

Codec Networks

Coding Threats. Decoding Solutions.

EDUCATION, EDTECH & RESEARCH

Protect the Student. Protect the Exam. Protect the Research.

Student data privacy, LMS and examination security, research IP protection, managed SOC and awareness for education, edtech and research organisations

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, the Public Examinations Act, UGC, AICTE and SEBI expectations



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



Education is among the most attacked sectors in the world

Global data and Indian incidents show the stakes for students, examinations and research

3rd

Most targeted industry
worldwide in 2024 (Microsoft)

66%

Of higher-education bodies hit
by ransomware (Sophos, 2024)

~22 m

Unacademy accounts offered for
sale after a 2020 breach

6 hours

To report cyber incidents to
CERT-In

What this means: institutions and platforms must protect the data of children and young adults, secure the systems that run examinations, keep research inside the lab, monitor campuses and clouds around the clock, train everyone who holds a login, and report incidents within six hours.

Sources: Microsoft Cyber Signals (2024), Sophos State of Ransomware in Education 2024, public reporting on the Unacademy breach, CERT-In.

Who we serve across education, edtech and research



University groups and deemed universities

Multi-campus, LMS, ERP, research



Engineering, medical and professional colleges

Entrance-driven, labs, hospitals



School chains and boards

K-12 networks, children's data



Coaching and test-prep

Large candidate bases, apps, centres



Online learning and edtech platforms

Apps, SaaS, payments, investors



Examination bodies and testing agencies

Question banks, centres, results



Research organisations and labs

Grants, data sets, HPC, IP



Education technology vendors

LMS, ERP, proctoring, hosting

The threats that cost institutions and platforms the most

Six priorities from our 18-threat education assessment



Student data breaches

Children's and parents' data exposed



Exam and paper compromise

Question banks, centres and results



Ransomware shutdowns

ERP and LMS encrypted in term time



Research IP theft

Espionage against labs and faculty



Account takeover and phishing

Students, parents and staff targeted



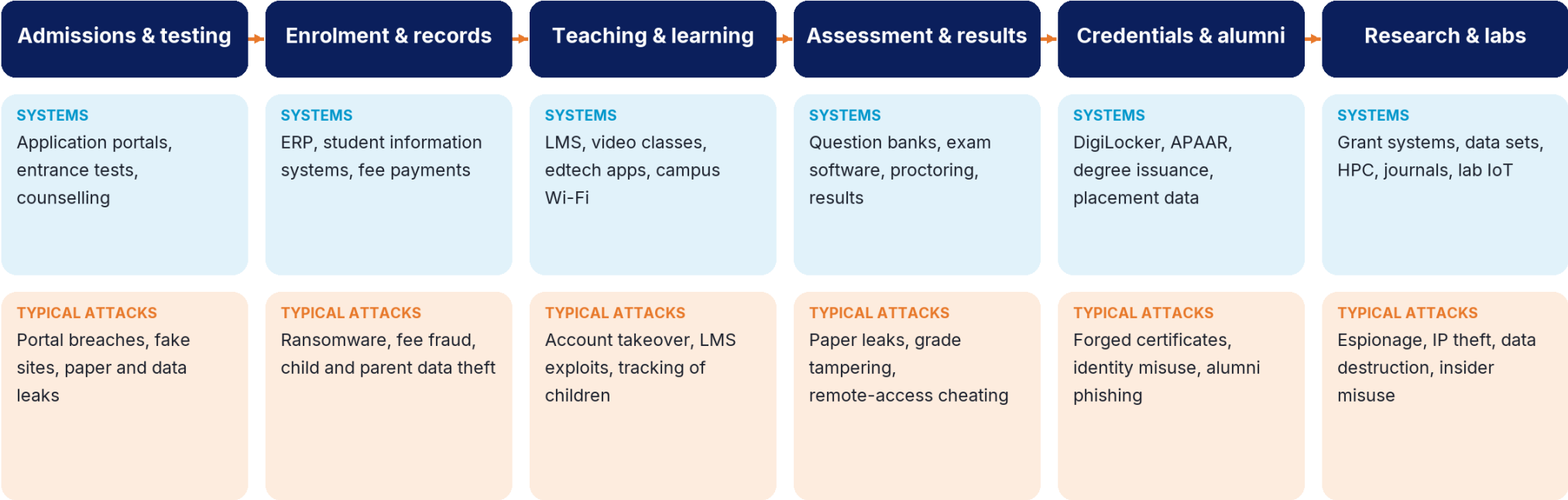
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from admission to research

Where Cyber Risk Sits Across the Education and Research Lifecycle

Every stage from admission to alumni and research carries its own attack surface



In education, a breach exposes children and young adults, a leak invalidates an examination for lakhs of candidates, and stolen research is lost for good.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, DPDP, the Public Examinations Act, UGC, AICTE and SEBI expectations

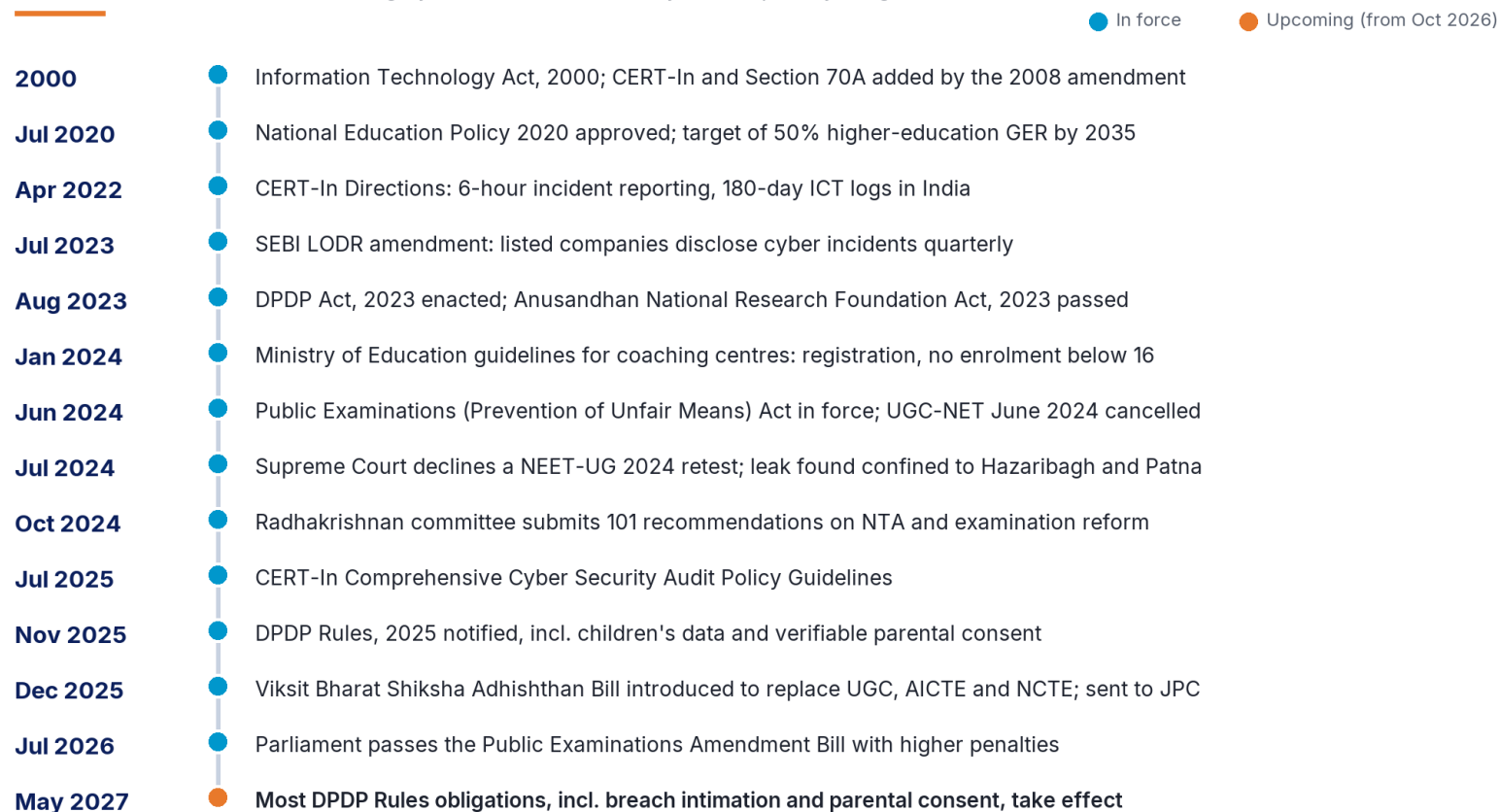
The rules shaping education and research cybersecurity

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
Independent cyber audits	Risk-based, incl. cloud and applications	CERT-In audit guidelines, 2025
Children's data and parental consent	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Examination integrity and leak prevention	Criminal liability; in force since June 2024	Public Examinations Act 2024 (amended 2026)
Coaching centre registration and conduct	Per state adoption	MoE coaching guidelines, 2024
Institutional and accreditation requirements	Per regulator and board	UGC, AICTE, CBSE and state boards
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023
Information security good practice	Standards	ISO/IEC 27001; ISO/IEC 27701

Key dates on the regulatory timeline

Regulatory and Policy Timeline Shaping Education and Research Cybersecurity

Sector instruments, examination-integrity law and cross-sector cyber and privacy obligations



Sources: MeitY, CERT-In, SEBI, Ministry of Education, Gazette of India, PRS. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Student privacy · LMS & exams · Research IP · Managed SOC · Awareness · Platform testing

One partner from admission to alumni



Student Data Privacy

DPDP, consent, children's data



LMS & Exam Security

Portals, question banks, proctoring



Research IP Protection

Classification, segmentation, hunting



24/7 Managed SOC

Campus, cloud and exam monitoring



Awareness & Drills

Phishing, scams, tabletop exercises



Edtech Platform Testing

Web, mobile, API, cloud, SDKs

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

Schools, colleges and coaching institutes

- Campus and portal assessment (B1)
- Backup and recovery review (B3)
- Privacy quick assessment (B6)
- Phishing and fee-fraud awareness (B10)

Assurance

Universities, school chains and edtech platforms

- LMS, app and API testing (B2)
- DPDP programme for children's data (B6)
- Annual independent audit (B4)
- 24x7 managed SOC (B7)

Continuous Resilience

Examination bodies, research organisations and listed edtech

- Continuous testing and red teaming (B1, B10)
- Exam-integrity and research programme (B2, B3)
- SOC with threat hunting (B7)
- Board, regulator and sponsor reporting (B4, B5)

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
Independent cyber audits (CERT-In audit guidelines, 2025)	Independent campus and cloud audits	B4, B1
Children's data and parental consent (DPDP Act and Rules)	DPDPA programme for institutions	B6
Examination integrity and leak prevention (Public Examinations Act)	Exam-system testing and controls	B2, B1
Institutional and accreditation requirements (UGC, AICTE, boards)	Policies, evidence packs, ISO 27001	B5, B4
Quarterly incident disclosure, listed companies (SEBI LODR)	Incident records, disclosure support	B4, B8
Sponsor, collaborator and vendor security clauses (contracts)	Research and vendor assurance	B9, B3

Five new case studies, five broken chains

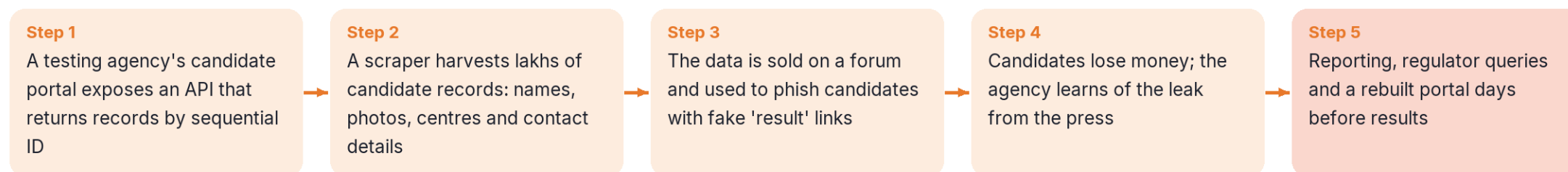
Illustrative composite scenarios written for 2026—not client engagements

1	The Admit Card API That Gave Everything Away	A testing agency's API leaks lakhs of candidate records; API testing and monitoring prevent it	B2 · B7 · B6
2	The Student Who Became the Examiner	An unpatched LMS lets a student alter grades; patching and role controls stop it	B1 · B2 · B7
3	The Grant Application That Opened the Lab	Spear phishing reaches research data; MFA, segmentation and hunting break the chain	B10 · B3 · B7
4	The Ransomware That Arrived in Admissions Week	A phished vendor account encrypts a school chain's ERP; backups and SOC limit it	B9 · B3 · B7
5	The Learning App That Knew Too Much About Children	An open bucket and tracking SDKs expose children's data; privacy and cloud reviews prevent it	B6 · B3 · B9

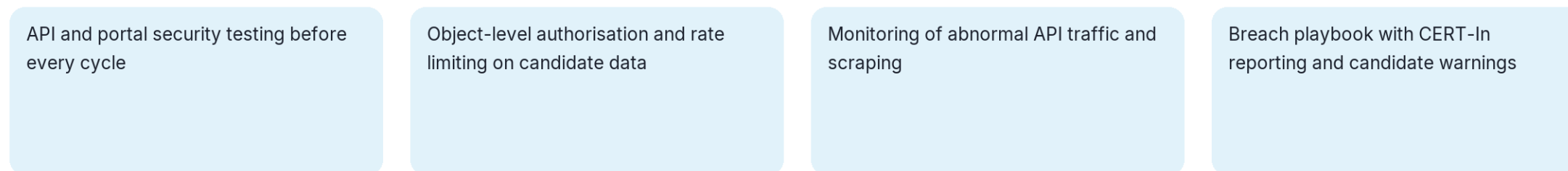
Example: breaking a candidate-data leak chain

Case 1: The Admit Card API That Gave Everything Away

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: whether portal and API endpoints enforce authorisation per candidate, whether scraping and abnormal traffic are detected, how candidate data is stored and shared with vendors, whether a breach can be reported within six hours, and how leadership handles candidates, press and regulators in a tabletop exercise.

Why institutions and platforms 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, examination-integrity expectations, UGC and AICTE requirements 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

Campuses, LMS, ERP and apps, examination systems and vendors, research networks, cloud estate and your academic and audit 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.