



Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · LOGISTICS, WAREHOUSING & SUPPLY CHAINS

Keep the Cargo Moving. Keep the Platform Trusted.

Fleet and IoT security, partner API testing, warehouse OT assurance, SOC and continuity planning for 3PL and 4PL providers, couriers and express companies, freight forwarders, trucking fleets, warehouse and cold-chain operators and supply-chain platforms.

Fleet & IoT Security

Partner API Testing

Warehouse OT Assurance

24/7 Logistics SOC

Continuity & Recovery

Supply-Chain Risk & Privacy

Coding Threats. Decoding Solutions.

www.codecnetworks.com

THE CHALLENGE

In logistics, a cyber incident is cargo that stops moving.

Indian logistics moves more than 14 crore e-way bills a month on platforms, partner APIs, telematics and warehouse automation that were never designed to be attacked. When Maersk lost its network to NotPetya in 2017 it rebuilt 45,000 PCs and lost US\$250–300 million; Expeditors shut down global systems for weeks in 2022; and in 2025 a 158-year-old UK haulier collapsed after one guessed password let ransomware in.

What keeps leadership teams awake

- Ransomware stopping TMS, WMS and hubs in peak
- Freight payment fraud through hijacked email
- Partner APIs and EDI leaking consignee data
- Telematics and fleet IoT open to the internet
- Automation vendors with standing warehouse access
- CERT-In reporting, DPDP and shipper audits



US\$300 m

Upper estimate of Maersk's NotPetya loss (2017)

~730 jobs

Lost when KNP Logistics collapsed after ransomware (2025)

7.2 m

Shipments in one day at India's largest logistics firm (2025)

6 hours

To report cyber incidents to CERT-In

The rulebook has changed

Instrument	What it means for you
CERT-In Directions and audit guidelines (2022, 2025)	6-hour reporting, 180-day logs; independent audits incl. OT
DPDP Act and Rules (2023, 2025)	Consignee, driver and employee data; most duties from May 2027
SEBI LODR · NCIIPC	Quarterly disclosure (listed); notified transport systems
Shipper and platform rules	Security questionnaires, NIS2 flow-down, GST and customs integrity

One partner from booking to delivery

Built around our primary proposition for the sector: **Fleet and IoT security, partner API testing, warehouse OT assurance, SOC and continuity planning.**

Fleet & IoT Security

- Telematics platform and device assessment
- Driver and rider app and OTP flow testing
- FASTag, fuel card and remote-command controls
- Data minimisation for load and route data

Partner API Testing

- Shipper, carrier and marketplace API and EDI testing
- Key scoping, rate limiting and enumeration defences
- Customer portal and tracking app VAPT
- Secure SDLC for platform releases

Warehouse OT Assurance

- WMS, AS/RS, sorter and PLC assessments
- Zone-and-conduit segmentation design
- Automation vendor remote access brokering
- Cold-chain monitoring integrity review

24/7 Logistics SOC

- Platform, cloud, hub and fleet monitoring
- BEC, mailbox rule and payment anomaly detection
- API abuse and bulk-access alerting
- 6-hour CERT-In reporting support

Continuity & Recovery

- Dependency mapping of operations on IT
- Immutable backups and restore testing
- Manual-operation and port-release playbooks
- Ransomware and peak-season tabletop exercises

Supply-Chain Risk & Privacy

- Supply-chain SaaS and vendor assessments
- Shipper questionnaire and ISO 27001 readiness
- DPDP programme for consignee and driver data
- Contract security and notification clauses

Who we serve: 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 and aggregators.

Packaged for how logistics companies buy

Eleven Codec Networks bundles apply directly to logistics, warehousing and supply chain companies:

B1

Cyber Assessment & VAPT Assurance

B2

Application, API & DevSecOps Security

B3

Cloud, Infrastructure & Zero Trust

B4

Regulatory Cyber Audit & Compliance

B5

GRC, ISO, SOC 2 & PCI DSS Maturity

B6

Data Privacy & DPDPA Program

B7

Managed SOC, MDR & Threat Monitoring

B8

Forensics, Incident Response & Malware RCA

B9

Third-Party & Supply-Chain Risk

B10

Cyber Simulation, Awareness & Tabletop

B11

Emerging Tech, AI & Web3 Security

Foundation

Regional fleets, warehouses and forwarders

- Platform and network assessment
- Email, BEC and payment control review
- Backup and recovery review
- Policy pack and shipper questionnaire support

Assurance

National 3PLs, couriers and multi-site operators

- Annual VAPT of portals, APIs and apps
- Warehouse OT and vendor access review
- Annual independent audit and ISO 27001
- 24x7 SOC with BEC and API monitoring

Continuous Resilience

Large integrated logistics groups and platforms

- Continuous testing and red teaming
- Fleet, IoT and automation security programme
- Supply-chain SaaS and partner risk programme
- SOC with threat hunting and Board reporting

Mapped to your obligations

Requirement	How we help	Bundle
Incidents to CERT-In in six hours; 180-day logs (CERT-In Directions)	SOC, IR retainer and reporting support	B7, B8
Independent cyber audits incl. OT and cloud (CERT-In guidelines, 2025)	Independent IT/OT audits	B4, B1
Consignee, driver and employee personal data (DPDP)	DPDPA programme	B6
Quarterly incident disclosure, listed companies (SEBI LODR)	Incident records, disclosure support	B4, B8
Vehicle tracking devices and data (MoRTH AIS 140 notifications)	Telematics and VLT security review	B1, B11
E-way bill, GST and customs filing integrity (GSTN, ICEGATE)	Credential, access and filing controls	B3, B7
Shipper security requirements (contracts, NIS2 flow-down)	ISO 27001 and questionnaire readiness	B5, B9

Why logistics companies choose Codec Networks

CERT-In empanelled

Independent audits recognised by regulators, shippers and insurers.

Certified and accountable

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

Operations-aware methods

Testing planned around peak seasons, hub cut-offs and live automation.

Standards-mapped

Findings mapped to ISO/IEC 27001, IEC 62443, OWASP, CERT-In and DPDP expectations.

Full stack, one partner

Testing, OT, SOC, forensics, supplier risk and exercises connected from finding to closure.

Certified experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI and CHFI professionals.

How we engage

Discover & scope

Platforms, portals and APIs, hubs and warehouses, automation vendors, fleets and telematics, critical partners and your peak-season and audit calendar.

Assess & test

Threat-led testing and regulatory audits executed by certified specialists.

Report in business terms

Findings, risk ratings and a compliance gap matrix for the Board and regulators.

Remediate

Practical, prioritised fixes with technology and compliance teams.

Validate & prove

Retesting and an evidence tracker for auditors, regulators and partners.

Monitor & improve

Managed SOC, recurring testing and quarterly governance reviews.

What you receive: executive summary for the Board or its committee · technical findings with evidence and CVSS ratings · compliance gap matrix · prioritised remediation roadmap · retest reports · audit evidence tracker · SOC dashboards and MTTD/MTTR metrics.



START WITH A SCOPING SESSION

Let's make your next peak season, audit and incident a non-event.

Tell us 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, New Delhi – 110001

Gurugram

707, 7th Floor, Silverton Tower, Golf Course
Extension Road, Sector 50, Gurugram – 122018,
Haryana

Call

011 430 496 96 · 011 437 522 99
+91 99716 76124 · +91 88007 88220 · +91 88003
31124

Write

mktg@codecnetworks.com
www.codecnetworks.com

Codec Networks

Coding Threats. Decoding Solutions.

Secure Today. Innovate Tomorrow. Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Packages are proposed groupings of Codec Networks bundles, finalised through scoping. 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.