Codec Networks

Coding Threats. Decoding Solutions.

METALS, MINING & CEMENT

Keep the Furnaces Hot. Keep the Mines Moving.

Industrial security, remote operations protection, SOC and ERP and supply chain assessment for mining groups, metal producers, smelters, foundries and cement manufacturers

What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

CERT-In, NCIIPC, SEBI, DPDP, mining statutes and the export rules that reach Indian producers

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 metals, mining and cement stop output

Global incidents and India's scale show the operational stakes

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

What this means: producers must separate plants, mines and captive power from IT, make ERP and dispatch recoverable, control OEM and contractor access, protect dispatch and compliance data, monitor every site around the clock and report incidents within six hours.

Sources: Ministry of Steel, Economic Survey 2025-26, Hydro quarterly reporting (2019), Nucor Form 8-K (May 2025), CERT-In.

Who we serve across metals, mining and cement

Coal mining

Coal India, captive and commercial mines

Iron ore and mineral mining

Iron ore, bauxite, limestone, zinc, critical minerals

Steel producers

Integrated plants, mini mills, specialty steel

Aluminium and non-ferrous

Smelters, refineries, zinc and copper

Foundries and secondary metals

Castings, forgings, recyclers

Cement manufacturers

Integrated plants, grinding units, RMC

Captive power and utilities

Captive plants, substations, water and gas

Logistics and dispatch units

Rail sidings, ports, trucking, depots

The threats that cost producers the most

Six priorities from our 18-threat metals, mining and cement assessment

Ransomware shutdowns

ERP, dispatch and plant systems encrypted

Remote operations hijack

Fleets and dispatch reached from outside

Vendor and contractor access

OEM and MDO links into control networks

Dispatch and permit fraud

Weighbridge, e-permit and royalty data altered

Flat plant and mine networks

Malware reaching DCS and captive power

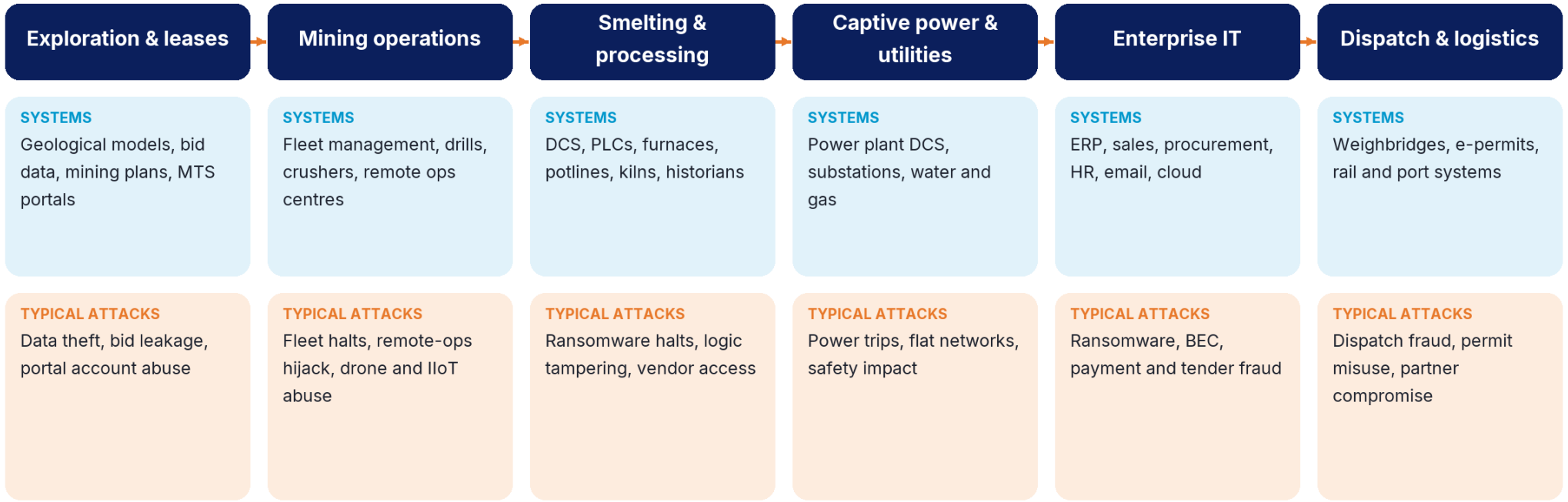
Slow detection at remote sites

Missing the 6-hour window

Attacks target every stage from exploration to dispatch

Where Cyber Risk Sits Across the Metals, Mining and Cement Value Chain

Every stage from exploration to dispatch carries its own attack surface



A blast furnace, potline or kiln cannot simply be switched off—an unplanned stop costs days of output and can damage the asset itself.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, NCIIPC, SEBI, DPDP, mining statutes and the export rules that reach Indian producers

Codec Networks
Coding Threats. Decoding Solutions.

The rules shaping metals, mining and cement 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
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023
Protected systems	Per notification	NCIIPC (IT Act Section 70A)
Employee, contractor and dealer data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Mine safety and statutory records	Continuous	OSH Code 2020; DGMS; MMDR Act
Embedded emissions data for EU exports	Definitive period from Jan 2026	EU CBAM
Industrial security good practice	Standards	IEC 62443; ISO/IEC 27001

Key dates on the regulatory timeline

Regulatory and Policy Timeline Shaping Metals, Mining and Cement Cybersecurity

Sector statutes, auction reforms, cross-sector Indian cyber instruments and the export rules that reach Indian producers

In force · Upcoming (from Oct 2026)

1952	Mines Act, 1952 governs mine safety, administered by the Directorate General of Mines Safety
1957	Mines and Minerals (Development and Regulation) Act, 1957 enacted
2000	Information Technology Act, 2000; CERT-In and protected-system provisions added in 2008
2017	National Steel Policy targets 300 million tonnes of capacity by 2030-31
Jun 2020	Commercial coal mining auctions begin; about 125 mines auctioned across eleven rounds
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
Aug 2023	DPDP Act enacted; MMDR amendment opens critical mineral auctions to the Centre
Jan 2025	National Critical Mineral Mission approved with a ₹34,300 crore outlay over seven years
Jul 2025	CERT-In Comprehensive Cyber Security Audit Policy Guidelines, including OT/ICS
Aug 2025	MMDR Amendment Act, 2025 passed to support the critical mineral mission
Nov 2025	DPDP Rules notified; OSH Code 2020 in force from 21 November, subsuming the Mines Act
Jan 2026	EU CBAM definitive period begins for steel, aluminium and cement imports
May 2027	**Most DPDP Rules obligations, including breach intimation, take effect**

Sources: Ministries of Mines, Coal and Steel, DGMS, MeitY, CERT-In, SEBI, EU Official Journal. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Industrial security · Remote operations · ERP & dispatch · Supply chain · IT/OT SOC · Resilience

Codec Networks
Coding Threats. Decoding Solutions.

One partner from pit to port

Industrial Security

DCS, PLCs, furnaces, kilns, mills

Remote Operations Protection

Remote-ops centres, fleets, site links

ERP & Dispatch Security

ERP, weighbridges, e-permits, portals

Supply Chain Assessment

MDOs, contractors, transporters, ports

24/7 IT/OT SOC

Plant, mine and site monitoring

Ransomware Resilience

Backups, safe-stop playbooks, exercises

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

Single plants, foundries and mid-sized mines

- IT and plant assessment (B1)
- Backup and dispatch recovery review (B3)
- Vendor remote access review (B3, B9)
- Policy and lender evidence pack (B5)

Assurance

Multi-site producers and mining groups

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

Continuous Resilience

Integrated groups, exporters and PSUs

- OT testing and red teaming (B1, B10)
- Contractor and logistics risk programme (B9)
- SOC with threat hunting (B7)
- Board, SEBI and NCIIPC 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	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

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Kiln That Kept Turning While Nothing Left the Gate**	Ransomware stops a cement group's dispatch; segmentation and tested backups keep trucks moving	**B3 · B7 · B8**
2	**The Remote Operations Centre With One Password**	A contractor's shared account reaches a mine's fleet system; brokered access and monitoring stop it	**B9 · B3 · B1**
3	**The Furnace Vendor's Laptop**	An OEM laptop infects furnace HMIs; device checks and OT segmentation prevent it	**B9 · B1 · B7**
4	**The Weighbridge That Rounded Up**	An insider edits dispatch weights to divert ore; integrity controls and analytics catch it	**B2 · B7 · B8**
5	**The Smelter's Captive Power Plant**	A phished engineer account reaches the power plant HMI; segmentation and exercises prevent it	**B3 · B1 · B10**

Example: breaking an ERP-to-dispatch shutdown chain

Case 1: The Kiln That Kept Turning While Nothing Left the Gate

ILLUSTRATIVE ATTACK PATH

Step 1	Step 2	Step 3	Step 4	Step 5
Phishing gives attackers a foothold in a cement group's corporate network	Ransomware encrypts ERP, the dispatch system and the weighbridge servers	Kilns keep running but no invoice, permit or gate pass can be issued	Trucks queue for days and silos fill; plants cut clinker output	Recovery costs, lost sales and a quarterly disclosure to the exchanges

WHERE CONTROLS BREAK THE CHAIN

IT/OT segmentation so plants and dispatch survive an IT outage	Immutable, tested backups of ERP, dispatch and weighbridge systems	EDR and 24x7 SOC to catch the intrusion before encryption	Manual dispatch playbooks rehearsed with plant and sales teams

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

Codec Networks

What we test: which plant, dispatch and permit processes depend on ERP and weighbridge systems, IT/OT segmentation, the ability to run kilns and dispatch without IT, immutable backups and restore times, EDR and SOC detection, and crisis decision-making in a tabletop exercise with plant and sales leadership.

Why producers 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 IEC 62443, ISO/IEC 27001, CERT-In and NCIIPC expectations and your lenders' and buyers' 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 MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Plants, mines, DCS and PLCs, remote operations, ERP and dispatch, OEMs and contractors, and your audit, lender and disclosure 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.