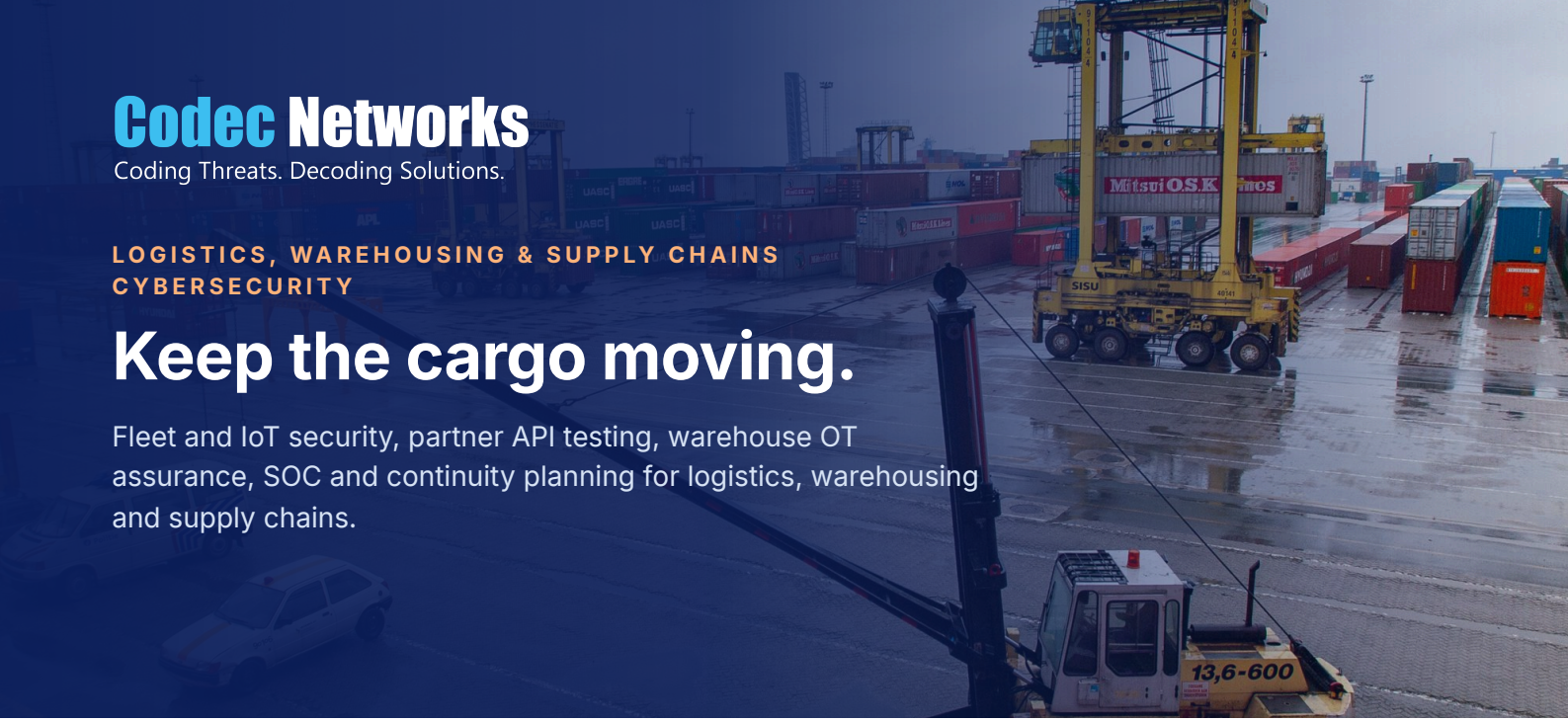

Codec Networks

Coding Threats. Decoding Solutions.

LOGISTICS, WAREHOUSING & SUPPLY CHAINS CYBERSECURITY

Keep the cargo moving.

Fleet and IoT security, partner API testing, warehouse OT assurance, SOC and continuity planning for logistics, warehousing and supply chains.

Three questions every logistics leader should be able to answer

If our TMS and WMS went dark tonight, could cargo move tomorrow?

Mapping what hubs, fleets and customs filings depend on and testing restores decides whether ransomware is a bad day or a bad quarter.

Who holds API keys and VPN access into our platform?

Merchants, carriers, automation vendors and SaaS providers are the most common unmonitored paths to shipment data and operations.

Would our finance team pay an invoice to a changed bank account?

Business email compromise is the most common and most expensive logistics fraud; verification procedures and mailbox monitoring stop it.

US$300 m
Maersk's NotPetya loss, upper estimate

~730 jobs
Lost after one ransomware attack

7.2 m
Shipments in one day (India, 2025)

6 hours
Incident reporting to CERT-In

Built for every link in the chain

3PL and 4PL providers · express and courier companies · freight forwarders and customs brokers · trucking and fleet operators · warehouse and fulfilment operators · cold storage and cold chain · supply-chain platforms.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CERT-In Directions · audit guidelines (2022, 2025)	6-hour reporting, 180-day logs; independent audits incl. OT
DPDP · SEBI LODR	Consignee and driver data safeguards; quarterly disclosure (listed)
Shipper and platform rules	Questionnaires, NIS2 flow-down; GST, customs and AIS 140 integrity

WHAT WE DO

Fleet, APIs, warehouse OT, SOC, continuity and supply-chain risk

Fleet & IoT Security
Telematics, driver apps, FASTag and remote-command controls assessed.

Partner API Testing
Shipper, carrier and merchant APIs, EDI, portals and tracking apps tested.

Warehouse OT Assurance
WMS, AS/RS, sorters, PLCs, segmentation and vendor access.

24/7 Logistics SOC
Platform, hub, fleet and mailbox monitoring with 6-hour reporting support.

Continuity & Recovery
Dependency mapping, immutable backups, playbooks and exercises.

Supply-Chain Risk & Privacy
SaaS and vendor assessments, shipper questionnaires, DPDP programme.

Choose your starting point

Foundation
Platform and network assessment, BEC and payment control review, backup review, policy and questionnaire pack. For regional fleets, warehouses and forwarders.

Assurance
Annual VAPT of portals, APIs and apps, warehouse OT and vendor access review, independent audit and ISO 27001, 24x7 SOC. For national 3PLs, couriers and multi-site operators.

Continuous Resilience
Continuous testing and red teaming, fleet, IoT and automation programme, SaaS and partner risk, SOC with hunting and Board reporting. For large integrated groups and platforms.

Why Codec Networks

CERT-In empanelled
for information security auditing services, and empanelled with NICSI for application audit services.

Certified
ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018.

Regulation-mapped
Every finding mapped to ISO/IEC 27001, IEC 62443, OWASP, CERT-In expectations, DPDP and your shippers' security requirements.

One connected partner
Testing, audits, SOC, forensics and privacy linked from finding to closure.

Book a scoping session

Share your platforms, hubs, fleets, partners and shippers. We will propose a practical, operations-aware assessment and assurance plan.

New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001
Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018
Call: 011 430 496 96 · +91 99716 76124 · +91 88007 88220
Email: mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Sources: Maersk statements, FRP Advisory and public reporting, Delhivery, CERT-In. Confirm obligations against the official instruments.