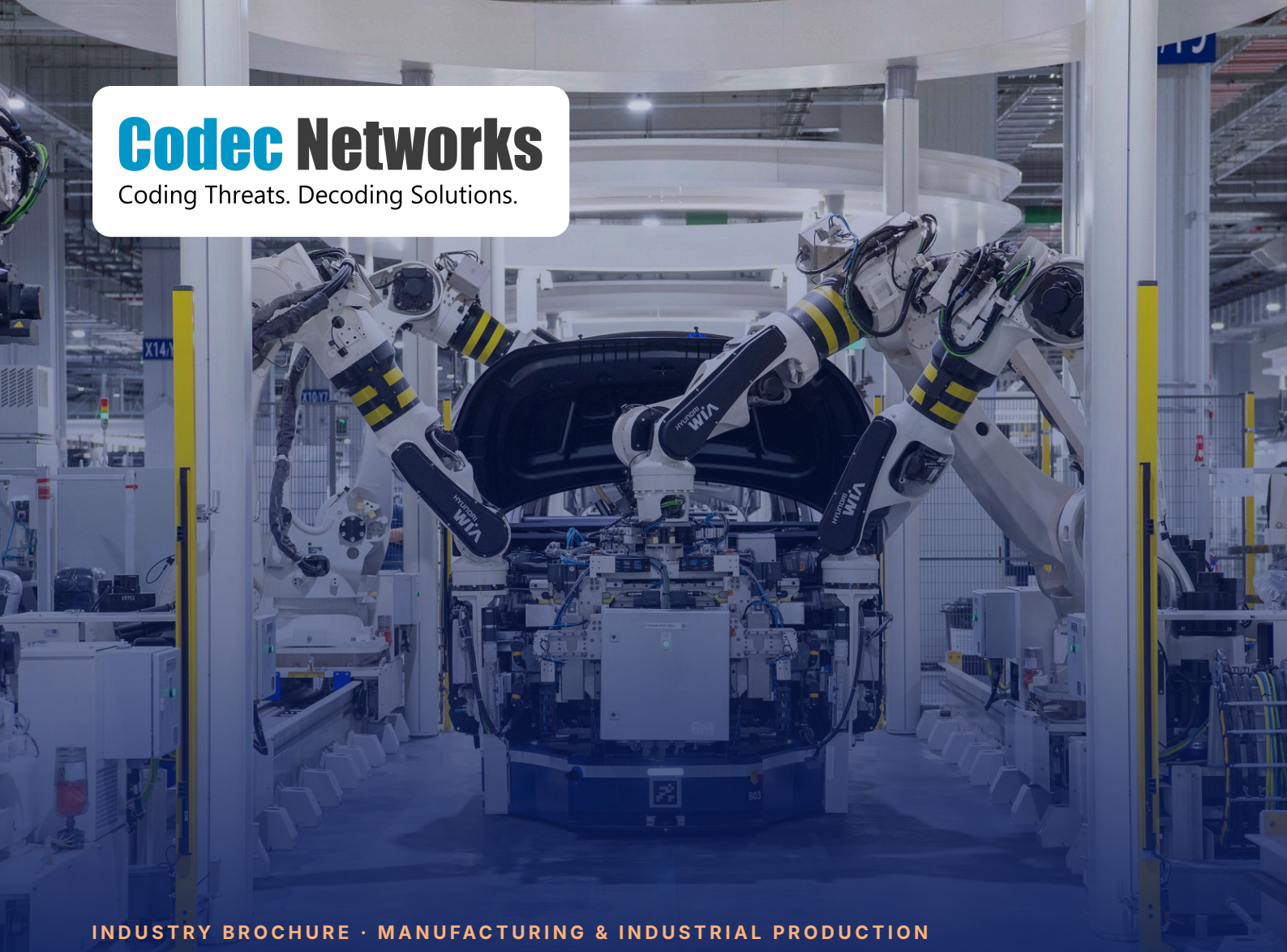


Codec Networks
Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · MANUFACTURING & INDUSTRIAL PRODUCTION

Keep the Lines Running. Keep the Designs In.

IEC 62443-aligned assessments, OT segmentation, ransomware resilience and ERP security for engineering, machinery, electronics, industrial equipment, component makers and smart factories.

- IEC 62443 Assessments
- OT Segmentation
- Ransomware Resilience
- ERP & MES Security
- Supplier Cyber Risk
- 24/7 IT/OT SOC

THE CHALLENGE

In manufacturing, a cyber incident is a production incident.

Manufacturing has been the most attacked industry worldwide for five years running, and more than half of industrial ransomware victims are manufacturers. Plants depend on ERP, MES and PLCs that were never designed to face the internet, on OEMs with remote access, and on suppliers whose outage becomes yours—as Toyota found in 2022 when one supplier's incident halted all fourteen of its Japanese plants.



What keeps leadership teams awake

- Ransomware that stops the plant and the shipments
- A supplier's incident halting just-in-time lines
- OEM remote maintenance access nobody controls
- Theft of designs, recipes and customer data
- ERP, MES and PLCs on one flat network
- CERT-In reporting, SEBI disclosure and customer audits

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

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
SEBI LODR · Companies Act	Listed manufacturers disclose cyber incidents quarterly; Boards are accountable for risk management
DPDP Act and Rules (2023, 2025)	Safeguards for employee, dealer and consumer data; most obligations from May 2027
Customer and export rules	EU Cyber Resilience Act for connected products (reporting from Sep 2026), NIS2 supply-chain duties, OEM questionnaires; IEC 62443 and ISO 27001 as the common language

Codec Networks
Coding Threats. Decoding Solutions.

OUR SERVICE OFFERINGS

One partner from design to dispatch

Built around our primary proposition for the sector: **IEC 62443-aligned assessments, OT segmentation, ransomware resilience and ERP security.**

IEC 62443 Assessments

- OT asset inventory and zone-and-conduit architecture review
- PLC, HMI, SCADA, robot and MES assessments
- Safe, passive testing planned with production
- Gap assessment against IEC 62443 and ISO/IEC 27001

OT Segmentation

- IT/OT and plant DMZ design
- Removal of dual-homed and flat networks
- Secure OEM and vendor remote access
- IIoT and edge network isolation

Ransomware Resilience

- Attack-path assessment and EDR validation
- Immutable backups and restore testing for ERP and MES
- Manual-operation and restart playbooks
- Leadership and plant tabletop exercises

ERP & MES Security

- ERP, MES and PLM configuration and access reviews
- Dealer, supplier and service portal testing
- Payment and master-data change controls
- Cloud ERP and SaaS posture reviews

Supplier Cyber Risk

- Assessment of critical and single-source suppliers
- Contract security and notification clauses
- Supplier onboarding and recertification
- Joint supplier incident exercises

24/7 IT/OT SOC

- IT and plant network monitoring
- Industrial protocol threat detection
- Threat hunting and remote-session monitoring
- 6-hour CERT-In reporting support

Who we serve: capital goods and heavy engineering · electronics and EMS · industrial machinery and equipment · components and contract manufacturers · smart factories · engineering PSUs and strategic units.

BUNDLED SERVICE MODELS

Packaged for how manufacturers buy

Eleven Codec Networks bundles apply directly to manufacturing and industrial production 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

Component makers, MSMEs and single plants

- IT and plant assessment
- Backup and recovery review
- OEM remote access review
- Policy pack and customer questionnaire support

Assurance

Mid-sized manufacturers and multi-plant groups

- IEC 62443 assessment and segmentation
- ERP and portal testing
- Annual independent audit
- 24x7 IT/OT SOC

Continuous Resilience

Large manufacturers, exporters and PSUs

- Continuous OT testing and red teaming
- Supplier cyber risk programme
- SOC with threat hunting
- Board, SEBI and customer reporting

Mapped to your obligations

Requirement	How we help	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

THE CODEC NETWORKS VALUE ADD

Why manufacturers choose Codec Networks

CERT-In empanelled

Independent IT/OT audits recognised by regulators and customers.

Certified and accountable

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

Production-aware OT methods

Passive discovery and planned testing coordinated with plant and maintenance teams.

Standards-mapped

Findings mapped to IEC 62443, ISO/IEC 27001, CERT-In and customer frameworks.

Full stack, one partner

IT/OT testing, SOC, forensics, supplier risk and exercises connected from finding to closure.

Certified experts

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

How we engage

Discover & scope

Plants and lines, PLCs, MES and ERP, OEMs with remote access, critical suppliers, connected products and your audit and customer 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 audit, customer review and incident a non-event.

Tell us your plants, control systems, suppliers and customers. We will propose a practical, production-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: IBM X-Force Threat Intelligence Index 2026, Dragos OT Cybersecurity Report 2025, public reporting, CERT-In. Confirm obligations against the official instruments.