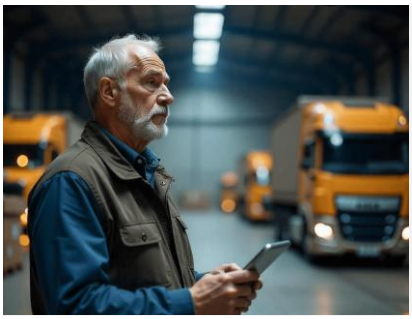
Securing Autonomous Logistics Through Intelligent Cyber Defense



About the Customer

The customer is a logistics automation company specializing in AI-driven communication platforms for supply chain operations. Their SaaS-based offerings enable manufacturers, shippers, and logistics providers to automate workflows using autonomous agents powered by AI and NLP. With integration capabilities across TMS, ERPs, CRMs, and freight systems, the customer's platform handles sensitive business data, shipment records, and customer communications across regions and sectors.

The Challenge

As an emerging player in intelligent supply chain automation, the company faced unique cybersecurity challenges:

Securing AI-powered communication agents that handle confidential client instructions and transportation data.	Protecting APIs and integrations that connect with customer ERPs, logistics platforms, and carrier networks.	Preventing misuse of automation triggers, such as those involving invoice generation or shipment updates.
Managing data privacy risks in handling international freight, vendor, and financial communications.	Meeting compliance expectations for clients in regulated sectors like manufacturing and healthcare.	Maintaining service availability while scaling across multi-tenant cloud environments.

These challenges required continuous security monitoring and proactive defense mechanisms to protect the integrity of automation systems and data flows.

Threat Deception with XDR+

Deception strategies focused on detecting misuse of automation and unauthorized agent access:

- Deployed fake command agents and decoy shipment workflows to detect threat actors simulating customer requests.
- Planted dummy vendor accounts and contract files to bait internal misuse or credential theft.
- Alert-to-response time improved by 45%, enhancing the platform's ability to prevent silent threats.

Security Compliance Enablement with GSOS

To ensure customer trust and audit readiness, the customer used GSOS to:

- Align internal practices with ISO 27001 and GDPR standards.
- Track remediation workflows across DevOps, engineering, and compliance functions.
- Build real-time dashboards for data processing controls and incident reporting.

CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Mapped 2,000+ digital assets, including API endpoints, cloud services, and AI modules.
Discovery	Identified 27 critical vulnerabilities, primarily around unsecured APIs and exposed configuration files.
Prioritization	Flagged 10 business-impacting scenarios, including invoice manipulation, agent spoofing, and data leakage.
Validation	Simulated attack paths mimicking rogue command injection and data extraction from unsecured agents.
Mobilization	Resolved 89% of critical issues within 30 days, using platform automation and engineering team collaboration.

Executive Quote

"As we automate logistics across continents, Invinsense has become a critical enabler of secure scale. Their ability to simulate attack paths and secure our intelligent agents ensures we innovate without compromise."

– Head of Engineering, AI-Powered Logistics Automation Company

Solutions Used

To address these needs, the customer implemented the full Invinsense platform:

- Invinsense XDR for monitoring all application activities, user behaviors, and data exchanges.
- Invinsense XDR+ for embedding deception into communication agents, shipment datasets, and internal service accounts.
- Invinsense OXDR for conducting continuous threat exposure assessments across APIs, SaaS connectors, and AI pipelines.
- Invinsense GSOS to align with international compliance standards and maintain secure vendor collaboration.

Key Results

- 89% of critical vulnerabilities remediated in less than 30 days.
- 45% faster threat detection and response, thanks to deception layers.
- 35% reduction in misconfigured automation scripts through continuous validation.
- Strengthened API security posture across all customer integrations.
- Improved client trust in autonomous agents handling operational decisions.

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

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