



Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · IT SERVICES & SYSTEMS INTEGRATION

Secure What You Build. Protect Who You Serve.

Secure code review, DevSecOps, infrastructure testing, ISO readiness, SOC and supply chain security for software developers, IT consultancies, system integrators and managed service providers.

Secure Code Review

DevSecOps

Infrastructure Testing

ISO Readiness

24/7 SOC

Supply Chain Security

Coding Threats. Decoding Solutions.

www.codecnetworks.com

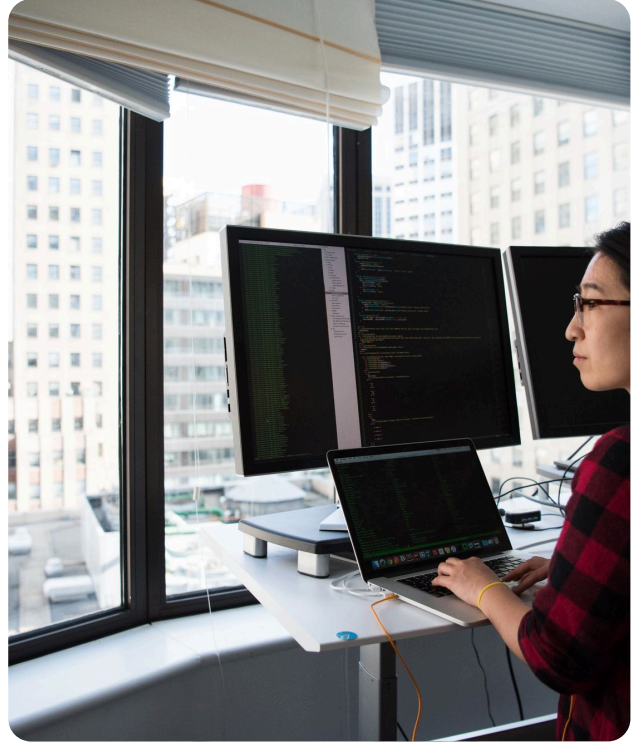
THE CHALLENGE

Your access reaches every client. So does your risk.

IT service providers hold code, credentials and privileged access to many client environments. Regulated and global clients now pass their regulators' third-party requirements down to their providers.

What keeps leadership teams awake

- A compromised build reaching every client
- Remote-management tools used to deploy ransomware
- Source code, keys and client data leaking from repositories
- Subcontractor and former-staff access that is never removed
- Client due-diligence questionnaires and audits
- CERT-In, DPDP and international obligations



6 hours

To report cyber incidents to CERT-In

Annual

Third-party cyber audits under CERT-In's 2025 audit guidelines

Sep 2026

EU Cyber Resilience Act reporting obligations apply

May 2027

Most DPDP obligations take effect

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 third-party cyber audits at least annually
Client regulator flow-down	RBI IT outsourcing Directions, SEBI CSCRF, IRDAI vendor controls: audit rights, security and incident clauses
DPDP Act & Rules	Processing under contract with reasonable security safeguards; breach intimation from May 2027
International obligations	GDPR, NIS2, DORA and the EU CRA for clients and products in Europe; ISO/IEC 27001 and SOC 2 expectations

One partner from code to operations

Built around our primary proposition for the sector: **secure code review, DevSecOps, infrastructure testing, ISO readiness, SOC and supply chain security.**

Secure Code Review

- Manual and tool-assisted code review
- SAST, DAST and SCA
- Secrets and credential scanning
- Remediation guidance for developers

DevSecOps

- CI/CD pipeline security review
- Build integrity and signing
- SBOM generation and governance
- Security gates and developer training

Infrastructure Testing

- Internal and external VAPT
- Jump host and RMM tool testing
- Active Directory and cloud reviews
- Red teaming

ISO Readiness

- ISO/IEC 27001:2022 gap and implementation
- SOC 2 readiness
- Client due-diligence evidence packs
- Policies and risk registers

24/7 SOC

- Managed SOC with SIEM and EDR/XDR
- Privileged and RMM activity monitoring
- Threat hunting
- 6-hour CERT-In reporting support

Supply Chain Security

- Subcontractor and vendor assessments
- Open-source dependency risk
- Joiner-mover-leaver reviews
- Client-impact incident playbooks

Who we serve: software developers and product engineering firms · IT consultancies · system integrators · managed service providers · staffing and subcontracting partners.

Packaged for how IT service firms buy

Eleven Codec Networks bundles apply directly to IT service providers and system integrators:

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

Smaller developers and consultancies

- Secure code review and SCA
- External VAPT
- ISO 27001 gap assessment
- Policy pack and awareness

Assurance

Mid-sized SIs and MSPs

- DevSecOps and pipeline review
- Infrastructure and RMM testing
- ISO 27001 or SOC 2 readiness
- 24x7 managed SOC

Continuous Resilience

Large SIs, MSPs and product firms

- Continuous testing and red teaming
- Subcontractor and supply-chain assurance
- SOC with privileged-access signals
- Client and Board reporting

Mapped to your obligations

Requirement	How we help	Bundle
Cyber incidents to CERT-In within six hours; 180-day logs (CERT-In Directions)	SOC monitoring, IR retainer and reporting support	B7, B8
Risk-based third-party cyber audits (CERT-In audit guidelines, 2025)	Independent audit and VAPT	B1, B4
Client regulator flow-down: RBI, SEBI, IRDAI vendor controls	Audit evidence and control assessments	B4, B5
Secure development and software integrity	Secure code review and DevSecOps	B2
Processing client personal data with safeguards (DPDP)	DPDPA processor programme	B6
Subcontractor and supplier controls	Third-party risk programme	B9
ISO/IEC 27001:2022 and SOC 2 expectations	Readiness and implementation	B5

Why IT service firms choose Codec Networks

CERT-In empanelled

Independent audits and penetration testing that clients and regulators recognise.

Certified and accountable

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

Developer-friendly depth

Code, pipeline and build integrity reviews with practical fixes.

Client-ready evidence

Reports and closure evidence that answer client questionnaires.

Full stack, one partner

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

Certified experts

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

How we engage

Discover & scope

Delivery model, client sectors, tools with privileged access, pipelines and your audit 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 client audit, release and incident a non-event.

Tell us your delivery model, clients and certifications. We will propose a practical 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: CERT-In, MeitY, European Union. Confirm obligations against the official instruments.