



Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · METALS, MINING & CEMENT

Keep the Furnaces Hot. Keep the Mines Moving.

Industrial security, remote operations protection, 24x7 IT/OT SOC and ERP and supply chain assessments for mining groups, steel and aluminium producers, smelters, foundries and cement manufacturers.

Industrial Security

Remote Operations Protection

ERP & Dispatch Security

Supply Chain Assessment

24/7 IT/OT SOC

Ransomware Resilience

Coding Threats. Decoding Solutions.

www.codecnetworks.com

THE CHALLENGE

In metals, mining and cement, a cyber incident stops output.

India is the world's second-largest producer of steel and cement and mined over a billion tonnes of coal in FY 2024-25. The furnaces, kilns, fleets and dispatch systems behind those numbers run continuously at remote sites on decades-old control systems connected to ERP, OEMs and contractors. Norsk Hydro ran plants manually for weeks after ransomware in 2019.

What keeps leadership teams awake

- Ransomware stopping dispatch while kilns run
- Remote operations and fleets reached from outside
- OEM, MDO and contractor access uncontrolled
- Weighbridge, e-permit and dispatch data altered
- Captive power and safety on flat networks
- CERT-In reporting, SEBI disclosure and NCIIPC



2nd

Largest producer of crude steel and cement in the world

NOK 600 m

Norsk Hydro's first-half 2019 ransomware cost (550–650 m)

May 2025

Nucor halted production at several sites after a cyber incident

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 audits covering IT and OT/ICS
NCIIPC · SEBI LODR	Protection of notified protected systems; listed producers disclose cyber incidents quarterly
DPDP Act and Rules (2023, 2025)	Safeguards for employee, contractor and dealer data; most obligations from May 2027
Sector statutes and export rules	MMDR Act, OSH Code and DGMS, state e-permits; EU CBAM data from January 2026; IEC 62443

One partner from pit to port

Built around our primary proposition for the sector: **industrial security, remote operations protection, SOC, and ERP and supply chain assessment.**

Industrial Security

- OT asset inventory across plants, mines and captive power
- DCS, PLC, HMI, furnace, kiln and mill assessments
- Safe, passive testing planned with operations
- Gap assessment against IEC 62443 and ISO/IEC 27001

Remote Operations Protection

- Remote operations centre architecture review
- Fleet management, dispatch and autonomy system testing
- Site link and wireless network security
- Brokered OEM, MDO and contractor access

ERP & Dispatch Security

- ERP, sales and procurement configuration and access reviews
- Weighbridge, e-permit and gate system testing
- E-auction, trading and customer portal testing
- Payment, master-data and dispatch change controls

Supply Chain Assessment

- Assessment of MDOs, EPC and maintenance contractors
- Transporter, rail and port integration reviews
- Contract security and notification clauses
- Supplier onboarding and recertification

24/7 IT/OT SOC

- Monitoring across plants, mines and remote sites
- Industrial protocol and remote-session detection
- Dispatch and weighbridge anomaly analytics
- 6-hour CERT-In reporting support

Ransomware Resilience

- Dependency mapping for dispatch and control systems
- Immutable backups and restore testing
- Manual-operation and safe-stop playbooks
- Leadership, plant and mine tabletop exercises

Who we serve: coal, iron ore, bauxite and mineral mining groups · steel producers and integrated plants · aluminium, zinc and copper smelters · foundries and secondary metal producers · cement manufacturers · captive power and logistics units within them.

Packaged for how producers buy

Eleven Codec Networks bundles apply directly to metals, mining and cement 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

Single plants, foundries and mid-sized mines

- IT and plant assessment
- Backup and dispatch recovery review
- Vendor remote access review
- Policy pack and lender evidence

Assurance

Multi-site producers and mining groups

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

Continuous Resilience

Integrated groups, exporters and PSUs

- Continuous OT testing and red teaming
- Contractor and logistics risk programme
- SOC with threat hunting
- Board, SEBI and NCIIPC reporting

Mapped to your obligations

Requirement	How we help	Bundle
Cyber incidents to CERT-In within six hours; 180-day logs	IT/OT SOC, IR retainer and reporting support	B7, B8
Risk-based independent audits incl. OT (CERT-In guidelines 2025)	Independent IT/OT audits	B4, B1
Quarterly cyber incident disclosure by listed companies (SEBI)	Incident records, disclosure support	B4, B8
Protection of notified protected systems (NCIIPC)	CII-aligned assessments and controls	B4, B3
Employee, contractor and dealer personal data (DPDP)	DPDPA programme	B6
Mine safety and statutory records (OSH Code, DGMS, MMDR)	Safety system and records integrity reviews	B1, B5
Lender, buyer and CBAM data assurance (contracts, EU rules)	ISO 27001, IEC 62443 and evidence readiness	B5, B9

Why producers choose Codec Networks

CERT-In empanelled

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

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, mine and safety teams.

Standards-mapped

Findings mapped to IEC 62443, ISO/IEC 27001, CERT-In and NCIIIPC expectations.

Full stack, one partner

IT/OT testing, SOC, forensics, supply chain 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, mines and sites, DCS and PLCs, remote operations centres, ERP and dispatch, OEMs and contractors with access, and your audit, lender and disclosure 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, lender review and incident a non-event.

Tell us your plants, mines, control systems, contractors 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: Ministry of Steel, Economic Survey 2025-26, Hydro quarterly reporting (2019), Nucor Form 8-K (May 2025), CERT-In. Confirm obligations against the official instruments.