

Codec Networks

Coding Threats. Decoding Solutions.

DEFENCE & STRATEGIC INDUSTRIES

Protect the Design. Protect the Mission.

Supply chain assurance, secure development, restricted environment assessments, managed SOC and forensics for defence and strategic industries

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

SMLDI 2025, CERT-In, NCIIPC, Official Secrets Act and US CMMC



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



Defence industry is growing fast, and so is its attack surface

Official figures show the scale of what must be protected

₹1.78 lakh cr

Record defence production in FY
2025-26

₹38,424 cr

Record defence exports in FY
2025-26

24%

Private share of defence
production (FY26)

6 hours

To report cyber incidents to
CERT-In

What this means: defence PSUs, private manufacturers, suppliers and strategic organisations must protect designs, drawings and source code from espionage, hold every tier of the supply chain to account, keep isolated networks isolated, assure the integrity of firmware and components, meet SMLDI 2025 and partner obligations, and report incidents within six hours.

Sources: PIB releases of 2 April and 17 June 2026 (Ministry of Defence), CERT-In Directions (2022).

Who we serve across defence and strategic industries



Defence PSUs

Aircraft, ships, electronics, munitions



Ordnance companies

Ammunition, vehicles, weapons, optics



Private defence primes

Platforms, systems, integration



MSME suppliers

Machining, castings, cables, sub-assemblies



Defence R&D organisations

Laboratories, test ranges, design centres



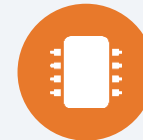
Defence start-ups

Drones, AI, sensors, iDEX innovators



Space and satellite firms

Satellites, ground segment, launch



Strategic electronics

Radar, communications, EW, semiconductors

The threats that cost defence industry the most

Six priorities from our 18-threat defence and strategic industry assessment



State-linked espionage

Spear-phishing of engineers and officers



Supplier compromise

Tier-2 and tier-3 firms holding drawings



Ransomware on production

IT-to-shop-floor spread, stalled lines



Firmware and part tampering

Altered builds, counterfeit components



Insider and media leaks

Removable media, air-gap crossings



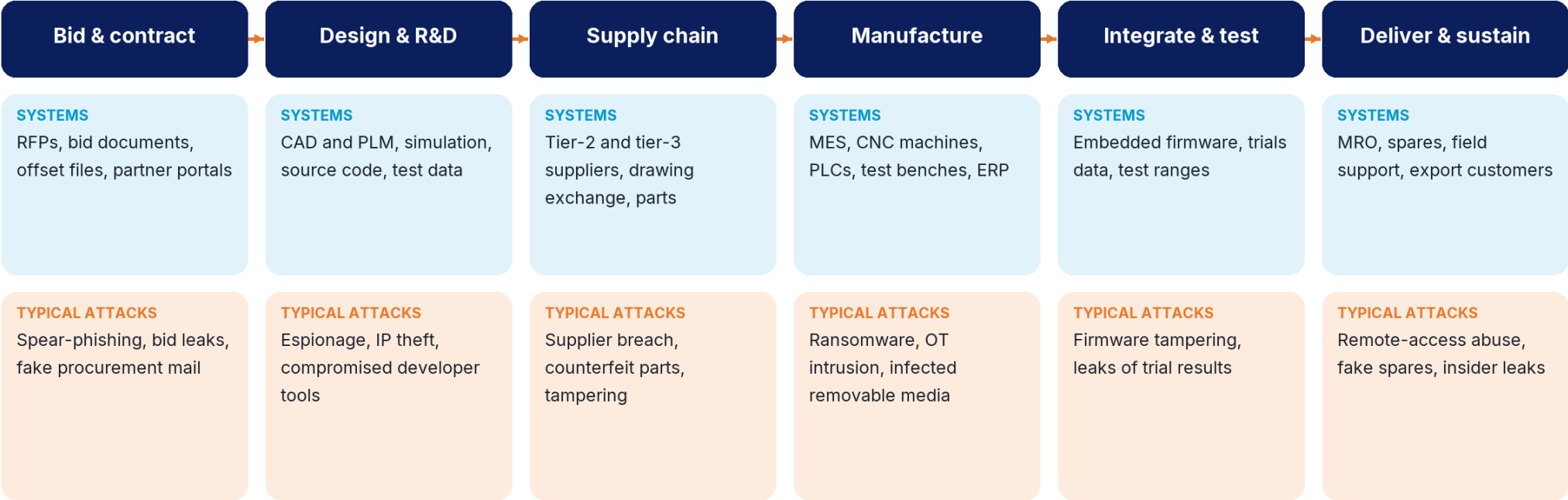
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from bid to sustainment

Where Cyber Risk Sits Across the Defence Programme Lifecycle

Every stage from bid to sustainment carries its own attack surface



In defence, confidentiality and integrity are the product: a leaked drawing, a tampered component or an altered firmware image can surface years later, in the field.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

SMLDI 2025, CERT-In, NCIIPC, Official Secrets Act and US CMMC

The rules shaping defence industry 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
CISO and security officers	Dedicated CISO above ₹250 crore turnover	SMLDI 2025
Official work	On air-gapped networks	SMLDI 2025
Log integration	With the MoD CSOC, where applicable	SMLDI 2025
Independent cyber audits	Risk-based, incl. OT/ICS	CERT-In audit guidelines, 2025
Protected systems	NCIIPC controls for notified CII	IT Act, Sections 70 and 70A
Classified information	Protection and need-to-know	Official Secrets Act, 1923
US defence information	NIST SP 800-171 controls	DFARS 252.204-7012; CMMC

Key dates on the regulatory timeline

Policy and Regulatory Timeline Shaping Defence Industry Cybersecurity

Security, acquisition, licensing and cyber instruments that reach defence PSUs, private manufacturers and their suppliers

● In force ● Upcoming (from Oct 2026)

1923	● Official Secrets Act, 1923 protects classified official information
2000	● IT Act, 2000; Sections 70A (NCIIPC) and 70B (CERT-In) added in 2008
Apr 2018	● IDEX launched to fund defence innovation by start-ups, MSMEs and innovators
Oct 2019	● NPCIL confirms malware on an administrative network at Kudankulam after a CERT-In alert
Sep 2020	● FDI in defence raised to 74% through the automatic route (Press Note 4, 2020)
Oct 2020	● Defence Acquisition Procedure 2020 takes effect, with priority for Buy (Indian-IDDM)
Oct 2021	● Ordnance Factory Board dissolved; its factories pass to seven new defence PSUs
Apr 2022	● CERT-In Directions: 6-hour incident reporting and 180-day ICT logs in India
Jul 2025	● SMLDI 2025 issued: CISO, air-gapped official work, logs integrated with MoD CSOC
Jul 2025	● CERT-In Comprehensive Cyber Security Audit Policy Guidelines, incl. OT/ICS
Nov 2025	● US CMMC clauses enter DoD contracts (Phase 1); DPDP Rules notified in India
Feb 2026	● Draft Defence Acquisition Procedure 2026 released for stakeholder comment
Jun 2026	● Defence production reaches a record ₹1.78 lakh crore for FY 2025-26
May 2027	● Most DPDP Rules obligations, incl. security safeguards and breach intimation, apply

Sources: MoD, DDP, DPIIT, CERT-In, PIB, US DoD, Gazette of India. Confirm against the official instruments.

Codec Networks

How Codec Networks helps

Supply chain · Secure development · Restricted environments · SMLDI & audits · Managed SOC · Forensics

One partner from design to delivery



Supply Chain Assurance

Tiered supplier reviews



Secure Development

Software and firmware



Restricted Environments

Air gaps and transfers



SMLDI & Audits

SMLDI, CERT-In, NIST



24/7 Managed SOC

Detection and hunting



Forensics & IR

Leaks, espionage, ransomware

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



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

MSME suppliers and defence start-ups

- SMLDI and supplier gap review (B4, B9)
- Infrastructure and cloud VAPT (B1, B3)
- Secure development quick check (B2)
- Awareness for engineers (B10)

Assurance

Private primes, mid-size manufacturers and labs

- SMLDI and CERT-In audits (B4, B1)
- IT–OT segmentation review (B3)
- Supplier assurance programme (B9)
- 24x7 managed SOC (B7)

Continuous Resilience

Defence PSUs and strategic organisations

- Restricted environment reviews (B1, B3)
- Threat hunting and compromise checks (B7)
- Firmware and supply chain assurance (B2, B9)
- Crisis exercises and IR retainer (B10, B8)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1

The Drawing That Left Through a Supplier

A machining MSME without MFA leaks defence drawings for months; supplier controls stop it

B9 · B7 · B8

2

The Directive That Was Not From Headquarters

A spoofed directive plants an implant at a defence PSU; email controls and hunting catch it

B7 · B10 · B8

3

The Night the Shop Floor Stopped

Ransomware crosses from IT into MES and CNC cells; segmentation and SOC contain it

B3 · B7 · B8

4

The Firmware Update Nobody Signed

An exposed build token lets firmware be altered; signing and secure pipelines prevent it

B2 · B9 · B11

5

The Stick That Crossed the Air Gap

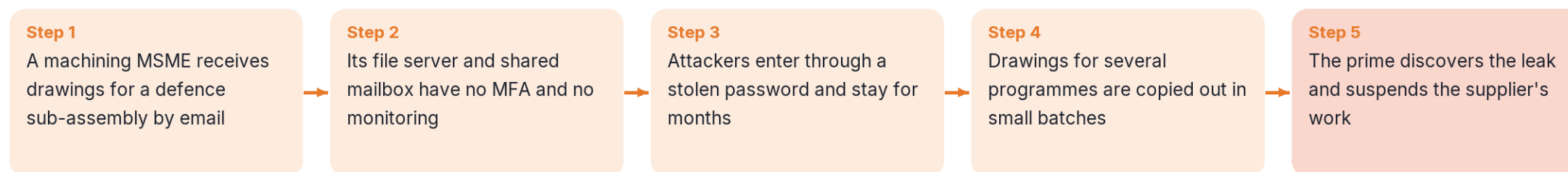
A personal USB drive carries malware into an isolated design network; transfer controls stop it

B3 · B1 · B8

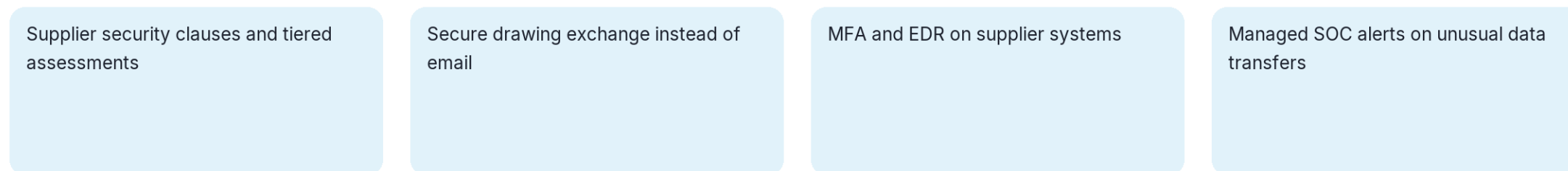
Example: breaking a supplier leak chain

Case 1: The Drawing That Left Through a Supplier

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: which suppliers hold controlled drawings and how they receive them, whether supplier mail, file servers and remote access use MFA and EDR, whether contracts set security, audit and reporting duties, whether unusual data transfers raise alerts, and how the prime and supplier handle containment, CERT-In reporting and programme notifications in a joint tabletop exercise.

Why defence and strategic industries 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 SMLDI 2025, CERT-In Directions and audit guidelines, NCIIPC, NIST SP 800-171 and ISO/IEC 27001



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 MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Design and PLM systems, source code and build pipelines, plant and test-bench networks, isolated networks, suppliers and partner portals, remote access, and SMLDI, CERT-In and partner obligations

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.