Infopercept

INSENSE

The Ultimate Buyer's Guide to Real MDR

Redefining Managed Detection and Response for the Modern Cybersecurity Era

Table of Contents

Executive Summary

Cyber threats have evolved, and so must our defenses. Traditional MDR offerings—while useful—are limited to reactive incident response and passive threat monitoring. In contrast, Infopercept's Real MDR solution goes far beyond by offering a consolidated and integrated platform that merges detection, response, proactive exposure reduction, remediation, and compliance into a single service. Powered by the Invinsense platform, Real MDR is not just a tool—it's an ecosystem for cyber resilience.

The Evolution of MDR: From Reactive to Proactive

MDR originated as an extension to managed security services, with a focus on detecting anomalies and alerting clients about suspicious activity. However, today's threat landscape demands:

Proactive identification of exposures

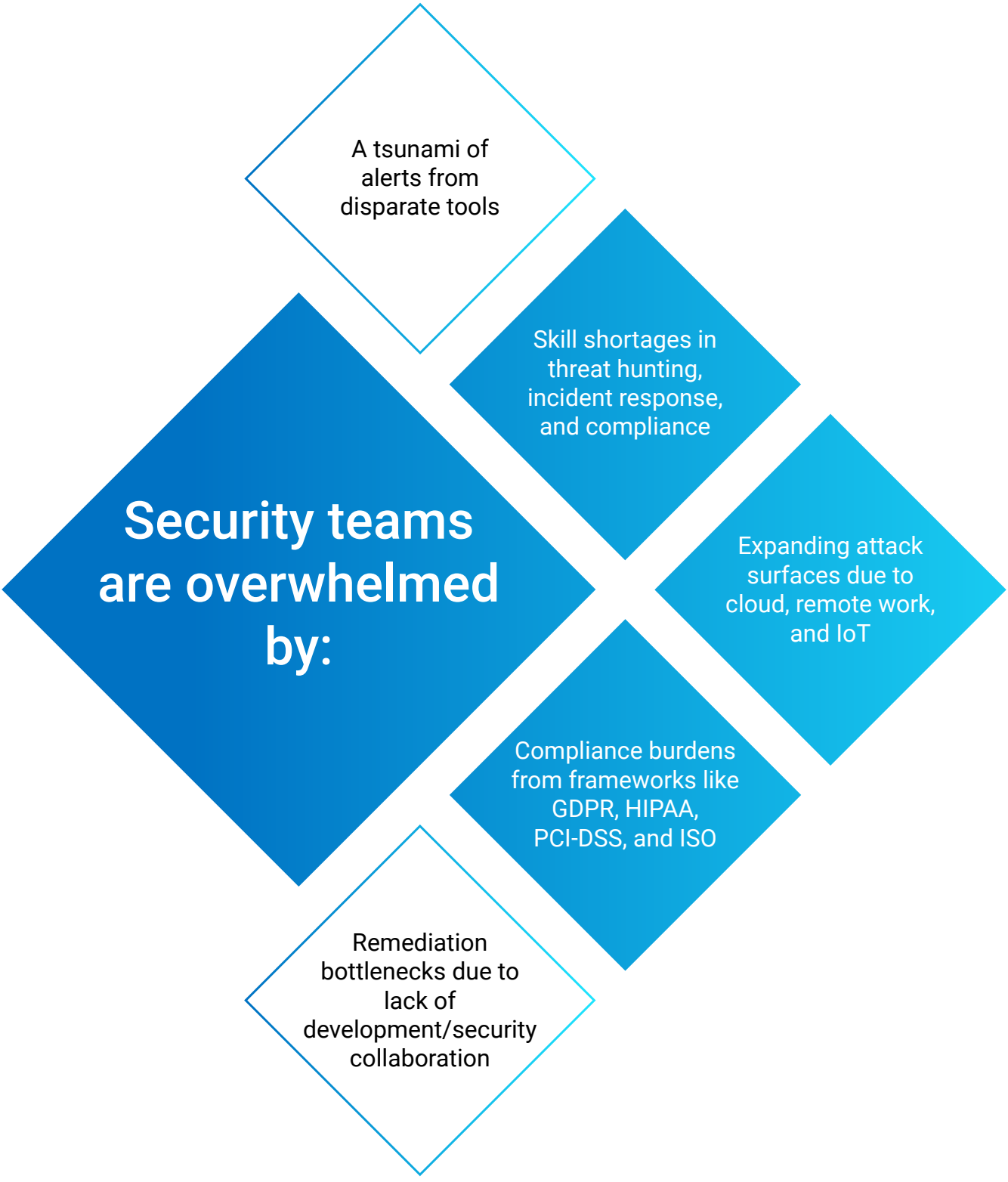
Validation of controls

Integrated compliance oversight

Engineering-level remediation of vulnerabilities

Real MDR is the natural evolution that combines these demands into one seamless model.

Key Challenges Facing Security Leaders Today



Traditional MDR providers only scratch the surface of these problems.

The Need for Real MDR

Real MDR was built to address security in its entirety, not just detection

Need	Real MDR Capability
Reduce exposure before a breach	Continuous Threat Exposure Management
Rapid response to live threats	XDR + Deception + SOAR
Maintain regulatory posture	Built-in GRC/Compliance Layer
Fix root causes	Security Engineering Support
Visibility across hybrid environments	Unified Platform (SIEM, SOAR, EDR, ASM, VM, GRC)

Overview of Infopercept's Real MDR Solution

Infopercept's Real MDR, launched in 2025, is a service-based solution delivered via the Invinsense platform. It spans:

- XDR & deception-led detection and response
- CTEM (Continuous Threat Exposure Management) via Invinsense OXDR
- Security Compliance Management via Invinsense GSOS
- Security Engineering Support for real-world remediation at the system and application level

Key Components of Real MDR

6.1 Detection & Response

- Invinsense XDR: Aggregates telemetry from endpoints, servers, cloud, and networks; correlates with threat intelligence; surfaces prioritized threats.
- Deception Technology (XDR+): Deploys traps and lures to catch attackers that bypass traditional defenses.
- Automated & Manual Response: Orchestrated playbooks and 24x7 human support.
- Threat Intelligence Feeds: Integrated with Invinsense for timely detection of evolving threats.

6.2 Exposure Management (Invinsense OXDR)

Attack Surface Monitoring (ASM): Inventory and monitor internet-facing assets.
Vulnerability Management (VM): Prioritize risks based on exploitability and business impact.
Breach & Attack Simulation (BAS): Continuous validation of security controls using real-world attack paths.
Continuous Automated Red Teaming (CART): RedOps teams simulate adversary behavior to stress-test your defenses over time.

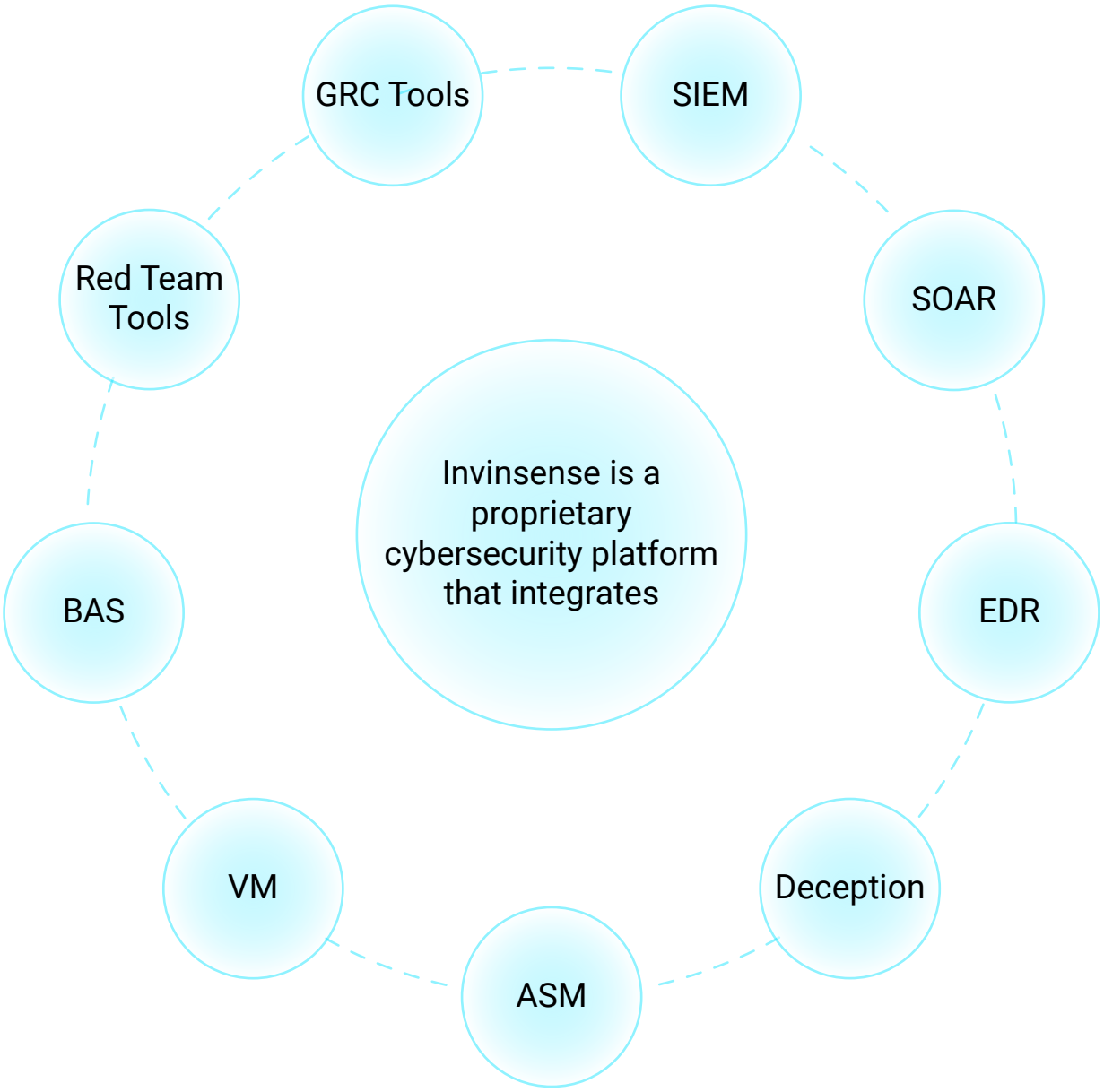
6.3 Security Compliance (Invinsense GSOS)

- Automate tracking of compliance with:
  - GDPR
  - HIPAA
  - ISO 27001
  - NIST 800-53
  - PCI-DSS
- Map controls to frameworks
- Evidence collection and reporting
- Manage audits, risks, and governance centrally

6.4 Security Engineering

- DevSecOps Support: Integrate with CI/CD pipelines.
- Custom Application Remediation: Get hands-on help for fixing vulnerable code and misconfigurations.
- Patch Management: Orchestrate automatic and manual patches via XDR+ and engineering teams.

Real MDR Platform: Invinsense

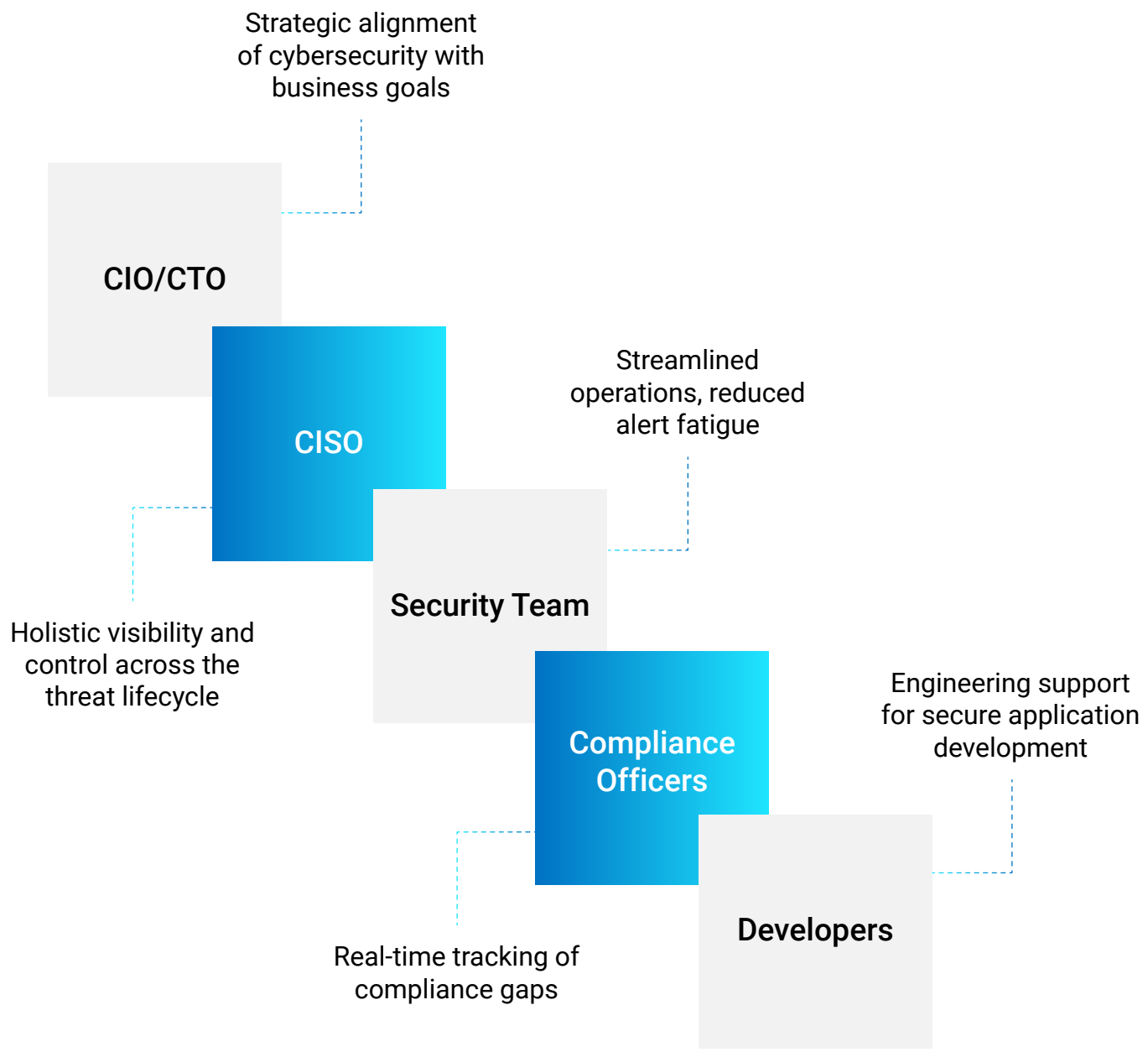


This consolidation reduces complexity, enhances visibility, and lowers operational costs.

Competitive Advantage: Real MDR vs Traditional MDR

Feature	Traditional MDR	Real MDR
24x7 Monitoring	✓	✓
XDR Integration	✓	✓
Deception Technology	✗	✓
Attack Surface Monitoring	✗	✓
Red Teaming	✗	✓
Vulnerability Management	✗	✓
Application Remediation	✗	✓
Compliance Management	✗	✓
Platform Unification	✗	✓
Engineering Support	✗	✓

Benefits Across Stakeholders



Use Cases of Real MDR

10.1 Ransomware Prevention

ASM identifies exposed RDP ports, VM highlights vulnerable services, CART simulates lateral movement, engineering teams harden endpoints.

10.2 Regulatory Readiness

GSOS maps controls to GDPR and ISO 27001, tracks control effectiveness, and prepares evidence for auditors.

10.3 Post-Breach Analysis

XDR captures incident details, SOAR initiates playbooks, compliance logs the event for forensics.

10.4 DevSecOps Alignment

Security engineers guide developers in remediating SQL injection identified in app pentests.

Buying Considerations and Evaluation Criteria

When evaluating MDR vendors, ask:

- Does the MDR support exposure management or just detection?
- Are deception technologies included to detect stealthy attackers?
- Is there a unified platform or a patchwork of third-party tools?
- Does the service provide code-level remediation support?
- Can the MDR simulate real attacks continuously?

Real MDR Deployment Models

Fully Managed

End-to-end service including detection, response, engineering, and compliance.

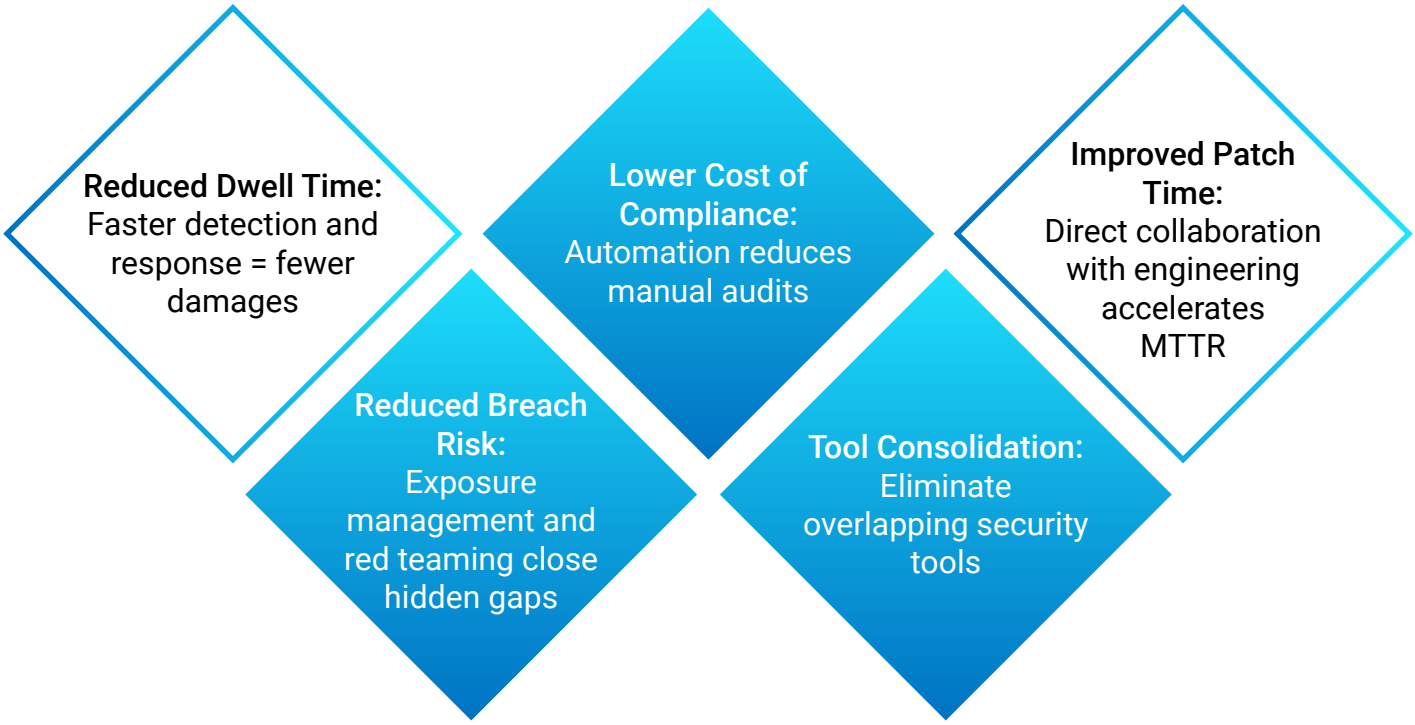
Co-Managed

Customer retains internal tools; Real MDR integrates to extend visibility and coverage.

Platform-Only

Invinsense licensed as a platform for customers with in-house security teams.

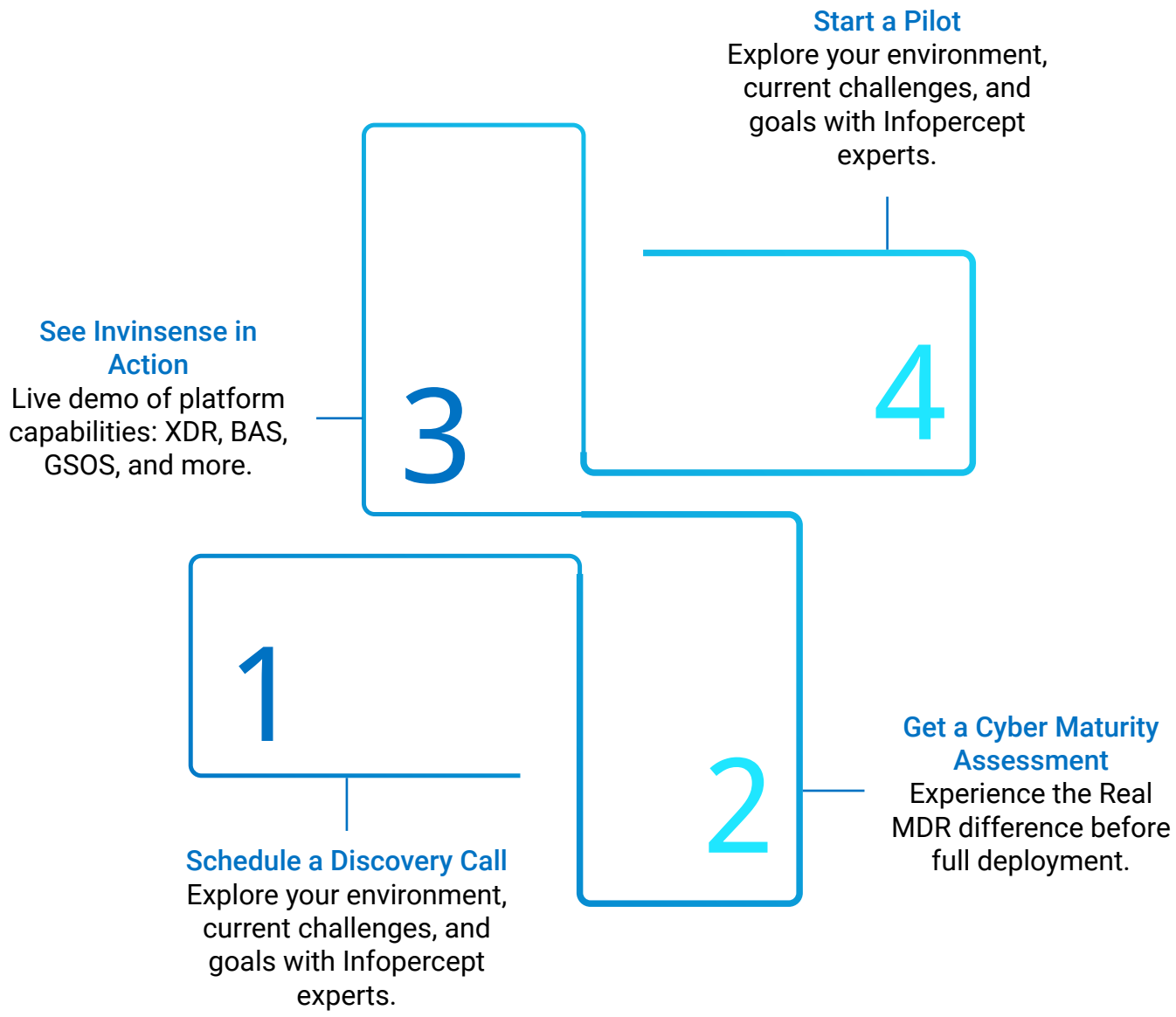
Measuring the ROI of Real MDR



Questions to Ask MDR Providers

- How do you validate that my controls work?
- Can you simulate real attacker behavior continuously?
- How is application remediation handled?
- Do you provide visibility into my external attack surface?
- How is compliance managed and reported?
- Do you support cloud, hybrid, and on-prem environments?
- Is threat intelligence contextualized or generic?
- Can your MDR align with DevSecOps processes?

Getting Started with Infopercept's Real MDR



Conclusion: Why Settle for Partial MDR?

Cybersecurity can no longer afford to be reactive or siloed. Infopercept's Real MDR reimagines managed detection and response as a complete cybersecurity lifecycle management solution—enabling organizations to detect, respond, reduce risk, comply, and remediate continuously and effectively.
This is the new standard. This is Real MDR.

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