Codec Networks
Coding Threats. Decoding Solutions.



INDUSTRY BROCHURE · RAILWAYS, METRO & SURFACE TRANSPORT

Keep the Trains Moving. Keep the Passenger Safe.

Ticketing and API testing, communications and OT assessments, SOC and incident exercises for Indian Railways and its PSUs, metro corporations, state transport undertakings, tolling and transit technology companies.

- Ticketing & API Testing
- Signalling & OT Assessment
- Communications Security
- 24/7 IT/OT SOC
- Incident Exercises
- Passenger Data Protection

THE CHALLENGE

In transport, a cyber incident becomes a public event in minutes.

Rail and transit operators run safety-critical signalling and control alongside India's largest consumer platforms—ticketing, fares and tolling—often through suppliers with remote access. Denmark's trains stopped for hours in 2022 when a supplier's app went down after an attack; Transport for London spent about £29 million recovering from a 2024 intrusion.



What keeps leadership teams awake

- Ransomware halting operations or ticketing
- Intrusion into signalling, control and SCADA
- Supplier and OEM remote access
- Bots and fraud on ticketing and tolling APIs
- False announcements that cause crowd events
- CERT-In, NCIIPC, DPDP and payment obligations

741 crore
Passengers carried by Indian Railways in 2025-26

~1,095 km
Operational metro network across 26 Indian cities (2026)

£29 m
Reported cost of the 2024 Transport for London cyber attack

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 incident reporting, 180-day logs; risk-based independent cyber audits covering IT and OT/ICS
NCIIPC · CRS and CMRS safety regimes	Transport is a notified critical sector with protected-system duties; safety certification depends on trustworthy signalling and control
RBI and NPCI · PCI DSS	Card tokenisation, NETC and NCMC scheme rules and PCI DSS for ticketing, fare and toll payments
DPDP · SEBI LODR	Passenger and employee data safeguards from May 2027; quarterly cyber incident disclosure for listed railway PSUs

OUR SERVICE OFFERINGS

One partner from the control room to the ticket

Built around our primary proposition for the sector: **Ticketing and API testing, communications and OT assessments, SOC and incident exercises.**

Ticketing & API Testing

- PRS, UTS, AFC, toll and bus ticketing platform testing
- Mobile app and API security (OWASP, bot and fraud resistance)
- Payment, NCMC and FASTag integration reviews
- Pre-launch testing for new apps and corridors

Signalling & OT Assessment

- Interlocking, Kavach, CBTC and OCC architecture reviews
- Traction SCADA, depot and station system assessments
- IEC 62443-aligned gap analysis with safety teams
- Passive, planned methods that respect safety cases

Communications Security

- Train radio, GSM-R/LTE-R and telecom network reviews
- Passenger information, PA and display system security
- Station and depot network segmentation
- Wi-Fi, CCTV and IoT exposure reviews

24/7 IT/OT SOC

- Monitoring of stations, OCCs and enterprise IT
- Ticketing fraud and bot pattern detection
- Supplier remote-session monitoring
- 6-hour CERT-In reporting support

Incident Exercises

- Tabletops for ransomware, signalling and crowd scenarios
- Degraded-mode operation and recovery drills
- Crisis communication with passengers and media
- Joint exercises with suppliers and regulators

Passenger Data Protection

- DPDP programmes for passenger and commuter data
- Data mapping across apps, cards and CCTV
- Privacy by design for new platforms
- Breach readiness and intimation playbooks

Who we serve: Indian Railways zones and divisions · railway PSUs such as IRCTC, CRIS, RailTel, DFCCIL and RVNL · metro and RRTS corporations · state transport undertakings · toll concessionaires and FASTag issuers · ticketing, mobility and transit technology companies.

BUNDLED SERVICE MODELS

Packaged for how transport operators buy

Eleven Codec Networks bundles apply directly to rail, metro and surface transport organisations:

- **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

State transport undertakings, concessionaires and transit tech start-ups

- Ticketing and app security assessment
- IT and depot network review
- Backup and recovery review
- Policy, awareness and crisis plan pack

Assurance

Metro corporations, railway PSUs and tolling operators

- OT and signalling architecture assessment
- Ticketing, AFC and payment platform testing
- Annual independent audit
- 24x7 IT/OT SOC

Continuous Resilience

Indian Railways units, CII owners and multi-city operators

- Continuous testing and red teaming
- Kavach, CBTC and OCC security programmes
- SOC with threat hunting
- Board, regulator and NCIIPC reporting

Mapped to your obligations

Requirement	How we help	Bundle
Incidents to CERT-In in six hours; 180-day logs (CERT-In Directions)	IT/OT SOC, IR retainer, reporting support	B7, B8
Independent cyber audits incl. OT/ICS (CERT-In guidelines, 2025)	Independent IT/OT audits	B4, B1
Protected systems and CII duties (NCIIPC, IT Act s.70A)	CII-aligned assessments and controls	B4, B3
Safety certification of signalling and control (CRS, CMRS)	Signalling and OT security reviews	B1, B5
Card tokenisation, NETC and NCMC rules; PCI DSS (RBI, NPCI)	Payment flow testing, PCI DSS readiness	B2, B5
Quarterly incident disclosure, listed PSUs (SEBI LODR)	Incident records, disclosure support	B4, B8
Passenger, commuter and employee data (DPDP)	DPDPA programme	B6

THE CODEC NETWORKS VALUE ADD

Why transport operators choose Codec Networks

CERT-In empanelled

Independent IT/OT audits recognised by regulators, lenders and partners.

Certified and accountable

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

Safety-aware OT methods

Passive discovery and planned testing coordinated with signalling, operations and safety teams.

Platform-scale testing

Ticketing, AFC and toll platforms tested for bots, fraud and abuse at launch-day volumes.

Full stack, one partner

Testing, SOC, forensics, privacy and exercises connected from finding to closure.

Certified experts

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

How we engage

Discover & scope

Networks and corridors, signalling and control systems, ticketing, fare and toll platforms, suppliers with remote access, passenger data and your 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 launch, audit and incident a non-event.

Tell us your corridors, control systems, ticketing platforms and suppliers. We will propose a practical, safety-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: Ministry of Railways, MoHUA, UK National Crime Agency reporting, CERT-In. Confirm obligations against the official instruments.