

Codec Networks

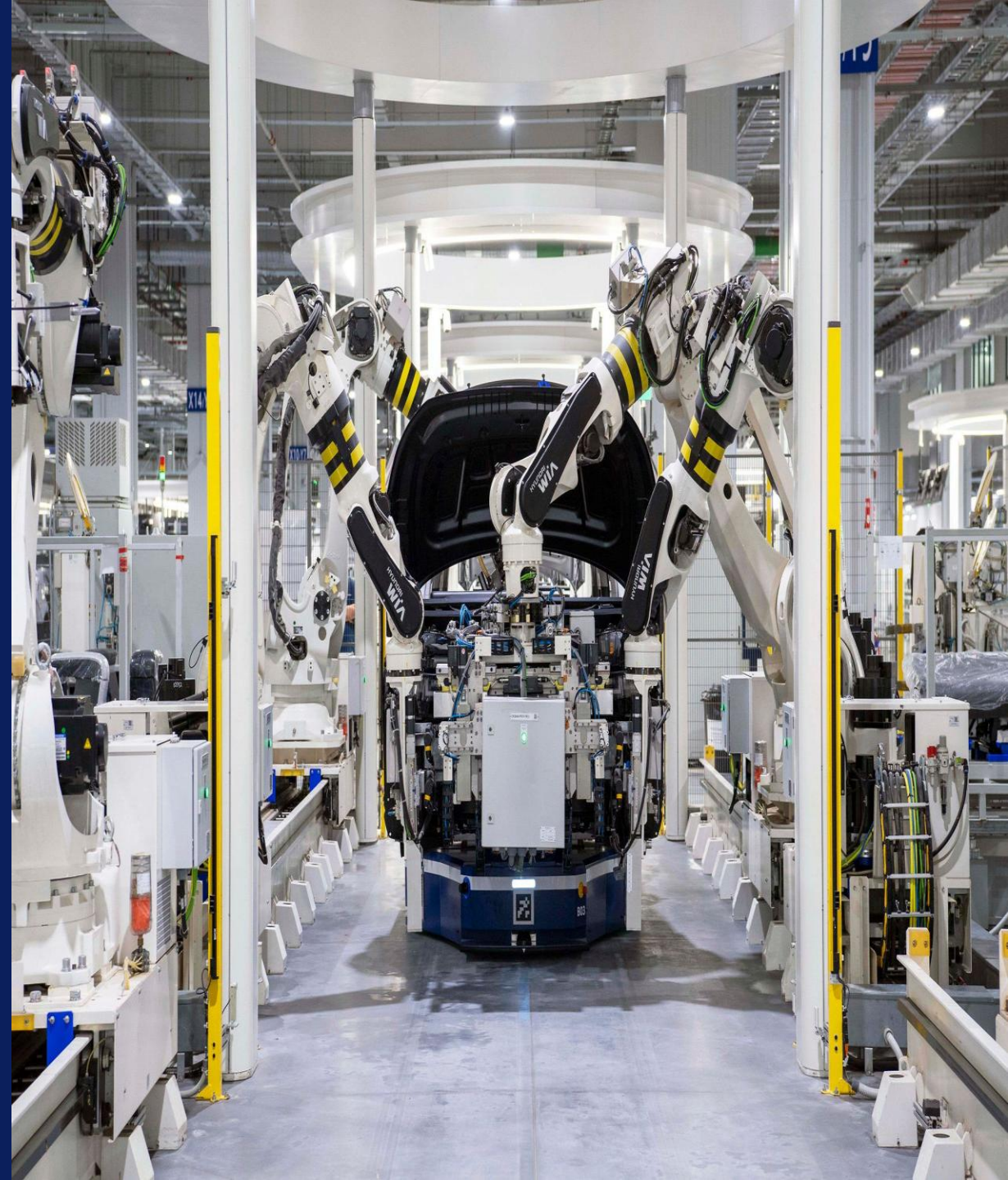
Coding Threats. Decoding Solutions.

MANUFACTURING & INDUSTRIAL PRODUCTION

Keep the Lines Running. Keep the Designs In.

IEC 62443-aligned assessments, OT segmentation, ransomware resilience and ERP security for manufacturing and industrial production companies

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

CERT-In, SEBI, DPDP and the customer and export rules that reach Indian plants



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 manufacturing stop production

Global data and incidents show the operational stakes

5 years

Manufacturing the most
attacked industry (IBM X-Force)

> 50%

Of industrial ransomware victims
are manufacturers (Dragos)

14 plants

Halted by one supplier's cyber
incident (Toyota, 2022)

6 hours

To report cyber incidents to
CERT-In

What this means: manufacturers must separate the plant from IT, make ERP and MES recoverable, control OEM and supplier access, protect designs, monitor IT and OT around the clock and report incidents within six hours.

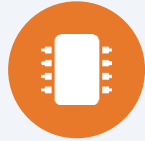
Sources: IBM X-Force Threat Intelligence Index 2026, Dragos OT Cybersecurity Report 2025, public reporting, CERT-In.

Who we serve across manufacturing and industrial production



Capital goods and heavy engineering

Turbines, boilers, plant equipment



Electronics and EMS

PCBs, devices, contract electronics



Industrial machinery

Machine tools, automation, pumps



Electrical equipment

Switchgear, motors, transformers



Components and contract manufacturers

Castings, precision parts, sub-assemblies



Smart factories

Industry 4.0, IIoT, digital twins



Engineering PSUs and strategic units

Public-sector and strategic production



Exporters and OEM suppliers

Global supply chains and projects

The threats that cost manufacturers the most

Six priorities from our 18-threat manufacturing assessment



Ransomware shutdowns

ERP, MES and plants encrypted



Supplier outages

One supplier's incident stops your lines



OEM remote access abuse

Maintenance tunnels into PLCs



Design and IP theft

CAD, recipes and customer data



Flat IT/OT networks

Malware reaching the plant floor



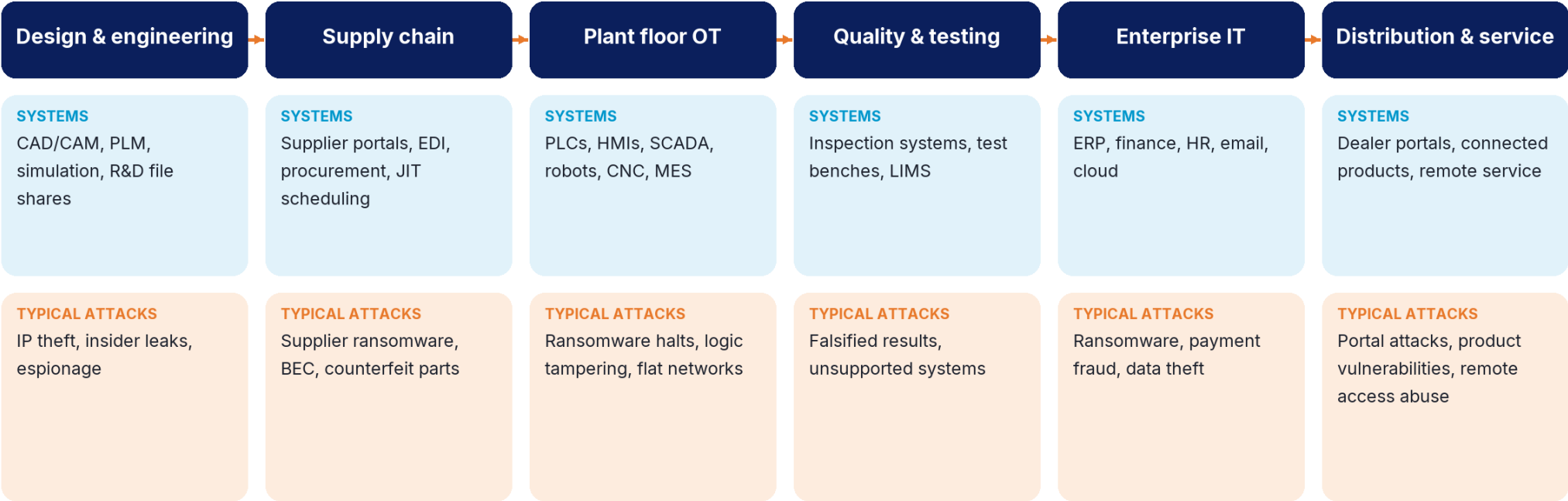
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from design to dispatch

Where Cyber Risk Sits Across the Manufacturing Value Chain

Every stage from design to after-sales carries its own attack surface



In manufacturing, a day of downtime is lost output that cannot be recovered—and a stolen design is lost forever.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, SEBI, DPDP and the customer and export rules that reach Indian plants

The rules and standards shaping manufacturing 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	CERT-In audit guidelines, 2025
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023
Protected systems	Per notification	NCIIPC (IT Act Section 70A)
Employee, dealer and consumer data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Connected product security	Reporting from Sep 2026; full from Dec 2027	EU Cyber Resilience Act
Industrial security good practice	Standards	IEC 62443; ISO/IEC 27001

Key dates on the regulatory timeline

Regulatory and Standards Timeline Shaping Manufacturing Cybersecurity

Cross-sector Indian instruments, listed-company rules and the export requirements that reach Indian plants

● In force

● Upcoming (from Oct 2026)

2000	● Information Technology Act, 2000 enacted; CERT-In and critical information infrastructure provisions added by the 2008 amendment
Sep 2014	● Make in India launched to raise manufacturing's share of the economy
2020	● Production Linked Incentive (PLI) schemes approved for 14 sectors with an outlay of about ₹1.97 lakh crore
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 in the quarterly corporate governance report
Aug 2023	● Digital Personal Data Protection Act, 2023 enacted
Dec 2024	● EU Cyber Resilience Act enters into force for products with digital elements sold in the EU
Feb 2025	● National Manufacturing Mission announced in the Union Budget 2025-26
Jul 2025	● CERT-In Comprehensive Cyber Security Audit Policy Guidelines
Nov 2025	● DPDP Rules, 2025 notified with phased commencement
Sep 2026	● EU CRA vulnerability and incident reporting obligations apply to manufacturers
May 2027	● Most DPDP Rules obligations, incl. breach intimation, take effect
Dec 2027	● EU CRA essential requirements and CE marking fully apply

Sources: MeitY, CERT-In, SEBI, DPIIT, EU Official Journal. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

IEC 62443 · Segmentation · Resilience · ERP & MES · Suppliers · IT/OT SOC

One partner from design to dispatch



IEC 62443 Assessments

OT inventory, PLCs, SCADA, MES, robots



OT Segmentation

Plant DMZ, remote access, IIoT isolation



Ransomware Resilience

Backups, playbooks, exercises



ERP & MES Security

Configuration, portals, payment controls



Supplier Cyber Risk

Critical supplier assessments



24/7 IT/OT SOC

Monitoring and threat hunting

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



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

Component makers, MSMEs and single plants

- IT and plant assessment (B1)
- Backup and recovery review (B3)
- OEM remote access review (B3, B9)
- Policy and questionnaire pack (B5)

Assurance

Mid-sized manufacturers and multi-plant groups

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

Continuous Resilience

Large manufacturers, exporters and PSUs

- OT testing and red teaming (B1, B10)
- Supplier cyber risk programme (B9)
- SOC with threat hunting (B7)
- Board, SEBI and customer reporting (B4, B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Cyber incidents to CERT-In within six hours; 180-day logs (CERT-In Directions)	IT/OT SOC, IR retainer and reporting support	B7, B8
Risk-based independent cyber audits including OT (CERT-In audit guidelines, 2025)	Independent IT/OT audits	B4, B1
Quarterly cyber incident disclosure by listed companies (SEBI LODR)	Incident records, disclosure support	B4, B8
Protection of any notified protected systems (NCIIPC)	CII-aligned assessments and controls	B4, B3
Employee, dealer and consumer personal data (DPDP)	DPDPA programme	B6
Customer security questionnaires and audits (OEM, EU, US contracts)	ISO 27001, IEC 62443 and questionnaire readiness	B5, B9
Connected product security and vulnerability reporting (EU CRA)	Product and firmware security assessment	B2, B11

Five new case studies, five broken chains

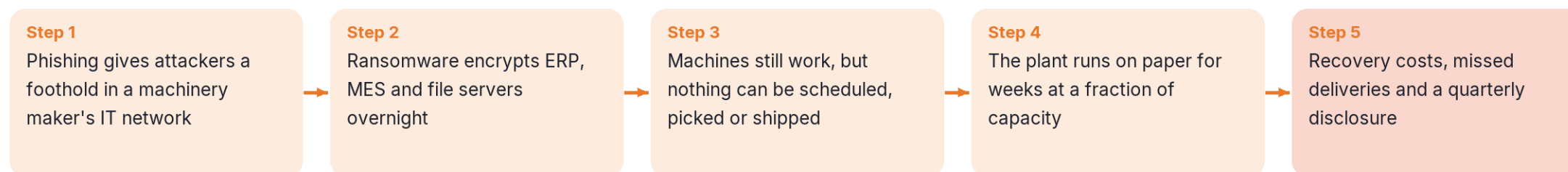
Illustrative composite scenarios written for 2026—not client engagements

1	The Supplier That Stopped Fourteen Lines	A tier-2 supplier's ransomware halts an OEM's lines; supplier assessments and buffers prevent it	B9 · B10 · B7
2	The ERP That Ran the Plant	Ransomware encrypts ERP and MES; segmentation and tested backups keep shipping	B3 · B7 · B8
3	The Maintenance Tunnel Nobody Closed	A phished OEM account reaches PLCs; brokered access and OT monitoring stop it	B9 · B1 · B7
4	The Drawings That Walked Out	A leaver copies CAD and recipes; DLP and activity monitoring catch it	B3 · B7 · B8
5	The Smart Factory Pilot That Opened the Door	An exposed IIoT gateway reaches HMIs; assessment and isolation prevent it	B11 · B3 · B1

Example: breaking an ERP-to-plant shutdown chain

Case 2: The ERP That Ran the Plant

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: which plant processes depend on ERP and MES, IT/OT segmentation and DMZ design, the ability to run and ship without IT, immutable backups and restore times, EDR and SOC detection, and crisis decision-making in a tabletop exercise with plant leadership.

Why manufacturers choose Codec Networks



CERT-In empanelled

For information security auditing services; NISII empanelled for application audits



Certified

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



Regulation-mapped

Mapped to IEC 62443, ISO/IEC 27001, CERT-In expectations and your customers' requirements



Tests the whole chain

Technical, process and monitoring tests together



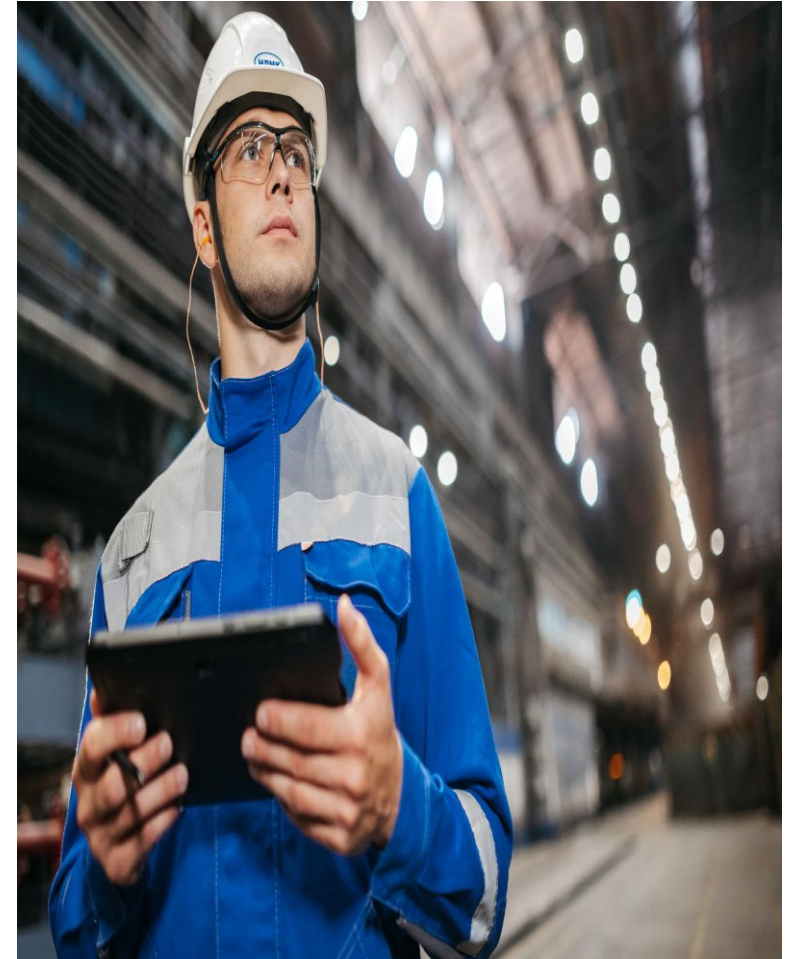
Full stack, one partner

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 MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Plants, PLCs, MES and ERP, OEM access, critical suppliers, connected products and your audit and customer 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.