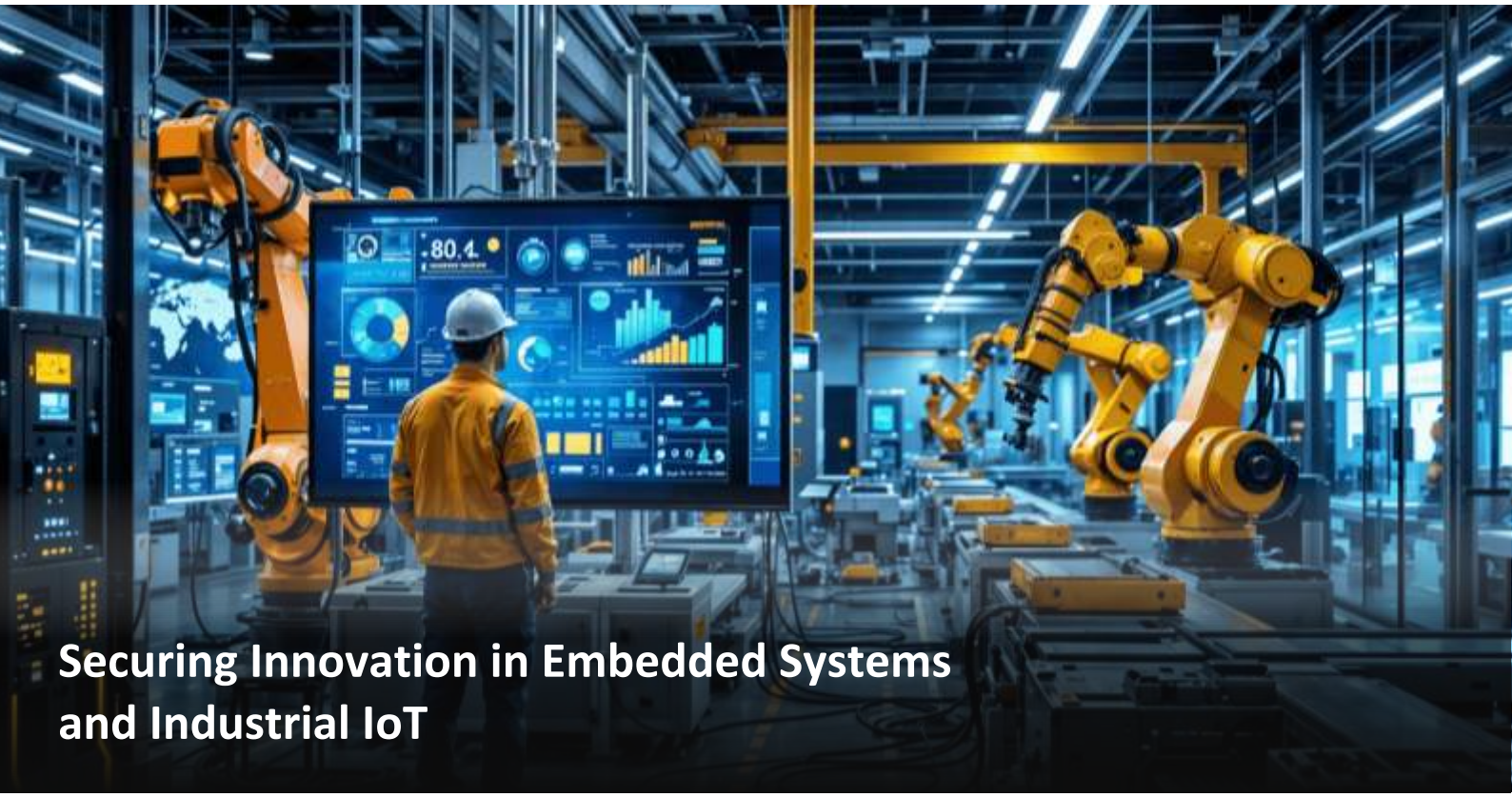

Securing Innovation in Embedded Systems and Industrial IoT

About the Customer

The customer is a technology-driven engineering and manufacturing solutions provider focused on embedded systems, industrial automation, and IoT applications. With over two decades of experience, their operations span product design, prototyping, system integration, and end-to-end production. Serving global clients in sectors such as automotive, healthcare, defense, and consumer electronics, the organization handles a complex digital ecosystem involving sensitive design data, proprietary firmware, and real-time system telemetry across connected devices.

The Challenge

As a provider of embedded and industrial technology solutions, the organization faced cybersecurity challenges unique to their domain:

Protecting intellectual property across design files, firmware repositories, and embedded code.	**Securing IoT endpoints and industrial controllers against** remote exploitation and firmware tampering.	**Maintaining traceability and security** in the product development lifecycle with external vendor collaboration.
Monitoring SCADA and MES systems that lacked traditional endpoint protection.	**Complying with client-imposed cybersecurity requirements** in highly regulated sectors like defense and medical devices.	**Preventing lateral movement between IT and OT networks** due to legacy system dependencies.

The customer needed a platform that could secure their hybrid environments—spanning cloud, OT networks, and edge devices—while aligning with stringent IP protection and quality assurance mandates.

Threat Deception with XDR+

By embedding deception into their engineering and manufacturing systems, the organization achieved:

- Early detection of unauthorized access attempts within restricted code repositories.
- Detection of 3 vendor-side anomalies attempting lateral access from shared test environments.
- Reduction in false positives and alert fatigue by over 50% in production environments.

Security Compliance Enablement with GSOS

The GSOS module helped the customer:

- Map security controls to client-specific cybersecurity checklists, including those required for export-controlled projects.
- Standardize audit reporting and vendor security assurance documentation.
- Maintain audit-ready status for all 7 major clients with quarterly cybersecurity audits.

CTEM in Action CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Identified 780+ assets, including firmware repositories, edge devices, and production PLCs.
Discovery	Revealed 43 critical vulnerabilities, 11 exposed services, and 5 hardcoded credentials in legacy systems.
Prioritization	Highlighted 27 business-impacting risks, particularly in firmware development and remote device access.
Validation	Simulated 8 attack chains including code injection, unauthorized firmware upload, and SCADA pivoting.
Mobilization	Achieved 85% remediation of critical issues within 28 days, including hardened firmware pipelines and segmented OT networks.

Executive Quote

"Our work depends on innovation and trust. Invinsense not only helped us secure our IP and industrial systems, but also provided the visibility and assurance our global clients expect from a technology partner."

– Director of Engineering Security, Embedded Systems & Automation Company

Solutions Used

To meet their security, visibility, and compliance needs, the customer deployed the Invinsense platform:

- Invinsense XDR consolidated detection across endpoints, firmware development environments, and IoT telemetry systems.
- Invinsense XDR+ introduced deception into both R&D and production environments to preempt insider and external threats.
- Invinsense OXDR enabled discovery and testing of exposures across industrial assets, cloud platforms, and third-party integrations.
- Invinsense GSOS helped formalize and document control requirements for secure product development workflows.

Key Results

- 85% reduction in exploitable vulnerabilities in OT and firmware ecosystems.
- 50% improvement in alert quality and triage efficiency.
- 100% compliance with client cybersecurity policies and control expectations.
- 28-day remediation cycle for the majority of critical issues.
- Strengthened IP protection across R&D and prototyping phases.

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.

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