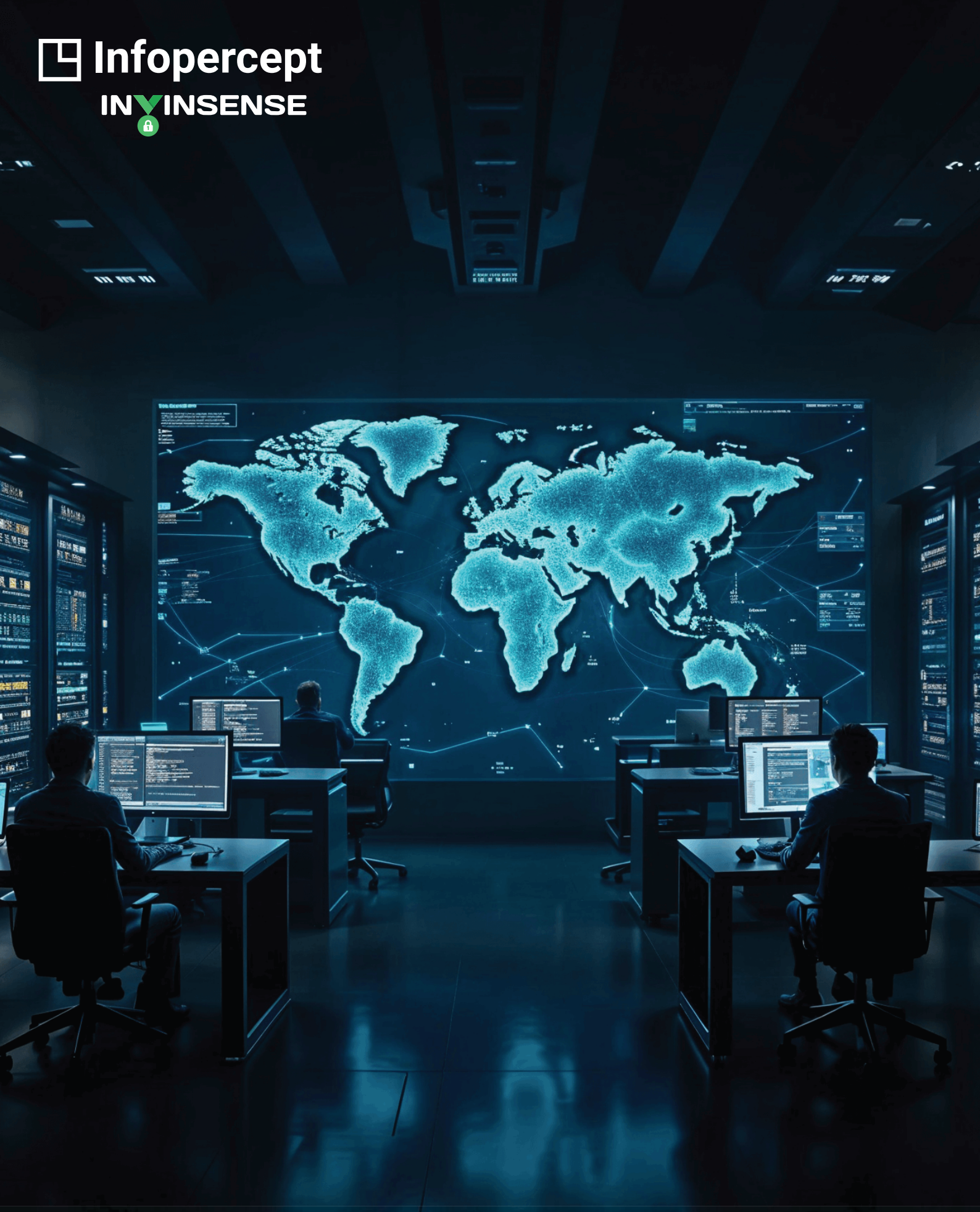
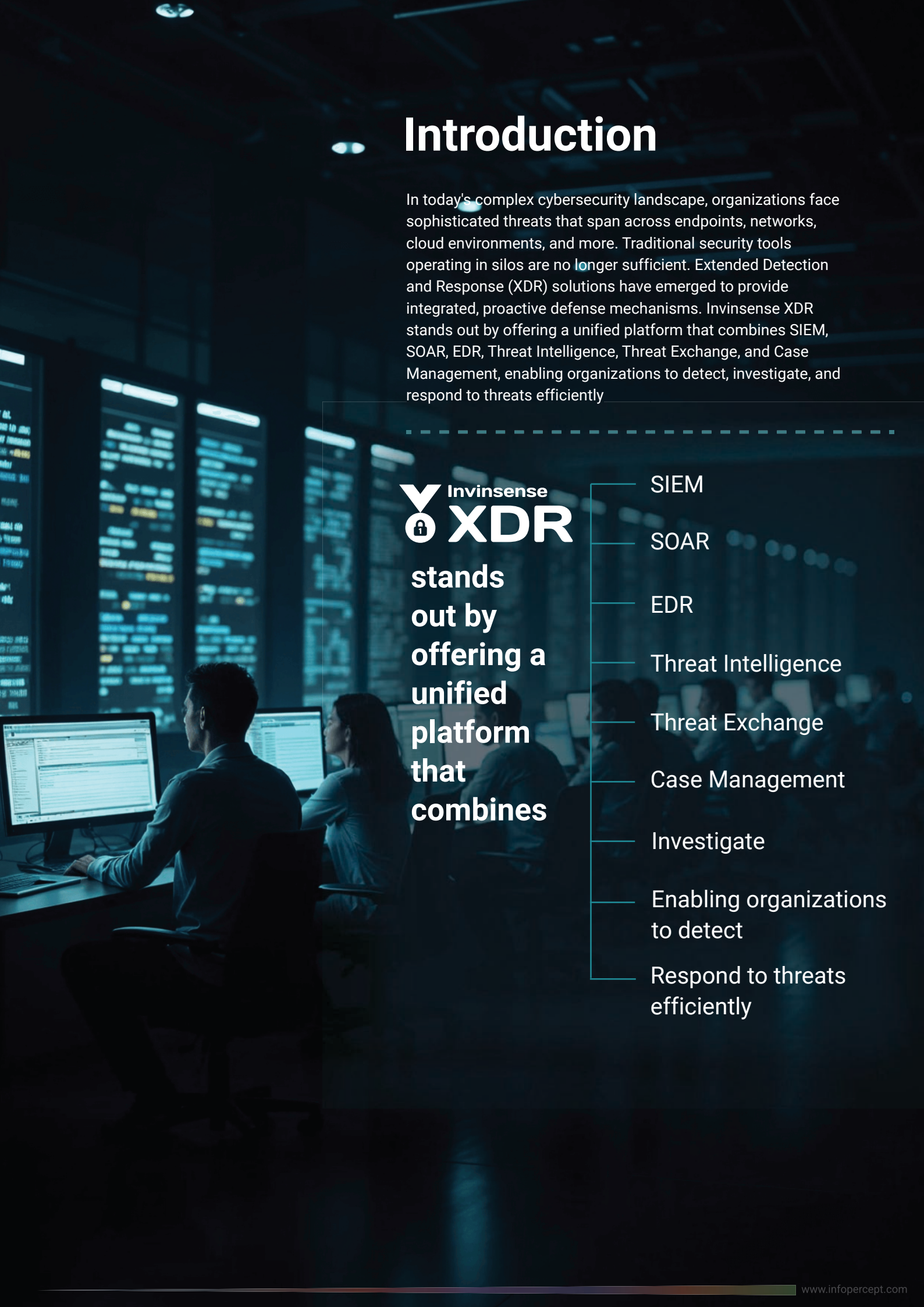
Infopercept

INVINSENSE



Invinsense XDR Buyer's Guide



Introduction

In today's complex cybersecurity landscape, organizations face sophisticated threats that span across endpoints, networks, cloud environments, and more. Traditional security tools operating in silos are no longer sufficient. Extended Detection and Response (XDR) solutions have emerged to provide integrated, proactive defense mechanisms. Invinsense XDR stands out by offering a unified platform that combines SIEM, SOAR, EDR, Threat Intelligence, Threat Exchange, and Case Management, enabling organizations to detect, investigate, and respond to threats efficiently

Invinsense XDR stands out by offering a unified platform that combines

- SIEM
- SOAR
- EDR
- Threat Intelligence
- Threat Exchange
- Case Management
- Investigate
- Enabling organizations to detect
- Respond to threats efficiently

Buyer Checklist: Key Questions to Ask

- Does the platform integrate with our existing tools (SIEM, endpoint, ticketing)?
- Can it detect and stop modern threats (fileless, insider, ransomware)?
- Is automation available for response and compliance workflows?
- How long will onboarding and use case tuning take?
- Does it help reduce alert fatigue and improve analyst focus?
- Can it scale across geographies, environments, and data volumes?

Key Considerations When Evaluating XDR Solutions

When selecting an XDR solution, consider the following critical factors:

1. Comprehensive Visibility and Telemetry Integration

An effective XDR solution should collect and correlate data from various sources, including endpoints, networks, cloud services, and applications.
Invinsense XDR offers:

- **100+ Prebuilt Datasource Integrations:** Supports both agent-based and agentless data collection.
- **Custom API Integration Support:** Allows integration with existing tools and platforms.
- **Support for Multiple Log Formats:** Including custom log formats to ensure compatibility.

2. Advanced Threat Detection and Response

The ability to detect sophisticated threats and respond promptly is paramount.
Invinsense XDR provides:

- **MITRE ATT&CK Mapping:** Aligns detected threats with known adversary tactics and techniques.
- **User Behavior Analytics (UBA):** Identifies anomalies in user behavior to detect insider threats.
- **Attack Trajectory Analysis:** Visualizes the path of fileless and in-memory attacks for better understanding.

3. Automation and Orchestration Capabilities

Reducing manual intervention through automation enhances efficiency.
Invinsense XDR includes:

- **SOAR with 1000+ Application Integration Support:** Supports both agent-based and agentless data collection.
- **No-Code Workflow Builder and Visual Playbook Editor:** Allows integration with existing tools and platforms.
- **Improved MTTD and MTTR:** Enhances Mean Time to Detect and Mean Time to Respond through automation.

4. Integrated Threat Intelligence and Collaboration

Access to up-to-date threat intelligence and collaboration tools is essential.
Invinsense XDR offers:

- **Integrated Threat Intelligence:** Provides real-time insights into emerging threats.
- **Threat Exchange:** Facilitates sharing of threat information across organizations.
- **Case Management:** Streamlines incident investigation and documentation processes.

5. Compliance and Reporting

Meeting regulatory requirements and generating reports is simplified with:

- **Compliance Support and Visibility:** Assists in adhering to standards like PCI-DSS, ISO 27001, and HIPAA.
- **Custom Dashboards and Reports:** Provides tailored views for different stakeholders.

Why Choose Invinsense XDR?

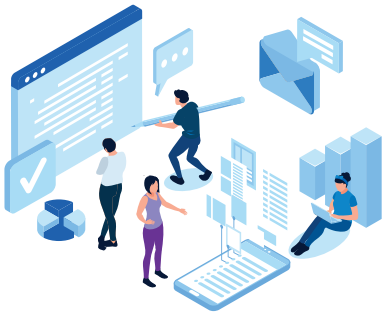
Invinsense XDR delivers measurable improvements across visibility, automation, detection, and compliance:

50%

faster threat detection with unified telemetry and MITRE ATT&CK mapping

60–70%

reduction in incident response time through SOAR-driven playbooks



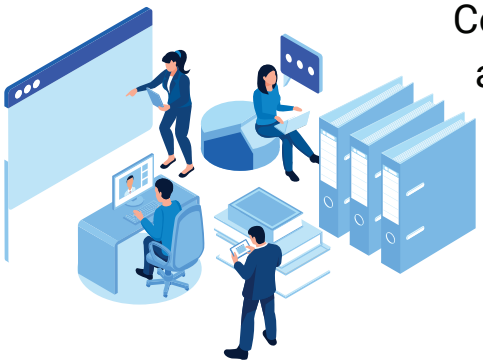
Over 500

Prebuilt use cases for rapid time-to-value across diverse technologies

30%

increase in analyst productivity by automating

L1 & L2 tasks



Comprehensive visibility across endpoints, logs, vulnerabilities, and compliance

Real-time + historical analytics to support

threat hunting, audits, Investigations

Invinsense XDR

What Makes Invinsense XDR Stand Out

Capability	Invinsense XDR Advantage
Unified Stack	Combines SIEM, SOAR, EDR, Intel & Case Management in one pane
Customizability	Onboards custom logs, supports APIs, builds tailored use cases
Deception & Compliance Ready	Optional integration with deception tech and regulatory mapping
Scalable Architecture	Adapts to enterprises, MSSPs, and mid-size organizations
Real-Time Remediation	Supports manual & automated patching workflows
Purple Teaming Support	Integrates offensive & defensive operations for CTEM programs

Real-World Value Delivered

Based on existing deployments:

A large fintech reduced response time by 65% and detected unknown threats through memory-based attack tracing.

A logistics enterprise onboarded 75+ data sources and used automated patching for faster remediation.

A telecom provider aligned SOC operations to MITRE and eliminated blind spots in credential abuse.

Benefits and Deliverables from Invinsense XDR

Based on previous case studies and implementations, organizations utilizing Invinsense XDR have experienced:

Enhanced Security Posture

Through comprehensive visibility and proactive threat detection.

Operational Efficiency

By automating routine tasks and reducing alert fatigue.

Improved Incident Response

With integrated tools facilitating faster decision-making and action.

Regulatory Compliance

Simplified adherence to various compliance standards through built-in support.

Scalability

Adaptable to organizations of different sizes and industries.

Final Thoughts

Invinsense XDR is purpose-built for security teams seeking an integrated, agile, and intelligent defense strategy. Whether you're building a modern SOC, enabling a CTEM program, or simplifying compliance, Invinsense provides the capabilities to reduce complexity, enhance visibility, and accelerate response.

It's more than a tool — it's a force multiplier for your security operations.

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