Securing Logistics at the Speed of E-Commerce: How a Tech-Driven Delivery Platform Reduced Risk Across 7 Countries with Invinsense

About the Customer

This company is a fast-growing last-mile logistics provider powering e-commerce deliveries across Southeast Asia. With fully digital operations in markets like Singapore, Malaysia, Indonesia, the Philippines, and Thailand, they combine proprietary technology with on-ground operations to serve businesses of all sizes. Their logistics platform integrates with e-commerce sellers, payment gateways, warehousing partners, and real-time tracking tools — making security and uptime critical to their regional leadership.

Industry	Logistics & Last-Mile Delivery
Challenge	Protecting multi-country operations, APIs, customer data, and regulatory compliance
Solutions Used	Invinsense XDR, XDR+, OXDR, GSOS

The Challenge

Operating across multiple countries, the logistics firm faced increasing security demands driven by:

Exposed logistics APIs used for parcel tracking, route optimization, and order creation	**Credential theft** attempts targeting dashboards for merchants, riders, and partners	**Disparate cloud environments** across regions with inconsistent security configurations
Compliance obligations varying by country (e.g., PDPA, Cybersecurity Act, GDPR)	**Threat actors** trying to manipulate shipping fees, delivery windows, or proof-of-delivery (POD) uploads	**Slow remediation** across agile dev teams supporting logistics tech stacks

The Invinsense Solution

To bring centralized visibility, streamline compliance, and enable faster risk reduction, the company deployed the full Invinsense platform.

Invinsense XDR: Visibility Across Rider Apps, Dashboards, and APIs

Invinsense XDR unified telemetry from tracking APIs, merchant portals, rider apps, and route engines to deliver real-time threat detection.

Key Results:

- 72% faster containment of workflow-specific breaches (e.g., rerouting fraud attempts)
- 2.8x faster alert triage through playbook automation across ops and security teams
- 63% reduction in false positives through behavioral analytics tuned to logistics flows
- Detected token reuse attacks within 5 minutes of initial anomalous access

Invinsense OXDR + CTEM: Managing Exposure Across Cloud & Microservices

A CTEM (Continuous Threat Exposure Management) strategy was rolled out to improve exposure visibility across all regions.

Scoping	• Catalogued 6,800+ digital assets across 7 countries • Mapped parcel tracking APIs, rider onboarding portals, and warehouse management endpoints
Discovery	• Identified 270+ misconfigured APIs, including public endpoints exposing route IDs and parcel metadata • Discovered excessive privileges granted to legacy service accounts
Prioritization	• Prioritized threats involving delivery modification, spoofed tracking updates, and geo-spoofing • Mapped critical vulnerabilities to business impact on customer SLAs
Validation	• Simulated proof-of-delivery tampering and phantom delivery attacks • Used attack emulation to validate privilege escalation paths within microservices
Mobilization	• Closed 81% of validated risks in the first 45 days • Integrated findings into CI/CD pipelines with regional engineering teams

Invinsense XDR+: Deception to Catch Delivery & Rider Workflow Abuse

Custom decoys were deployed to mimic parcel updates, rider login dashboards, and shipment escalation requests.

Results:

6.2x improvement in detection of lateral movement across staging servers	Deception traps exposed a fraudulent merchant campaign abusing bulk shipping APIs	Identified bot activity mimicking customer complaints to trigger refund workflows	Lowered alert fatigue by 66% through deception-led prioritization

Key Result

- 72% faster containment of delivery workflow breaches
- 88% reduction in API misconfigurations
- 4.1x increase in patch cycle efficiency
- 93% control alignment with local cybersecurity regulations across SEA

Executive Insight

"We needed more than alerts — we needed answers. Invinsense gave us full visibility across countries, applications, and teams. Security now scales with our business."

CTEM Outcomes

- 4.1x increase in patch cycle efficiency
- 3.7x faster mean time to validate exposures
- 88% reduction in critical API misconfigurations
- Created a unified exposure dashboard for seven countries

Invinsense GSOS: Enabling Regional Compliance from a Single Pane of Glass

GSOS was implemented to help the security and compliance teams meet diverse regulatory requirements across their operating regions:

Singapore's Cybersecurity Act	Malaysia's PDPA (Personal Data Protection Act)	Philippines' Data Privacy Act	Thailand's PDPA	Indonesia's Electronic Information and Transactions Law

Compliance Outcomes:

93% control alignment across five national frameworks	Reduced audit prep effort by 5x through templated assessments	Enabled continuous monitoring and reporting of security control maturity	Mapped security controls to over 25 critical processes, including delivery escalation and merchant payments

Quantifiable Impact

Category	Improvement
API Misconfigurations	↓ 88%
Exposure Validation Speed	↑ 3.7x
Lateral Movement Detection via Deception	↑ 6.2x
Compliance Alignment Across Countries	↑ 93%
Delivery Workflow Breach Containment	↑ 72% faster
Audit Preparation Time	↓ by 5x

Conclusion

In a region where e-commerce logistics is a competitive battleground, this tech-enabled delivery firm turned cybersecurity into a growth enabler. Invinsense helped them strengthen trust, reduce exposure, and navigate cross-border compliance — all while keeping packages moving and customers satisfied.

Infopercept | INVINSENSE

Imprint

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