

Codec Networks

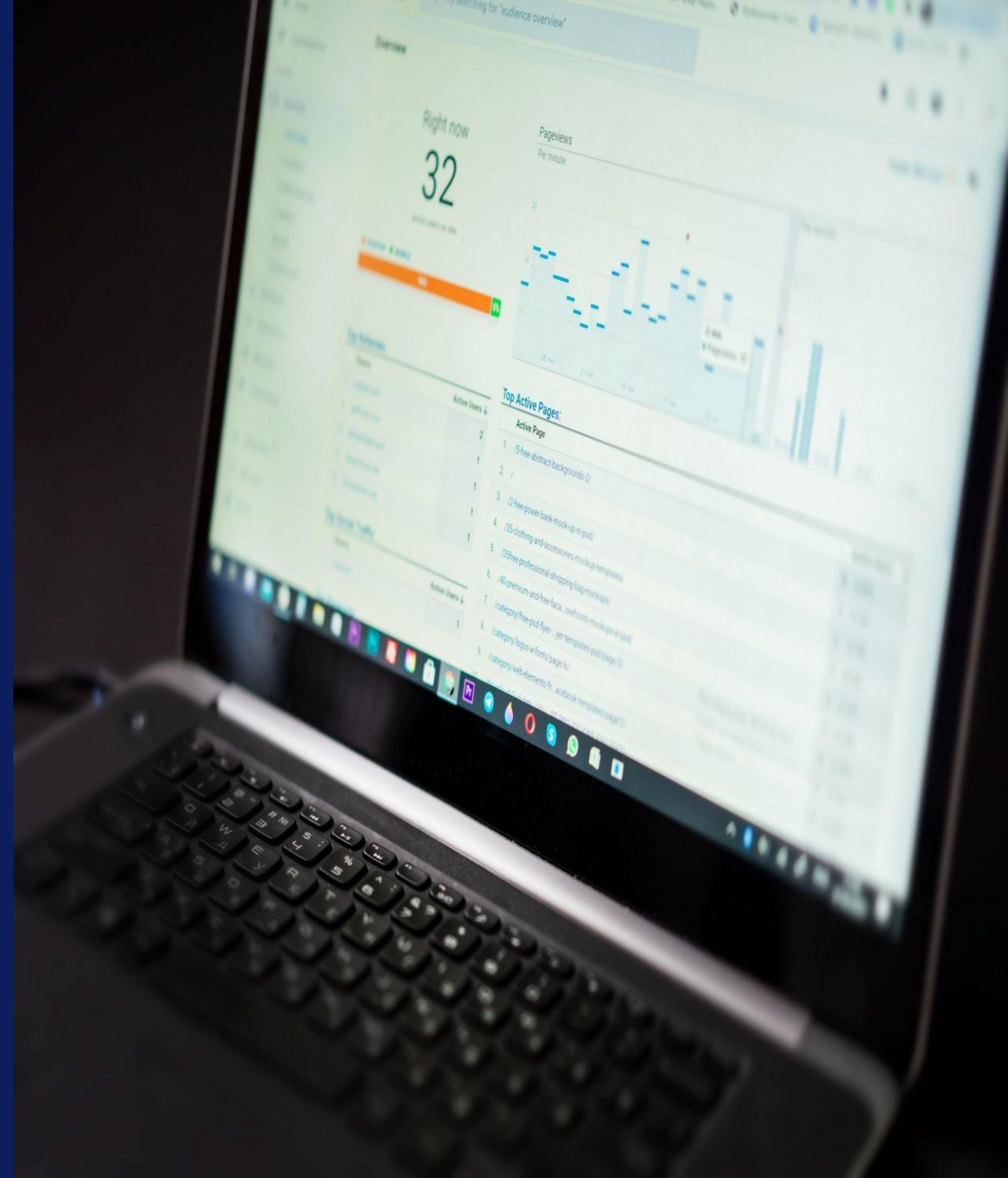
Coding Threats. Decoding Solutions.

SAAS & ENTERPRISE SOFTWARE

Ship Secure Software. Win Every Security Review.

Product VAPT, SAST/DAST/SCA, API testing, tenant isolation, cloud security and SOC 2 readiness for SaaS and enterprise software vendors

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, customer flow-down, SOC 2 and EU rules



How Codec Networks helps

Services, bundles and packages built for the sector



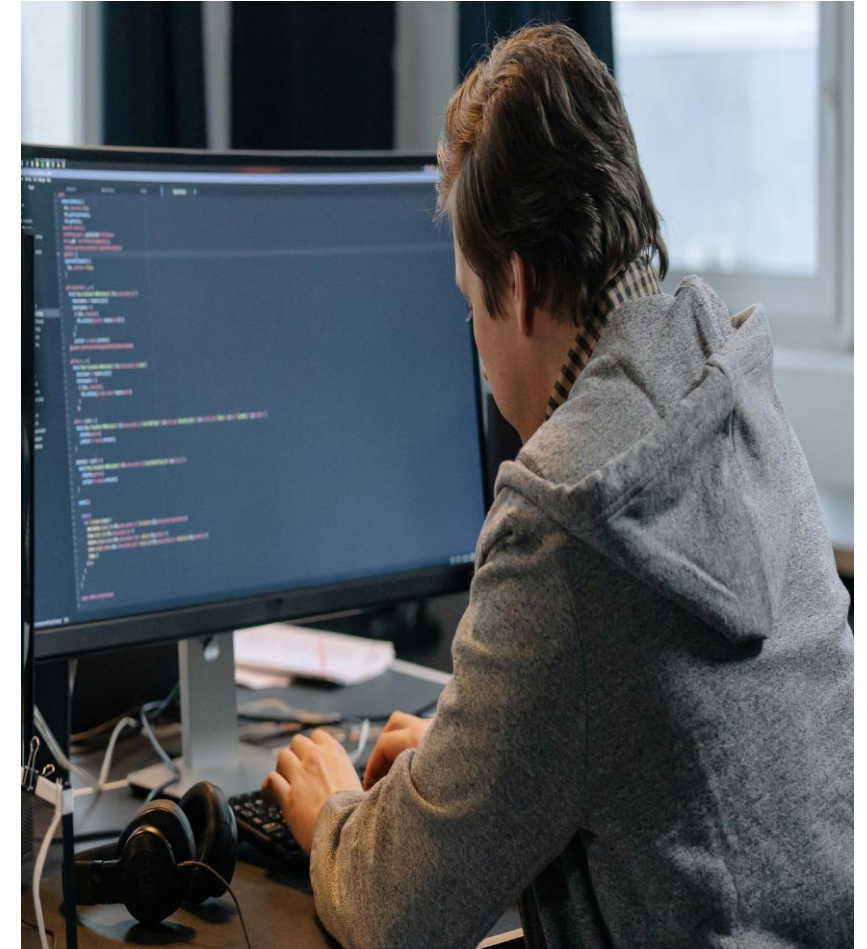
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Enterprise buyers now ask for proof

Security reviews, SBOMs and incident commitments are part of every deal

6 hours

To report cyber incidents to
CERT-In

Oct 2024

CERT-In SBOM technical
guidelines issued

Sep 2026

EU Cyber Resilience Act
reporting obligations apply

May 2027

Most DPDP obligations take
effect

What this means: SaaS vendors must prove tenant isolation, secure APIs and integrations, manage dependencies with SBOMs, protect customer and support access, and report incidents within six hours.

Sources: CERT-In, MeitY, European Union.

Who we serve across SaaS and enterprise software



ERP vendors

Finance and supply chain



CRM vendors

Sales and service



HRMS and payroll

People and payroll data



Collaboration platforms

Messaging and documents



Cybersecurity vendors

Security products



Vertical SaaS

Industry applications



Developer platforms

Tools and APIs



Data and analytics SaaS

Data platforms

The threats that cost SaaS vendors the most

Six priorities from our 18-threat SaaS assessment



Tenant isolation flaws

One customer sees another



Broken API authorisation

Data for anyone who asks



Account takeover

Customers without MFA



Integration token theft

OAuth apps as a back door



Vulnerable dependencies

Libraries nobody tracked



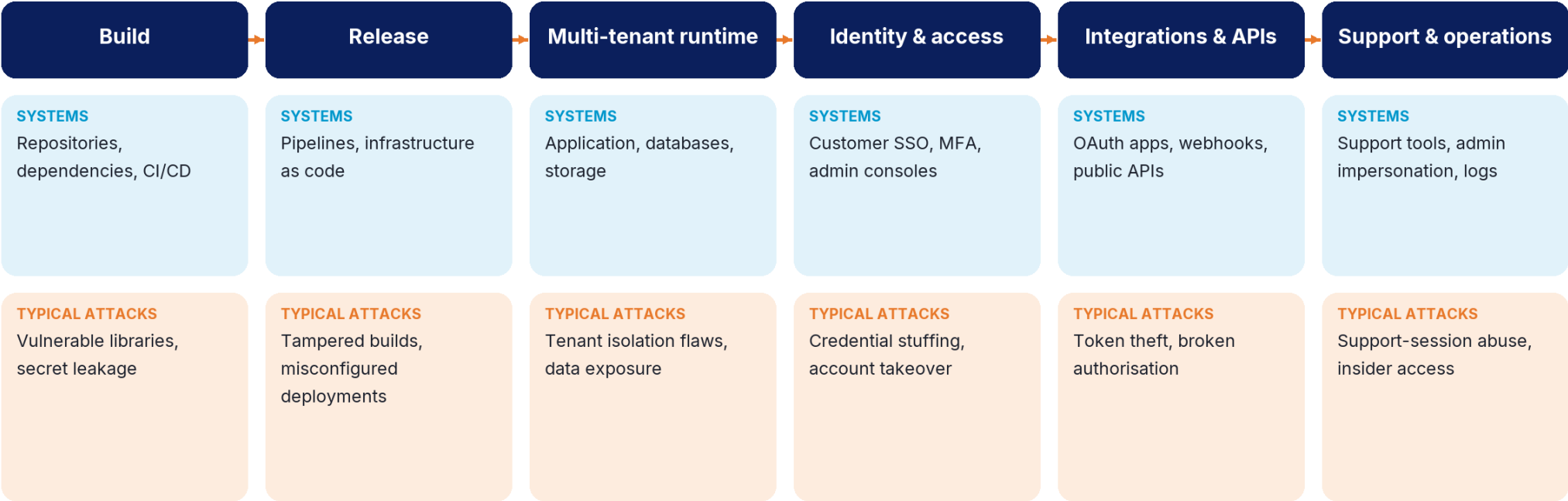
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage of the product lifecycle

Where Cyber Risk Sits in the SaaS Product Lifecycle

Every stage from code to customer support carries its own attack surface



Customers inherit every flaw in the code, the tenant model and the support tools behind the product.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, DPDP, customer flow-down, SOC 2 and EU rules

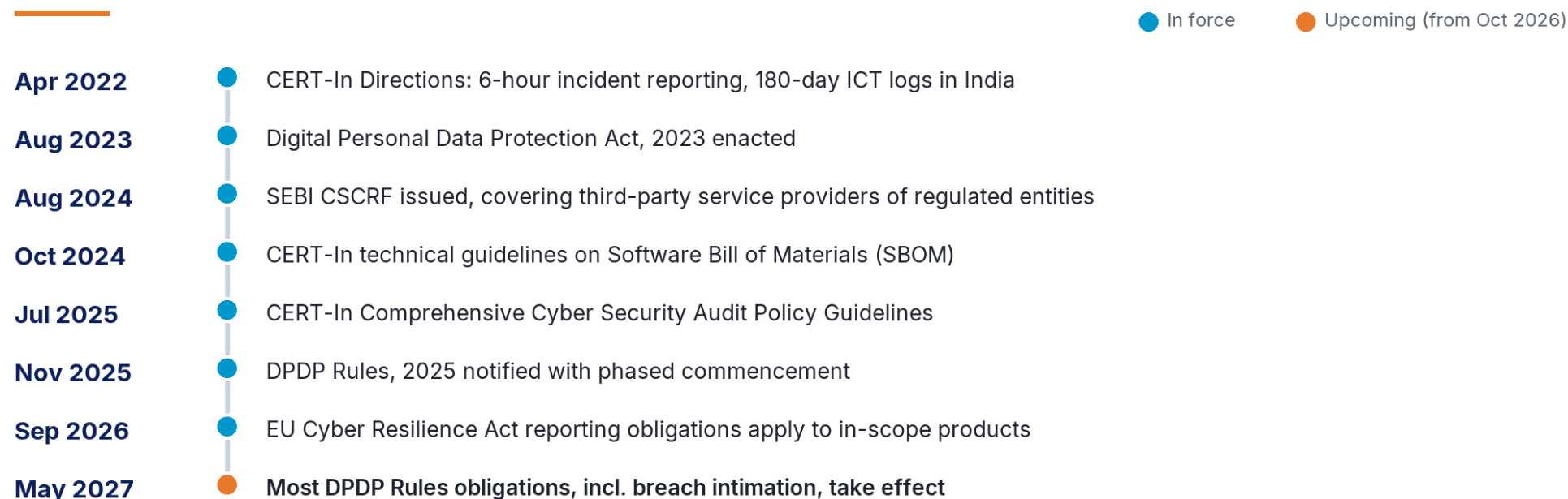
The rules and expectations SaaS vendors face

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
Software bill of materials	Recommended practices	CERT-In SBOM guidelines, 2024
Independent cyber audits	Risk-based	CERT-In audit guidelines, 2025
Processing customer personal data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Vendor controls for BFSI customers	Per contract	RBI, SEBI, IRDAI rules
Enterprise assurance	Annual reports and certificates	SOC 2, ISO/IEC 27001
In-scope products sold in the EU	Reporting from Sep 2026	EU Cyber Resilience Act

Key dates on the regulatory timeline

Regulatory Timeline Shaping SaaS Security

Indian, international and customer-driven instruments



Sources: CERT-In, MeitY, SEBI, European Union. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Product VAPT · SAST/DAST/SCA · API testing · Tenant isolation · Cloud · SOC 2

One partner from code to customer trust



Product VAPT

Web, mobile, admin and support consoles



SAST / DAST / SCA

Code review, dynamic testing, SBOM



API Testing

Public APIs, OAuth, webhooks



Tenant Isolation

Cross-tenant authorisation and partitioning



Cloud Security

Posture, IAM, IaC, Kubernetes



SOC 2 Readiness

SOC 2, ISO 27001, questionnaires

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

Early-stage SaaS

- Product VAPT and API testing (B1, B2)
- SCA and secrets scanning (B2)
- SOC 2 gap assessment (B5)
- Cloud posture review (B3)

Assurance

Growth-stage SaaS

- Tenant isolation testing (B1, B2)
- DevSecOps and SBOM (B2)
- SOC 2 and ISO 27001 (B5)
- 24x7 managed SOC (B7)

Continuous Resilience

Enterprise software vendors

- Red teaming and simulations (B1, B10)
- Integration assurance (B9)
- SOC with tenant signals (B7)
- Customer 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
Software bill of materials practices (CERT-In SBOM guidelines, 2024)	SCA and SBOM programme	B2
Processor safeguards for customer personal data (DPDP)	DPDPA programme and data mapping	B6
Vendor controls for BFSI customers (RBI, SEBI, IRDAI)	Flow-down assessments and evidence	B4
Secure multi-tenant architecture (customer contracts)	Tenant isolation and product VAPT	B1, B2
SOC 2 and ISO/IEC 27001 expectations	Readiness and implementation	B5
Cloud security (MeitY empanelment for government customers)	Cloud and IaC reviews	B3

Five new case studies, five broken chains

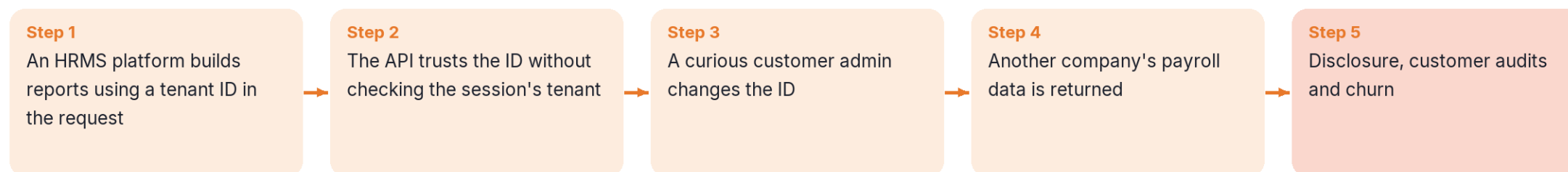
Illustrative composite scenarios written for 2026—not client engagements

1	The Tenant ID in the URL	A trusted tenant ID exposes another company's payroll; isolation tests prevent it	B1 · B2 · B7
2	The Integration Token That Opened Every CRM	A breached integration exports CRM data; scope and token reviews limit it	B9 · B2 · B7
3	The Support Session That Copied Customer Data	Stolen support sessions browse tenants; just-in-time access stops it	B3 · B7 · B8
4	The Customers Who Never Turned On MFA	Credential stuffing hits tenants without MFA; MFA by default stops it	B2 · B7 · B10
5	The Library Nobody Knew Was There	An untracked dependency is exploited; SCA and SBOM prevent it	B2 · B5 · B8

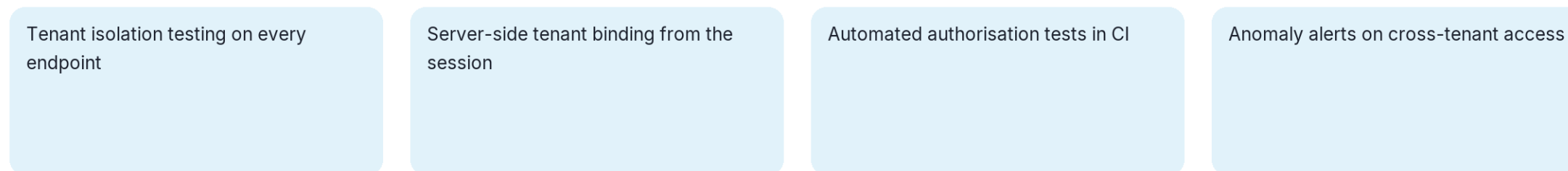
Example: breaking a tenant-isolation chain

Case 1: The Tenant ID in the URL

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: server-side tenant binding on every endpoint, cross-tenant access in APIs, caches, exports and background jobs, automated authorisation tests in CI, and alerting on cross-tenant anomalies.

Why SaaS companies 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 CERT-In, DPDP, customer flow-down, SOC 2 and ISO 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 MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Product architecture, tenant model, integrations and certification calendar

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.