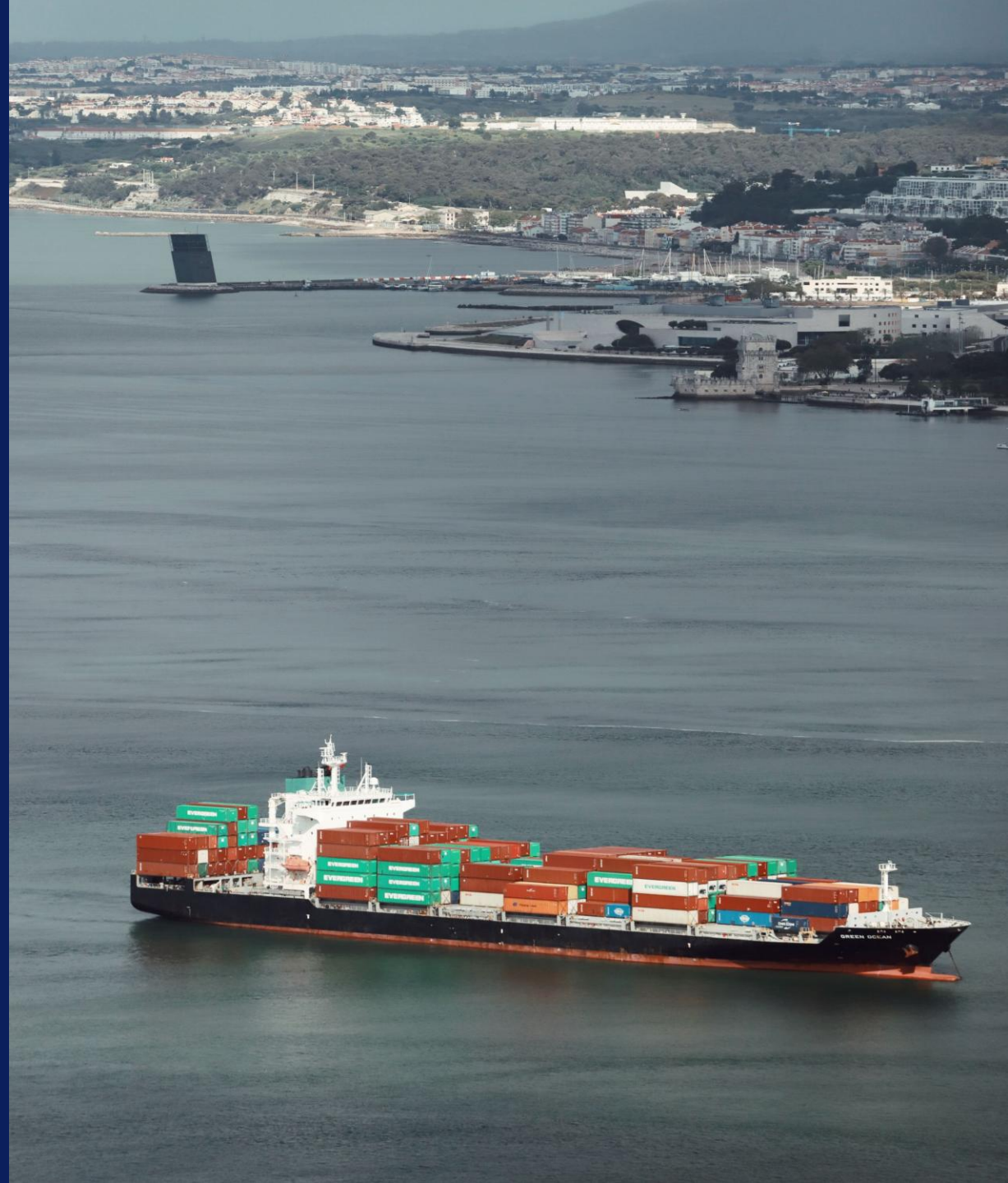
Codec Networks

Coding Threats. Decoding Solutions.

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 ports, terminals, shipping companies, shipyards and waterway operators



What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

CERT-In, NCIIPC, IMO and flag state, ISPS, the new Ports and Merchant Shipping Acts and DPDP

How Codec Networks helps

Services, bundles and packages built for the sector

Proof in scenarios

Five new case studies and the controls that break the chain

Why Codec Networks and next steps

Our value add and how to start



Cyber incidents in ports and shipping stop trade

Global incidents show the operational and economic stakes

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

What this means: ports and shipping companies must separate terminal OT and cargo systems from office IT, broker OEM and vendor access, test the platforms that release cargo, make TOS and control systems recoverable, monitor IT and OT around the clock and report incidents within six hours.

Sources: MoPSW, public reporting on DP World Australia and Maersk, CERT-In.

Who we serve across maritime, ports and shipping

Major ports

Port authorities and their terminals

Non-major ports

State maritime boards, private ports

Terminal operators

Container, bulk, liquid, Ro-Ro

Shipping lines

Container, tanker, bulk, coastal

Ship managers

Technical and crew management

Shipyards

Shipbuilding, repair, offshore

Inland waterways

IWAI terminals, barge operators

Port services

Pilotage, towage, dredging, bunkering

The threats that cost ports and shipping companies the most

Six priorities from our 18-threat sector assessment

Ransomware shutdowns

TOS, gates and back office stopped

Terminal OT intrusion

Cranes, PLCs and SCADA reached from outside

OEM and vendor access

Standing links and shared accounts

Cargo release fraud

Portal takeover and altered delivery orders

Ship system compromise

ECDIS, GNSS spoofing, engine control

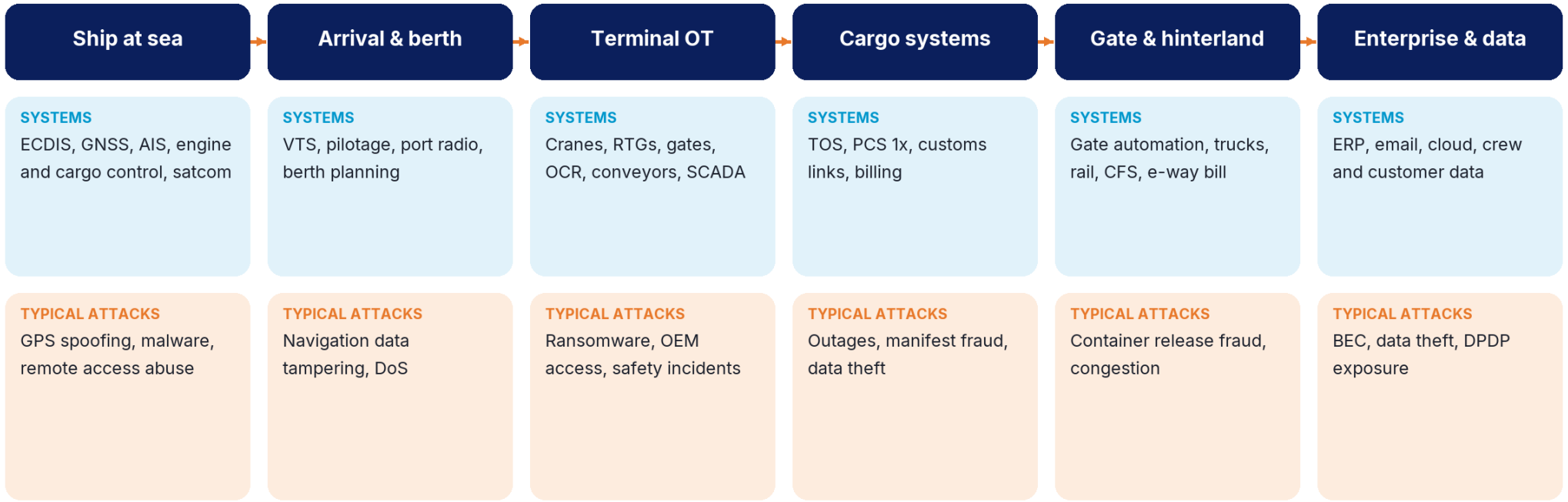
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from ship to hinterland

Where Cyber Risk Sits Across the Maritime and Port Value Chain

Every stage from ship to hinterland carries its own attack surface



A port that cannot see its yard or release a container stops trade—OT security, cargo platform assurance and recovery must be planned together.

Source: Codec Networks analysis

Codec Networks

Codec Networks
Coding Threats. Decoding Solutions.

What regulators now expect

CERT-In, NCIIPC, IMO and flag state, ISPS, the new Ports and Merchant Shipping Acts and DPDP

Codec Networks
Coding Threats. Decoding Solutions.

The rules and standards shaping maritime and port cybersecurity

Requirement	Frequency / deadline	Source
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
ICT log retention	180 days, in India	CERT-In Directions, 2022
Independent cyber audits	Risk-based, incl. OT/ICS	CERT-In audit guidelines, 2025
Protected systems and CII	Per notification	NCIIPC (IT Act Section 70A)
Cyber risk in ship safety management	From first DOC verification after 1 Jan 2021	IMO MSC.428(98); DGS circular
Cyber resilience of new ships	Ships contracted from 1 July 2024	IACS UR E26/E27
Port facility security assessment and plan	Per ISPS cycle	ISPS Code; MS (Ships and Port Facility Security) Rules 2024
Cyber incident disclosure (listed operators)	Quarterly corporate governance report	SEBI LODR, 2023
Customer, crew and visitor data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Key dates on the regulatory timeline

Regulatory and Standards Timeline Shaping Maritime and Port Cybersecurity

International, sector and cross-sector instruments and the standards that connect them

In force Upcoming (from Oct 2026)

2000	Information Technology Act, 2000; amended 2008 with CERT-In and protected systems (Section 70A)
2004	ISPS Code in force; DG Shipping acts as India's designated authority for port facility security
Mar 2015	Sagarmala programme launched for port-led development
Jun 2017	IMO Resolution MSC.428(98): cyber risk management in safety management systems
2017	DG Shipping circular on cyber risk in the SMS of Indian-flag ships; MSC-FAL.1/Circ.3 guidelines
Dec 2018	Port Community System PCS 1x launched by the Indian Ports Association
Jan 2021	Cyber risk to be addressed in SMS by the first annual DOC verification after 1 January 2021
Apr 2022	CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Jul 2023	SEBI LODR amendment: listed companies disclose cyber incidents quarterly
Jul 2024	IACS UR E26/E27 cyber resilience applies to new ships contracted from 1 July 2024; MS (Ships and Port Facility Security) Rules
Jul 2025	CERT-In Comprehensive Cyber Security Audit Policy Guidelines
Aug 2025	Indian Ports Act, 2025 and Merchant Shipping Act, 2025 notified, replacing the 1908 and 1958 Acts
Nov 2025	DPDP Rules, 2025 notified with phased commencement
May 2027	**Most DPDP Rules obligations, incl. breach intimation, take effect**

Sources: IMO, IACS, DG Shipping, MoPSW, IPA, MeitY, CERT-In, SEBI. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Port IT/OT · Cargo platforms · Remote access · IT/OT SOC · Recovery · Ship cyber risk

Codec Networks
Coding Threats. Decoding Solutions.

One partner from the quay crane to the cargo portal

Port IT/OT Security

Cranes, gates, SCADA, marine OT

Cargo Platform Testing

TOS, PCS 1x, portals, customs APIs

Remote Access Controls

OEMs, integrators, ship-to-shore

24/7 IT/OT SOC

Monitoring and threat hunting

Recovery & Resilience

Backups, manual playbooks, exercises

Ship Cyber Risk

MSC.428(98), UR E26/E27, bridge systems

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services

- **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

Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

Non-major ports, single terminals and ship managers

- IT and terminal OT assessment (B1)
- OEM remote access review (B3, B9)
- Backup and recovery review (B3)
- Policy, awareness and crisis plan pack (B5)

Assurance

Major ports and multi-terminal operators

- IEC 62443 assessment and segmentation (B1, B3)
- TOS, PCS 1x and portal testing (B2)
- Annual independent audit (B4)
- 24x7 IT/OT SOC (B7)

Continuous Resilience

Listed port groups, large fleets and CII owners

- OT testing and red teaming (B1, B10)
- Fleet-wide ship cyber programmes (B5, B1)
- SOC with threat hunting (B7)
- Board and regulator reporting (B4, B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Terminal That Lost Its Yard**	Ransomware encrypts the TOS, gates and backups; segmentation and tested restores prevent it	**B3 · B7 · B10**
2	**The Crane That Took Remote Commands**	A compromised OEM link alters crane PLCs; brokered access and isolation stop it	**B9 · B1 · B7**
3	**The Container Released to the Wrong Truck**	Stolen portal logins divert cargo; testing, MFA and anomaly detection catch it	**B2 · B7 · B9**
4	**The Ship That Sailed on a Spoofed Position**	GNSS spoofing grounds a bulk carrier; integrity checks and drills prevent it	**B5 · B1 · B10**
5	**The Shipyard Design Files on a Foreign Server**	A subcontractor's stolen credentials leak designs; access control and hunting catch it	**B3 · B9 · B7**

Example: breaking a phishing-to-terminal-shutdown chain

Case 1: The Terminal That Lost Its Yard

ILLUSTRATIVE ATTACK PATH

Step 1
Attackers phish a terminal planner and move laterally to domain control over weeks

→

Step 2
Ransomware encrypts the terminal operating system, gate servers and the backup server

→

Step 3
Cranes work but nobody knows where containers are; gates close and trucks queue for kilometres

→

Step 4
Ships are diverted to other ports; customers invoke service credits

→

Step 5
Rebuilding from a vendor image takes nine days; the incident is disclosed quarterly

WHERE CONTROLS BREAK THE CHAIN

- Segmentation of TOS, gate and OT networks from office IT
- Immutable, offline backups with tested TOS restore times
- 24x7 SOC with EDR monitoring and threat hunting
- Manual yard and gate continuity playbooks

Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: whether TOS, gate and OT networks are separated from office IT, whether backups are immutable and TOS restore times are proven, whether EDR alerts are watched around the clock, whether manual yard and gate playbooks exist, and how operations, customers and customs respond in a tabletop exercise.

Why ports and shipping companies choose Codec Networks

CERT-In empanelled

For information security auditing services; NICSI empanelled for application audits

Certified

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

Regulation-mapped

Mapped to CERT-In, NCIIPC, IMO MSC.428(98), IACS UR E26/E27, ISPS and DPDP expectations and IEC 62443

Tests the whole chain

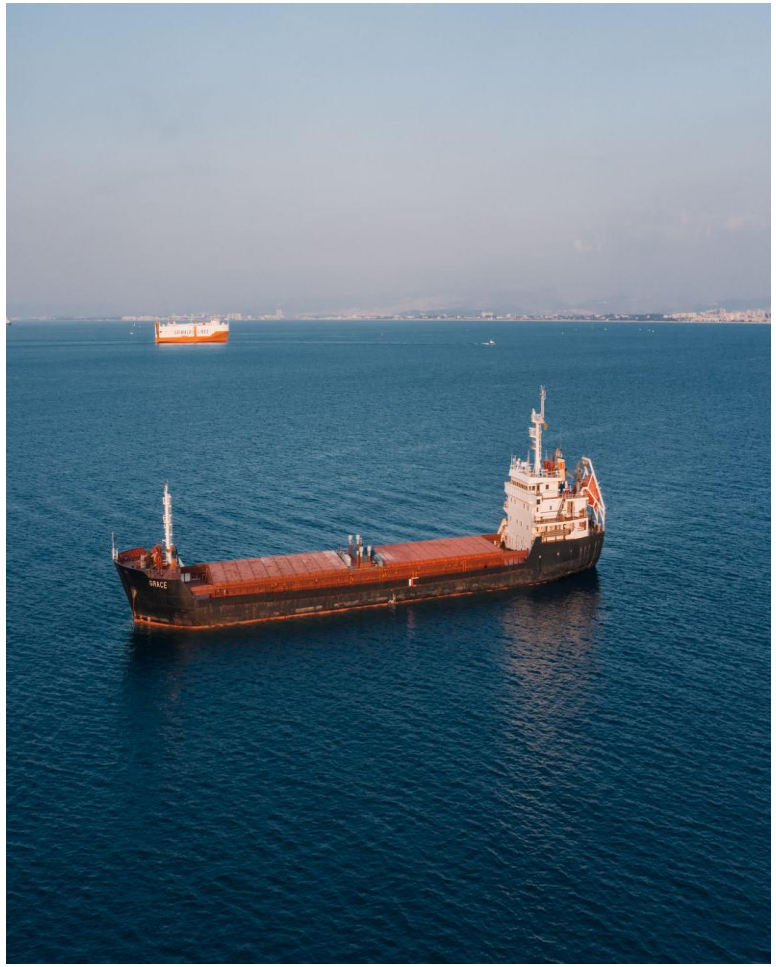
Technical, process and monitoring tests together

Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected

Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST



How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement



Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Terminals, cranes and SCADA, TOS and PCS integrations, OEMs and contractors with remote access, ships and fleets, and your audit calendar

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

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

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

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.

Codec Networks
Coding Threats. Decoding Solutions.