Codec Networks
Coding Threats. Decoding Solutions.



DEFENCE & STRATEGIC INDUSTRIES CYBERSECURITY

Keep designs secret.

Supply chain assurance, secure development, restricted environment assessments, managed SOC and forensics for defence PSUs, manufacturers, suppliers and strategic organisations.

Three questions every defence industry leader should be able to answer

Which suppliers hold our drawings today, and how do they protect them?
Tiered supplier assessments and secure exchange decide whether a tier-3 breach becomes your programme's leak.

Could anyone carry data across our air gap?
Controlled transfer, registered media and monitoring decide whether an isolated network stays isolated.

Would we report an incident to CERT-In within six hours?
24x7 monitoring, a named CISO and tested playbooks decide whether the clock is met or missed.

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

80+
Countries buying Indian defence exports

24%
Private share of defence production

6 hours
Incident reporting to CERT-In

Built for every tier of the defence supply chain

Defence PSUs · private defence manufacturers · MSME suppliers · DRDO-linked research and strategic organisations · defence start-ups · space and strategic electronics suppliers.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
SMLDI 2025 · CERT-In Directions · audit policy (2022–2025)	CISO; air-gapped official work; 6-hour reporting; audits
IT Act s.70 · NCIIPC · Official Secrets Act	Protected systems; protection of classified information
US CMMC · NIST SP 800-171 (2025)	Controls for suppliers handling US defence information

WHAT WE DO

Supply chain, development, restricted sites, SOC and forensics

Supply Chain Assurance
Tiered supplier assessments, secure exchange, tamper and counterfeit risk.

Secure Development
Secure SDLC, firmware and code review, build pipelines, code signing.

Restricted Environments
Air-gap, cross-domain and media controls, assessed under clearance.

SMLDI & Audits
SMLDI 2025 gap reviews, CERT-In audits, NIST 800-171 and ISO 27001.

24/7 Managed SOC
IT, plant and partner monitoring, threat hunting, 6-hour reporting.

Forensics & IR
Espionage, leak, insider and ransomware investigations and recovery.

Choose your starting point

Foundation
SMLDI and supplier security gap review, infrastructure and cloud VAPT, secure development quick check, awareness. For MSME suppliers and defence start-ups.

Assurance
SMLDI and CERT-In audit programme, IT–OT segmentation review, supplier assurance programme, managed SOC. For private primes, mid-size manufacturers and labs.

Continuous Resilience
Restricted environment assessments, threat hunting, firmware and supply chain assurance, crisis exercises and IR retainer. For defence PSUs and strategic organisations.

Why Codec Networks

CERT-In empanelled
for information security auditing services, and empanelled with NICSI for application audit services.

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

Regulation-mapped
Every finding mapped to SMLDI 2025, CERT-In Directions and audit guidelines, NCIIPC controls, NIST SP 800-171, ISO/IEC 27001 and your contract and programme obligations.

One connected partner
Testing, audits, SOC, forensics and privacy linked from finding to closure.

Book a scoping session

Share 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 – 110001
Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018
Call: 011 430 496 96 · +91 99716 76124 · +91 88007 88220
Email: 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. 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.