Codec Networks
Coding Threats. Decoding Solutions.



INDUSTRY BROCHURE · MARITIME, PORTS & SHIPPING

Keep the Cargo Moving. Keep the Port Running.

Port IT/OT security, cargo platform testing, remote access controls, SOC and recovery for major and non-major ports, terminal operators, shipping lines and ship managers, shipyards and inland waterway operators.

- Port IT/OT Security
- Cargo Platform Testing
- Remote Access Controls
- 24/7 IT/OT SOC
- Recovery & Resilience
- Ship Cyber Risk

THE CHALLENGE

A port that cannot see its yard stops trade.

Ports and ships run cranes, gates, navigation and engine systems alongside the trade platforms that release cargo—often maintained by OEMs with remote access. NotPetya cost Maersk US$250–300 million in 2017; DP World Australia's 2023 incident stranded about 30,000 containers; and ransomware halted Japan's Port of Nagoya for two days in 2023.



What keeps leadership teams awake

- Ransomware halting terminals and gates
- Intrusion into cranes, SCADA and ship systems
- OEM and vendor remote access
- Cargo release and manifest fraud
- GNSS spoofing and navigation interference
- CERT-In, NCIIPC, IMO, ISPS and DPDP obligations

915 MT
Cargo handled by India's major ports in 2025-26

30,000
Containers stranded by the 2023 DP World Australia cyber incident

US$300 m
Upper estimate of Maersk's NotPetya losses (2017)

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
IMO MSC.428(98) · IACS UR E26/E27 · DGS	Cyber risk in ship safety management systems since 2021; cyber resilience for new ships contracted from July 2024
ISPS Code · NCIIPC	Port facility security assessments and plans; transport is a notified critical sector with protected-system duties
DPDP · SEBI LODR	Customer, crew and visitor data safeguards from May 2027; quarterly cyber incident disclosure for listed operators

OUR SERVICE OFFERINGS

One partner from the quay crane to the cargo portal

Built around our primary proposition for the sector: **Port IT/OT security, cargo platform testing, remote access controls, SOC and recovery.**

Port IT/OT Security

- Crane, RTG, gate, conveyor and SCADA assessments
- IEC 62443-aligned terminal architecture reviews
- Safe, passive methods planned with operations
- Marine OT: VTS, pilotage and port radio reviews

Cargo Platform Testing

- TOS, PCS 1x and customer portal testing
- API security for customs, forwarder and rail links
- Fraud-resistance testing of release and billing flows
- Pre-go-live testing for new terminals and systems

Remote Access Controls

- Brokered OEM and integrator access with recording
- Ship-to-shore and satcom access reviews
- Contractor and dredging partner controls
- Access recertification

24/7 IT/OT SOC

- Terminal, port and enterprise monitoring
- Industrial protocol and OEM-session detection
- Cargo platform fraud and anomaly analytics
- 6-hour CERT-In reporting support

Recovery & Resilience

- Immutable backups of TOS, gate and PLC configurations
- Manual yard, gate and berth playbooks
- Tested restore times and vendor image readiness
- Port crisis exercises with customers and customs

Ship Cyber Risk

- MSC.428(98) cyber risk assessments for the SMS
- IACS UR E26/E27 readiness for newbuilds
- ECDIS, GNSS, AIS and engine-room reviews
- Bridge and crew awareness and drills

Who we serve: major port authorities · non-major ports and state maritime boards · PPP terminal operators · shipping lines, ship owners and managers · shipyards and repair yards · inland waterway, coastal and dredging operators.

BUNDLED SERVICE MODELS

Packaged for how ports and shipping companies buy

Eleven Codec Networks bundles apply directly to ports, terminals and shipping 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

Non-major ports, single terminals and ship managers

- IT and terminal OT assessment
- OEM remote access review
- Backup and recovery review
- Policy, awareness and crisis plan pack

Assurance

Major ports and multi-terminal operators

- IEC 62443 assessment and segmentation
- TOS, PCS 1x and portal testing
- Annual independent audit
- 24x7 IT/OT SOC

Continuous Resilience

Listed port groups, large fleets and CII owners

- Continuous OT testing and red teaming
- Fleet-wide ship cyber programmes
- SOC with threat hunting
- Board, regulator and customer 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
Cyber risk in ship safety management systems (IMO MSC.428(98))	Ship cyber risk assessments, SMS procedures	B5, B1
Cyber resilience of new ships (IACS UR E26/E27, from July 2024)	Newbuild readiness and verification	B5, B9
Port facility security assessments and plans (ISPS Code, DGS)	Cyber elements in PFSA and PFSP	B4, B1
Protected systems and CII duties (NCIIPC, IT Act s.70A)	CII-aligned assessments and controls	B4, B3
Customer, cargo and seafarer personal data (DPDP)	DPDPA programme	B6

THE CODEC NETWORKS VALUE ADD

Why ports and shipping companies choose Codec Networks

CERT-In empanelled

Independent IT/OT audits recognised by regulators, customers and insurers.

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 terminal operations and marine teams.

Standards-mapped

Findings mapped to IEC 62443, ISO/IEC 27001, IMO MSC.428(98), IACS URs and CERT-In expectations.

Full stack, one partner

OT testing, cargo platform assurance, SOC, forensics and exercises connected from finding to closure.

Certified experts

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

How we engage

Discover & scope

Terminals and berths, cranes, gates and SCADA, TOS and PCS integrations, OEMs and contractors with remote access, ships and fleets, 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 go-live, audit and incident a non-event.

Tell us your terminals, control systems, cargo platforms, vendors and fleet. 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: MoPSW, public reporting on DP World Australia and Maersk, CERT-In. Confirm obligations against the official instruments.