Codec Networks
Coding Threats. Decoding Solutions.



INDUSTRY BROCHURE · DEFENCE & STRATEGIC INDUSTRIES

Protect the Design. Protect the Mission.

Supply chain assurance, secure development, restricted environment assessments, managed SOC and forensics for defence PSUs, private defence manufacturers and MSME suppliers, defence R&D organisations, defence start-ups and space and strategic electronics suppliers.

- Supply Chain Assurance
- Secure Development
- Restricted Environments
- SMLDI & Audits
- 24/7 Managed SOC
- Forensics & IR

THE CHALLENGE

In defence, a cyber incident is a national security event.

Defence production reached a record ₹1.78 lakh crore in FY 2025-26 and exports ₹38,424 crore. As MSMEs, start-ups and private firms join DPSUs in the supply chain, espionage groups target designs and suppliers, and SMLDI 2025 makes cyber security a condition of licensed manufacture.



What keeps leadership teams awake

- Espionage against designs and drawings
- Suppliers leaking controlled data
- Ransomware stopping production lines
- Tampered firmware and counterfeit parts
- Insider leaks and removable media
- SMLDI, CERT-In and partner obligations

₹38,424 cr
Record defence exports in FY 2025-26

80+
Countries buying Indian defence exports (FY26)

24%
Private share of defence production (FY26)

6 hours
To report cyber incidents to CERT-In

The rulebook has changed

Instrument	What it means for you
Security Manual for Licensed Defence Industries (2025)	CISO and vetted security officers; official work on air-gapped networks; SIEM and PAM; logs to the MoD CSOC
CERT-In Directions and audit guidelines (2022, 2025)	6-hour incident reporting, 180-day logs in India; risk-based independent audits incl. OT/ICS
IT Act s.70 and 70A; Official Secrets Act	Protected systems in strategic and public enterprises; protection of classified information
US CMMC for suppliers to US primes (2025)	NIST SP 800-171 controls; Phase 1 self-assessments; Phase 2 certification suspended for review

OUR SERVICE OFFERINGS

One partner from design to delivery

Built around our primary proposition for the sector: **supply chain assurance, secure development, restricted environment assessments and forensics.**

Supply Chain Assurance

- Tiered supplier security assessments
- Secure drawing and data exchange
- Counterfeit and tamper risk reviews
- Supplier clauses and remediation

Secure Development

- Secure SDLC for software and firmware
- Code review and build pipeline security
- Code signing and SBOM practices
- Embedded and mobile app testing

Restricted Environments

- Air-gap and cross-domain reviews
- Removable media and transfer controls
- Assessments under clearance procedures
- Segmentation and privileged access

SMLDI & Audits

- SMLDI 2025 cyber gap assessments
- CERT-In risk-based audits incl. OT
- NIST SP 800-171 readiness for US work
- ISO/IEC 27001 and data classification

24/7 Managed SOC

- IT, plant and partner access monitoring
- Threat hunting for espionage activity
- Log readiness for MoD CSOC integration
- 6-hour CERT-In reporting support

Forensics & IR

- Espionage and leak investigations
- Ransomware response and recovery
- Insider and removable-media forensics
- Root cause and evidence handling

Who we serve: defence PSUs · private defence manufacturers and MSME suppliers · DRDO-linked research and strategic organisations · defence start-ups · space and strategic electronics suppliers.

BUNDLED SERVICE MODELS

Packaged for how defence industry buys

Eleven Codec Networks bundles apply directly to defence PSUs, private defence manufacturers, suppliers and strategic organisations:

- **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

MSME suppliers and start-ups

- SMLDI and supplier security gap review
- Infrastructure and cloud VAPT
- Secure development quick check
- Awareness for engineers and staff

Assurance

Private primes, mid-size manufacturers and labs

- SMLDI and CERT-In audit programme
- IT–OT segmentation and plant review
- Supplier assurance programme
- 24x7 managed SOC

Continuous Resilience

Defence PSUs and strategic organisations

- Restricted environment assessments
- Threat hunting and compromise checks
- Firmware and supply chain assurance
- Crisis exercises and IR retainer

Mapped to your obligations

Requirement	How we help	Bundle
Incidents to CERT-In in six hours; 180-day logs (CERT-In Directions)	SOC, IR retainer, reporting support	B7, B8
CISO, vetted officers and cyber controls (SMLDI 2025)	SMLDI gap review, policies, PAM	B4, B5
Air-gapped official work; logs to the MoD CSOC (SMLDI 2025)	Air-gap review, log readiness	B3, B7
Risk-based independent audits incl. OT (CERT-In guidelines, 2025)	Comprehensive and OT audits	B4, B1
Controls for notified protected systems (IT Act s.70, NCIIPC)	Control reviews, segmentation, SOC	B4, B3
NIST SP 800-171 controls for US defence work (DFARS, CMMC)	Readiness and gap assessment	B4, B9
Safeguards for staff and partner personal data (DPDP Act, Rules)	DPDPA programme	B6

THE CODEC NETWORKS VALUE ADD

Why defence and strategic industries choose Codec Networks

CERT-In empanelled
Information security audits recognised in defence and PSU tenders.

Defence-sector experience
Serving ministry-level defence bodies and defence PSUs.

Clearance-aware delivery
Restricted work under the customer's security procedures.

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

Full stack, one partner
Audit, testing, SOC and forensics connected from finding to closure.

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

How we engage

Discover & scope
Design and PLM systems, source code and build pipelines, plant and test-bench networks, isolated and restricted networks, suppliers and partner portals, remote access, and the SMLDI, CERT-In and partner obligations that apply to you.

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 programme, supplier onboarding and audit a non-event.

Tell us your sites, programmes, suppliers and obligations. We will propose a practical assurance, monitoring and readiness plan, delivered under your security procedures.

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: PIB releases of 2 April and 17 June 2026 (Ministry of Defence), CERT-In Directions (2022). Confirm obligations against the official instruments.