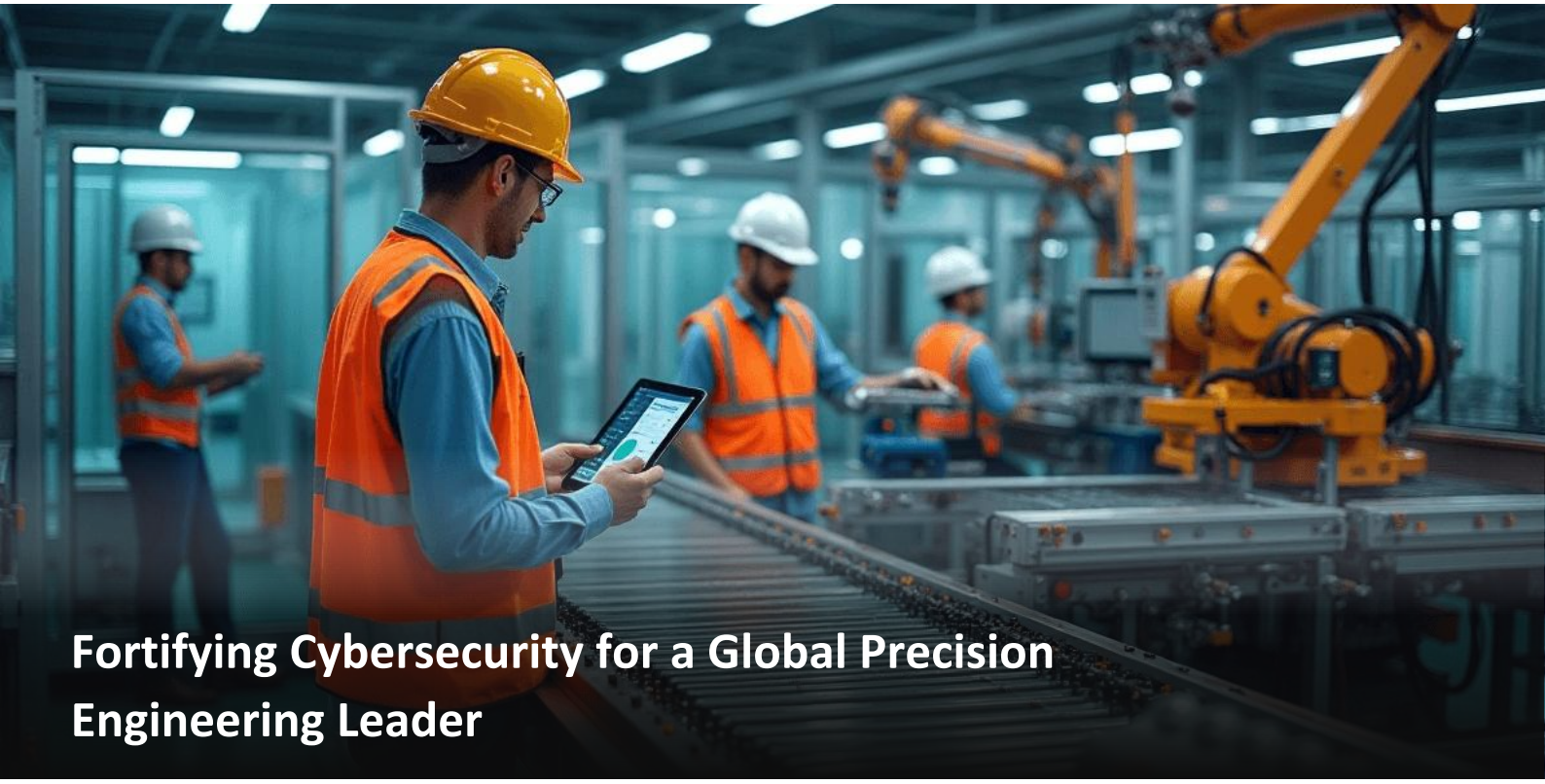

Fortifying Cybersecurity for a Global Precision Engineering Leader

About the Customer

The customer is a global leader in manufacturing precision bearing cages and high-precision components, serving clients across various industrial sectors. With a presence in multiple countries and a robust export network, the organization operates advanced manufacturing facilities supported by a strong engineering and design backbone. Their expansive digital infrastructure includes ERP systems, CAD/CAM platforms, CNC machines with IoT connectivity, and proprietary production control software.

Industry	Precision Manufacturing / Industrial Engineering
Challenge	Securing complex manufacturing operations and ensuring compliance across global facilities
Solutions Used	Invinsense XDR, XDR+, OXDR, GSOS

The Challenge

As the organization scaled its global operations and adopted digital technologies in its manufacturing lifecycle, several security and compliance challenges surfaced:

- Protecting sensitive design, manufacturing, and IP data across distributed facilities
- Addressing cyber risks introduced by IoT-connected production systems
- Meeting ISO 27001 and industry-specific compliance mandates
- Ensuring visibility into digital threats with limited internal cybersecurity bandwidth
- Maintaining operational continuity and uptime amidst rising threat activity

The Invinsense Solution

To address these challenges, the organization implemented Invinsense's unified platform that integrated monitoring, exposure management, deception, and compliance enforcement capabilities.

Invinsense XDR: Unified Threat Detection Across Operations

Invinsense XDR centralized the detection of security threats across global manufacturing sites and critical systems. It enabled continuous visibility, real-time alerting, and intelligent correlation of events across their digital assets.

Key Outcomes:

- 70% faster detection of threats across ERP, email, and IoT platforms
- Prevention of unauthorized access attempts via early detection mechanisms
- Significant reduction in false positives, streamlining incident response

Prevention of unauthorized access attempts via early detection mechanisms

The OXDR and Continuous Threat Exposure Management (CTEM) capabilities allowed the organization to identify and address cyber risks across their digital infrastructure systematically.

CTEM Breakdown:

Scoping	• Identified 3,000+ assets, including CAD systems, IoT-connected machinery, and plant control systems
Discovery	• Uncovered 200+ misconfigured endpoints and unpatched systems
Prioritization	• Mapped vulnerabilities to potential operational disruptions
Validation	• Simulated breach paths to validate exploitability
Mobilization	• Closed 90% of high-impact exposures in less than 15 days

Key Result

- 70% faster detection of security incidents
- 4.8x improvement in vulnerability remediation timelines
- 97% alignment with ISO 27001 and industry-specific compliance requirements
- 6.2x increase in early threat identification through deception technology

Executive Insight

"With Invinsense, we've moved from reactive to proactive security. Their unified platform gave us the visibility, control, and resilience we needed to secure our operations without slowing down innovation."

Chief Information Security Officer, Global Engineering Manufacturer

CTEM Outcomes:

- 4.8x improvement in remediation turnaround
- 70% fewer recurring misconfigurations
- Improved operational security posture with regular exposure reviews

Invinsense XDR+: Advanced Deception Capabilities

To proactively detect lateral movement and advanced threats, Invinsense XDR+ deployed deception assets within the environment.

Deception Outcomes:

6.2x increase in early threat detection	Discovery of unauthorized insider attempts and suspicious behavior	Deployment of decoy manufacturing data and dummy control systems for threat luring

Invinsense GSOS: Driving Continuous Compliance

With globally distributed operations and industry certifications in view, Invinsense GSOS automated control mapping, audit reporting, and continuous compliance assessments.

Compliance Outcomes:

97% alignment with ISO 27001 and related engineering compliance standards	Reduction in manual compliance tracking efforts by 65%	Audit-ready documentation and evidence tracking for all digital systems

Quantifiable Impact

Category	Improvement
Threat Detection Speed	↑ 70% faster
Remediation Efficiency	↑ 4.8x faster
Compliance Alignment	↑ 97% achieved
Early Threat Detection	↑ 6.2x increase
Audit & Reporting Effort	↓ 65% reduction

Conclusion

By leveraging Invinsense's integrated security stack, the customer significantly enhanced their threat visibility, reduced vulnerabilities, and met compliance standards across a complex, distributed manufacturing environment—allowing them to scale securely and confidently into the future.

Infopercept | INVINSENSE

About Infopercept - Infopercept is one of the fastest growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint
© Infopercept Consulting Pvt. Ltd.

Contact
sos@infopercept.com
www.infopercept.com/knowledge/casestudy