

Codec Networks

Coding Threats. Decoding Solutions.

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 IT service firms

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

CERT-In, DPDP, client regulator flow-down and EU rules



How Codec Networks helps

Services, bundles and packages built for the sector



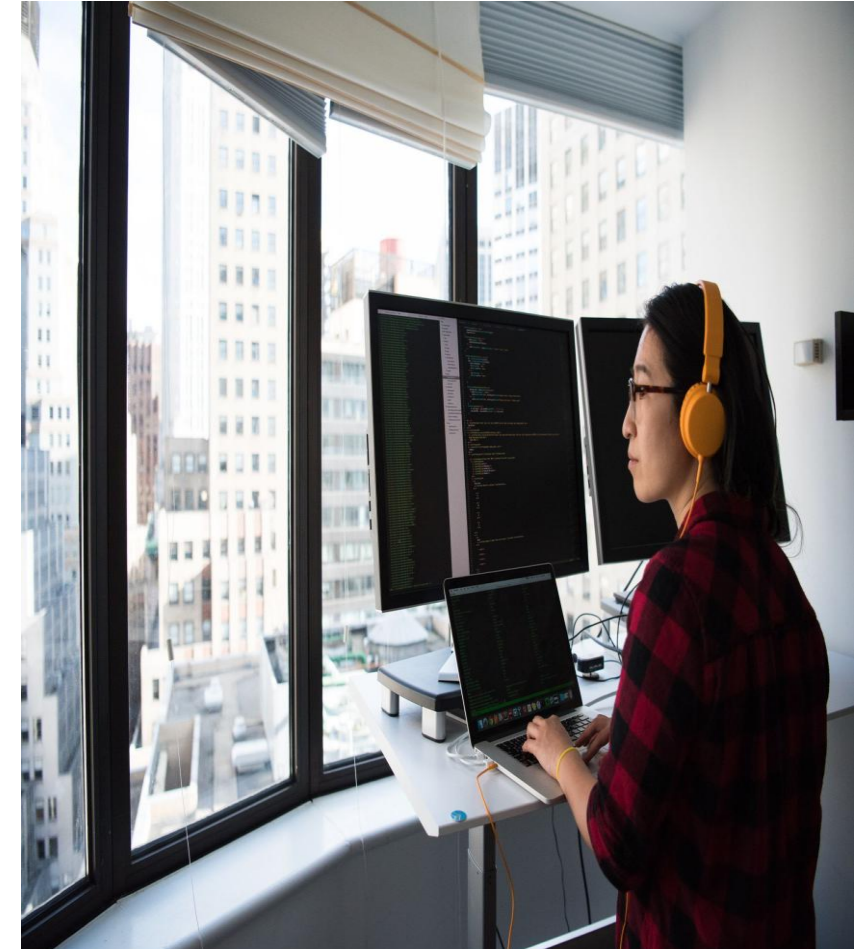
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Clients now pass their regulators' rules to you

CERT-In, DPDP and client regulators shape what providers must prove

6 hours

To report cyber incidents to
CERT-In

Annual

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

Sep 2026

EU Cyber Resilience Act
reporting obligations apply

May 2027

Most DPDP obligations take
effect

What this means: IT service firms must secure their pipelines and privileged tools, prove controls to regulated and global clients, manage subcontractors and report incidents within six hours.

Sources: CERT-In, MeitY, RBI, SEBI, European Union.

Who we serve across IT services



Software developers

Custom and product engineering



IT consultancies

Advisory and transformation



System integrators

Multi-vendor implementation



Managed service providers

Infrastructure and cloud operations



Product engineering firms

Software built for clients



Cloud partners

Migration and managed cloud



Security service providers

Managed security and SOC



Staffing and subcontractors

Engineers on client projects

The threats that cost IT service firms the most

Six priorities from our 18-threat IT services assessment



Supply-chain compromise

One build, many victims



RMM tool abuse

Ransomware at every client



Code and secret leakage

Keys in public repos



Privileged access misuse

Insiders and contractors



Ransomware

Own and client estates



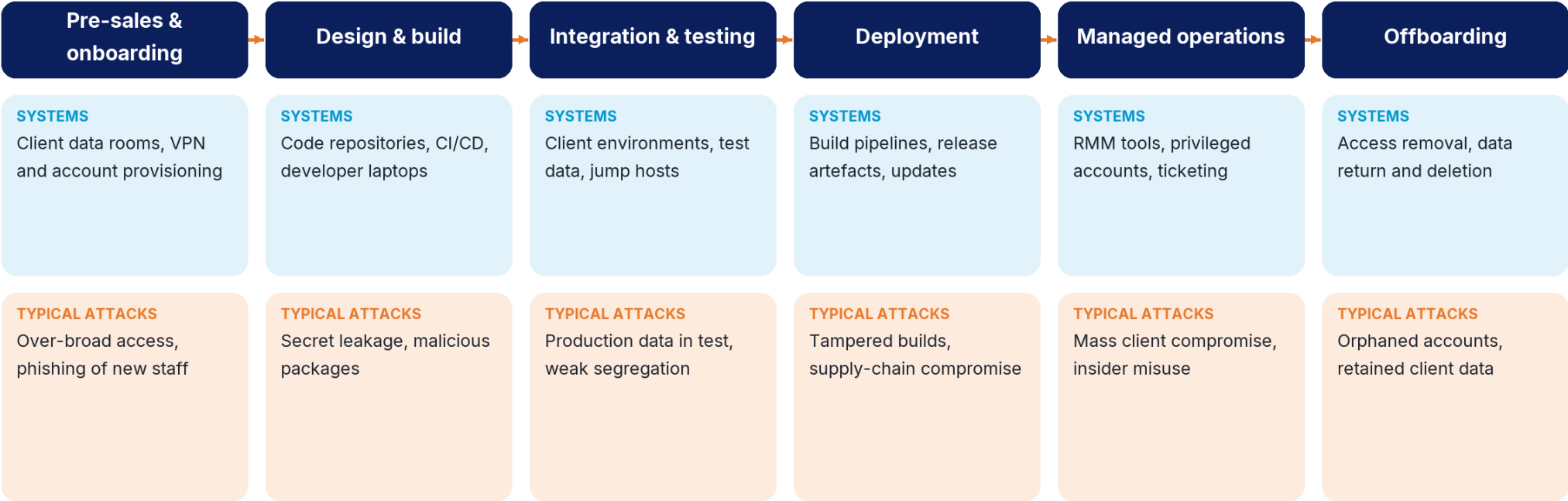
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage of delivery

Where Cyber Risk Sits in the IT Services Delivery Lifecycle

Every stage of delivery carries its own attack surface



Clients inherit the security of every developer laptop, pipeline and remote-management tool their provider uses.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, DPDP, client regulator flow-down and EU rules

The rules that reach IT service providers

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
Third-party cyber audits	At least annually, risk-based	CERT-In audit guidelines, 2025
Outsourced IT controls for bank clients	Per contract and RBI Directions	RBI IT outsourcing Directions, 2023
Third-party controls for market clients	Per SEBI CSCRF	SEBI CSCRF, 2024
Processing client personal data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Products with digital elements in the EU	Reporting from Sep 2026	EU Cyber Resilience Act
ICT providers to EU financial clients	Contractual requirements	EU DORA

Key dates on the regulatory timeline

Regulatory Timeline Shaping IT Services Security

Indian and international instruments that flow down to IT service providers

● In force ● Upcoming (from Oct 2026)

Apr 2022	● CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Apr 2023	● RBI Master Direction on Outsourcing of IT Services issued
Aug 2023	● Digital Personal Data Protection Act, 2023 enacted
Aug 2024	● SEBI Cybersecurity and Cyber Resilience Framework (CSCRF) issued
Jul 2025	● CERT-In Comprehensive Cyber Security Audit Policy Guidelines
Nov 2025	● DPDP Rules, 2025 notified with phased commencement
Sep 2026	● EU Cyber Resilience Act reporting obligations apply
May 2027	● Most DPDP Rules obligations, incl. breach intimation, take effect

Sources: CERT-In, RBI, SEBI, MeitY, EU. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Secure code · DevSecOps · Infrastructure testing · ISO · SOC · Supply chain

One partner from code to operations



Secure Code Review

Manual review, SAST, DAST, SCA, secrets



DevSecOps

Pipelines, build signing, SBOM



Infrastructure Testing

VAPT, RMM, AD, red teaming



ISO Readiness

ISO 27001:2022, SOC 2, evidence packs



24/7 SOC

Privileged and RMM monitoring



Supply Chain Security

Subcontractors, dependencies, access lifecycle

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

Smaller developers and consultancies

- Secure code review and SCA (B2)
- External VAPT (B1)
- ISO 27001 gap assessment (B5)
- Policy pack and awareness (B5, B10)

Assurance

Mid-sized SIs and MSPs

- DevSecOps review (B2)
- Infrastructure and RMM testing (B1)
- ISO 27001 or SOC 2 readiness (B5)
- 24x7 managed SOC (B7)

Continuous Resilience

Large SIs, MSPs and product firms

- Red teaming and simulations (B1, B10)
- Supply-chain assurance (B9)
- SOC with privileged signals (B7)
- Client and Board reporting (B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

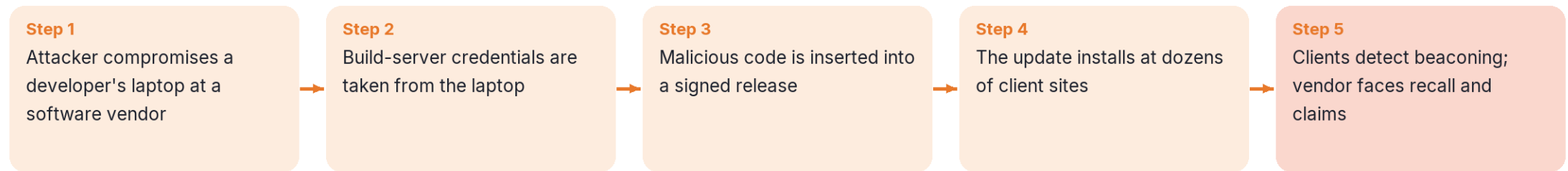
Illustrative composite scenarios written for 2026—not client engagements

1	The Update That Shipped a Backdoor	A compromised build reaches every client; pipeline hardening and SBOMs prevent it	B2 · B7 · B8
2	The RMM Console That Ran Everyone's Ransomware	A phished RMM login encrypts many clients; MFA, PAM and SOC stop it	B3 · B7 · B8
3	The Repository That Held the Client's Keys	Leaked cloud keys expose client data; secret scanning and vaulting prevent it	B2 · B3 · B7
4	The Contractor Who Kept the VPN	Orphaned access is reused months later; access lifecycle controls stop it	B9 · B7 · B5
5	The AI Assistant That Shared Client Code	Client code pasted into public AI; approved tools and DLP prevent it	B11 · B6 · B5

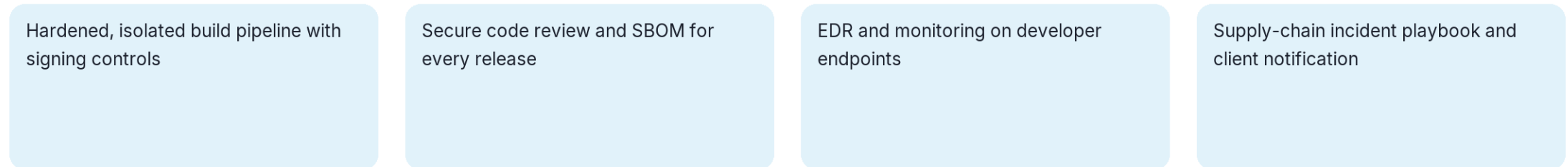
Example: breaking a software supply-chain chain

Case 1: The Update That Shipped a Backdoor

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: developer endpoint security, build-server isolation and credentials, code signing and release approvals, SBOM and dependency checks, and the client notification and CERT-In reporting steps.

Why IT service firms choose Codec Networks



CERT-In empanelled

For information security auditing services; NISCI empanelled for application audits



Certified

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



Regulation-mapped

Mapped to CERT-In, DPDP, client regulator and EU 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 MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Delivery model, clients, privileged tools, pipelines and certifications

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.