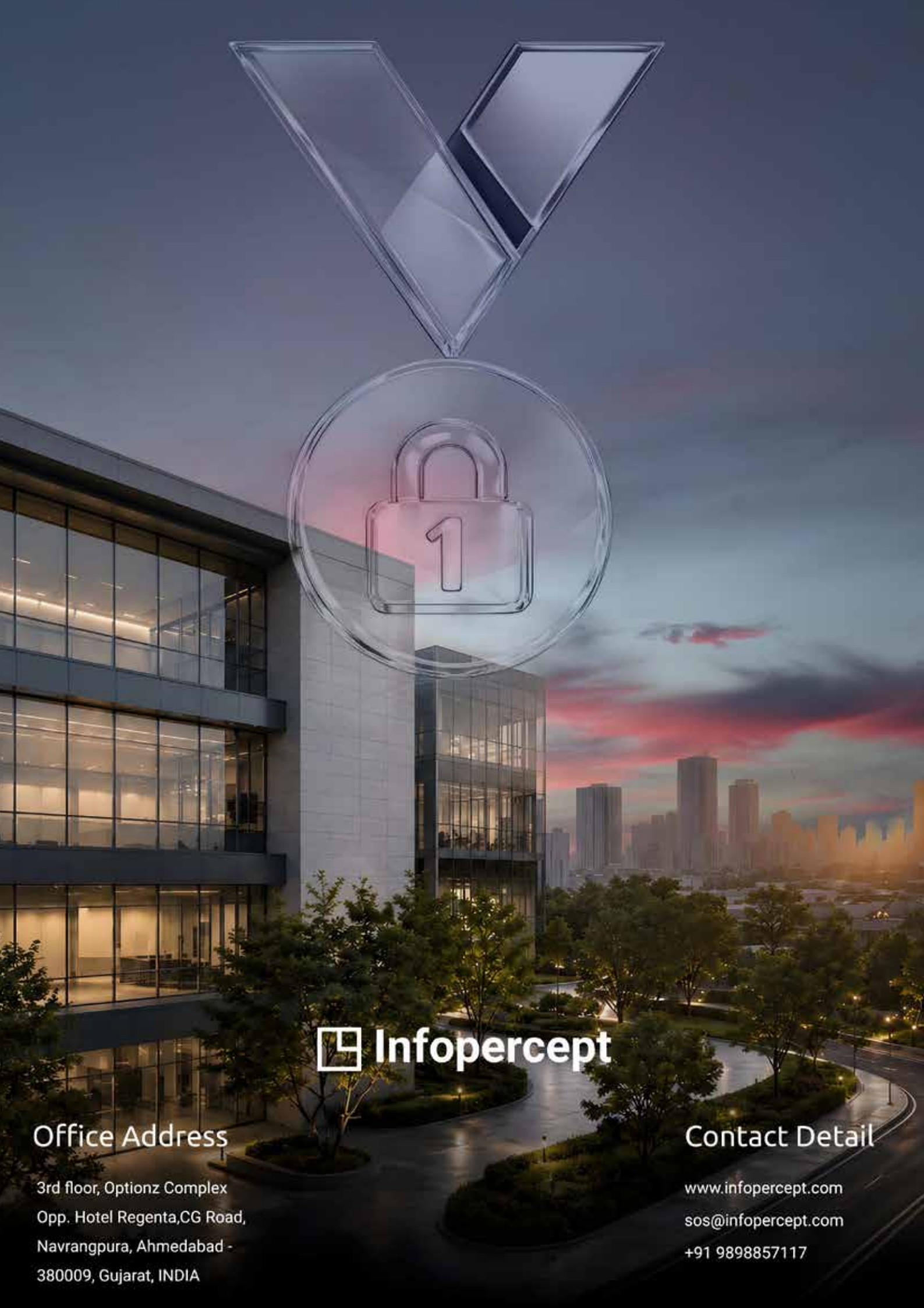
Fewer paths to money

Fewer paths to data

Fewer paths to downtime

Every CTEM cycle, every response, and every board report is designed around one goal:

Making cyber risk smaller, measurable, and explainable.



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