

Codec Networks

Coding Threats. Decoding Solutions.

MEDIA, ENTERTAINMENT & DIGITAL PLATFORMS

Protect the Content. Protect the Audience. Protect the Brand.

Platform and API security, content protection, account security, privacy and brand monitoring for media, entertainment and digital platform businesses

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 IT Rules, TRAI, the Online Gaming Act and SEBI expectations



How Codec Networks helps

Services, bundles and packages built for the sector



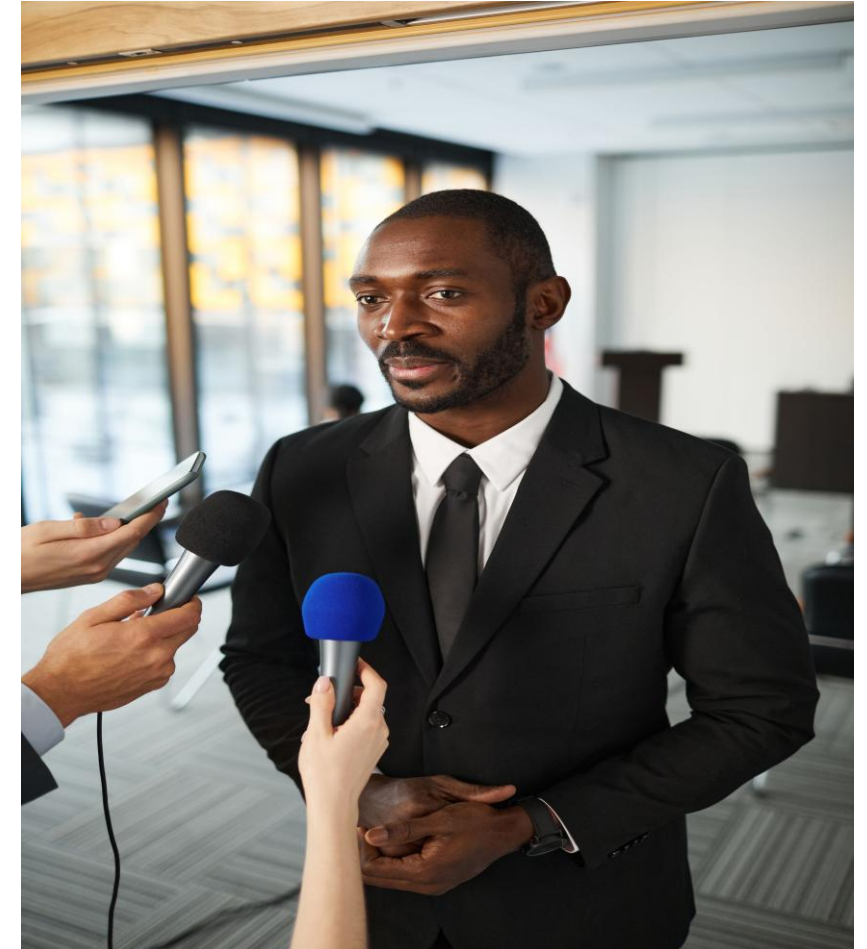
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Media is now a digital, live and always-on target

Indian market data and platform statements show the scale at stake

₹2.78 trillion

India's media and entertainment sector in 2025 (FICCI-EY)

₹22,400 cr

Lost to piracy in India in 2023 (EY-IAMAI)

6.12 crore

Peak concurrent viewers, Champions Trophy final 2025

6 hours

To report cyber incidents to CERT-In

What this means: media businesses and platforms must keep live events up and accounts safe at peak load, protect content from first cut to release, secure apps, APIs and game servers, govern viewer and children's data, spot impersonation and deepfakes fast, and report incidents within six hours.

Sources: FICCI-EY Media & Entertainment Report 2026, EY-IAMAI piracy report 2024, JioStar statement (March 2025), CERT-In.

Who we serve across media, entertainment and digital platforms



Broadcasters and TV networks

Playout, newsrooms, ad sales



Distribution platform operators

DTH, cable, CAS and SMS



OTT streaming services

Apps, CDNs, DRM, subscriptions



News publishers

Digital news, video, social reach



Advertising technology

Ad servers, SSPs, audience data



Film and music production

Studios, post, VFX, catalogues



Gaming and esports

Game servers, players, tournaments



Social and creator platforms

Creators, communities, payouts

The threats that cost media businesses the most

Six priorities from our 18-threat media and platform assessment



Account takeover at scale

Credential stuffing at peak events



Pre-release leaks

Films, episodes and music stolen



Ransomware off air

Playout and newsrooms encrypted



Deepfakes and impersonation

Anchors, stars and brands faked



API and data exposure

Subscriber and player data scraped



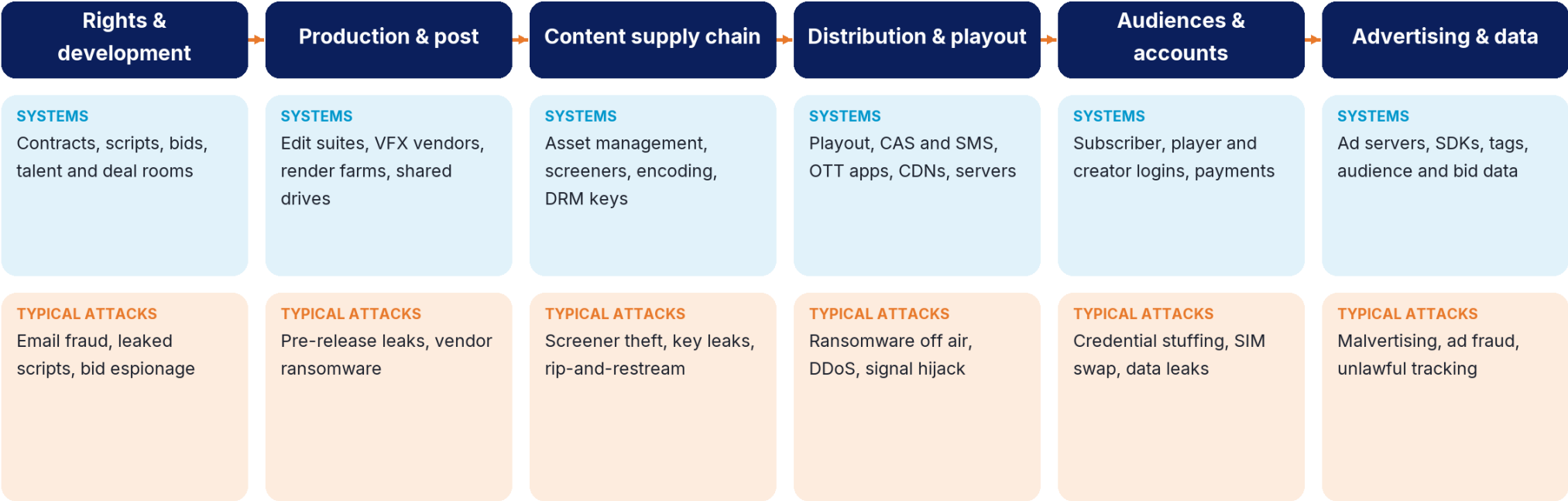
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from script to screen

Where Cyber Risk Sits Across the Media and Platform Lifecycle

Every stage from first script to final ad impression carries its own attack surface



In media, a leak spoils a release, an outage loses a live audience that never comes back, and a deepfake borrows the trust a brand spent decades building.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, DPDP, the IT Rules, TRAI, the Online Gaming Act and SEBI expectations

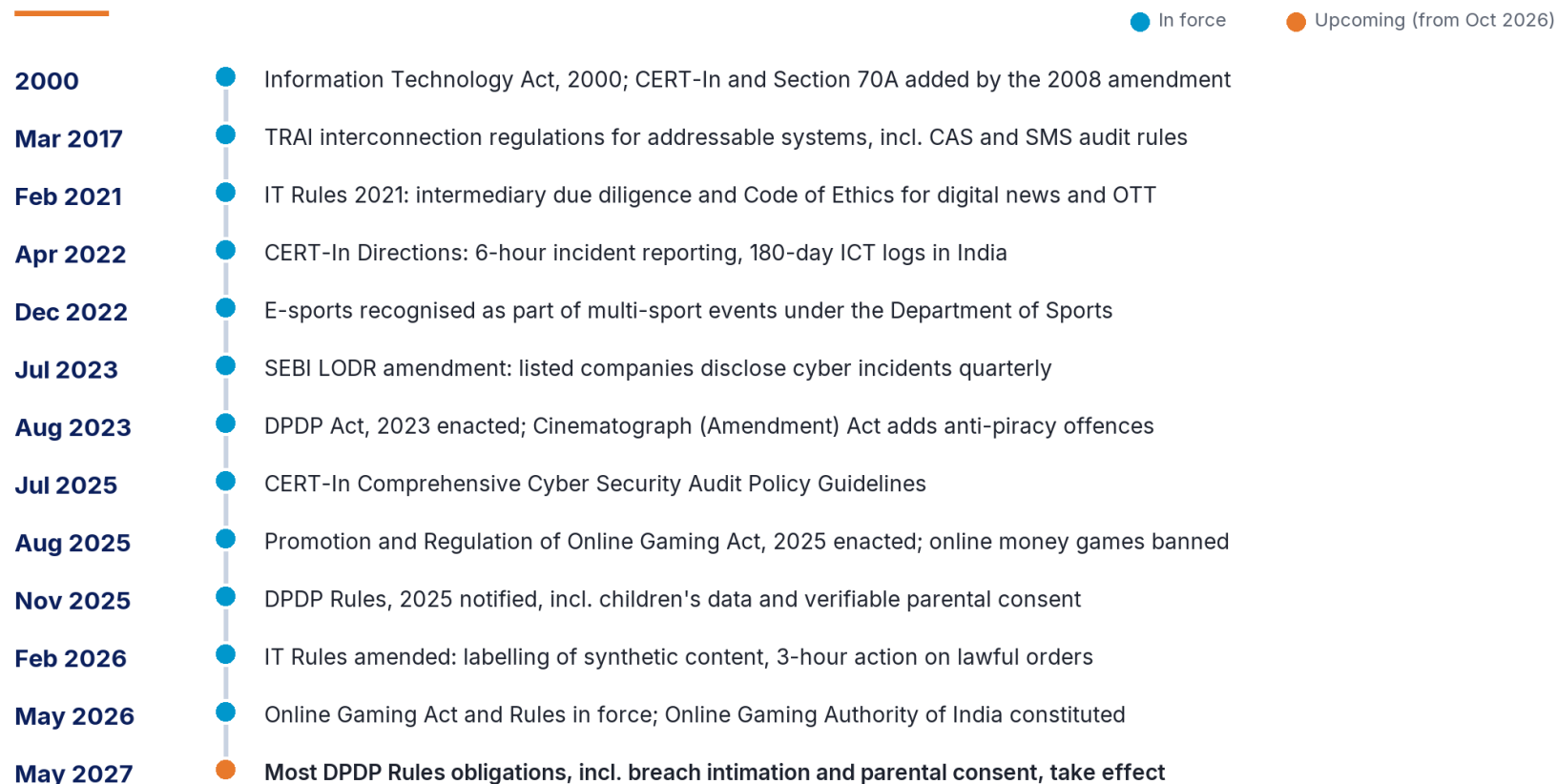
The rules shaping media and platform cybersecurity

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
Viewer, player and children's data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Intermediary and digital media duties	Synthetic-content labels; 3-hour orders	IT Rules 2021, amended Feb 2026
CAS and SMS security and audits	Annual audit for distributors	TRAI interconnection regulations
Online gaming	Money games banned; e-sports promoted	Online Gaming Act 2025, in force May 2026
Anti-piracy	Offences for unauthorised recording	Cinematograph Act as amended 2023
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023

Key dates on the regulatory timeline

Regulatory and Policy Timeline Shaping Media and Platform Cybersecurity

Broadcast, digital media, gaming and anti-piracy instruments, with cross-sector cyber and privacy obligations



Sources: MeitY, MIB, TRAI, CERT-In, SEBI, Gazette of India. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Platforms & APIs · Content protection · Accounts · Privacy · Brand monitoring · Managed SOC

One partner from script to screen



Platform & API Security

Apps, APIs, game servers, cloud



Content Protection

Supply chain, DRM, watermarking



Account Security

Bot defence, MFA, creators



Privacy & DPDP

Viewers, players, children, ads



Brand & Deepfake Monitoring

Impersonation and takedowns



24/7 Managed SOC

Live-event and release cover

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

Production houses, regional channels and digital publishers

- External and app assessment (B1)
- Vendor and screener review (B9)
- Privacy quick assessment (B6)
- Account-security awareness (B10)

Assurance

Broadcasters, OTT services and gaming platforms

- App, API and login testing (B2)
- Content-security programme (B3, B9)
- Annual independent audit (B4)
- 24x7 managed SOC (B7)

Continuous Resilience

Listed media groups, large platforms and studios

- Continuous testing and red teaming (B1, B10)
- Brand and deepfake monitoring (B7, B11)
- SOC with threat hunting (B7)
- Board, regulator and partner 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 platform and IT audits	B4, B1
Viewer, player and children's data (DPDP Act and Rules)	DPDPA programme for platforms	B6
Synthetic-content labels and fast takedowns (IT Rules, 2026)	Monitoring, evidence, playbooks	B7, B10
CAS and SMS security and audits (TRAI interconnection rules)	Audit readiness and evidence	B4, B3
Lawful gaming and player protection (Online Gaming Act 2025)	Platform, payment and data review	B2, B6
Quarterly incident disclosure, listed companies (SEBI LODR)	Incident records, disclosure support	B4, B8

Five new case studies, five broken chains

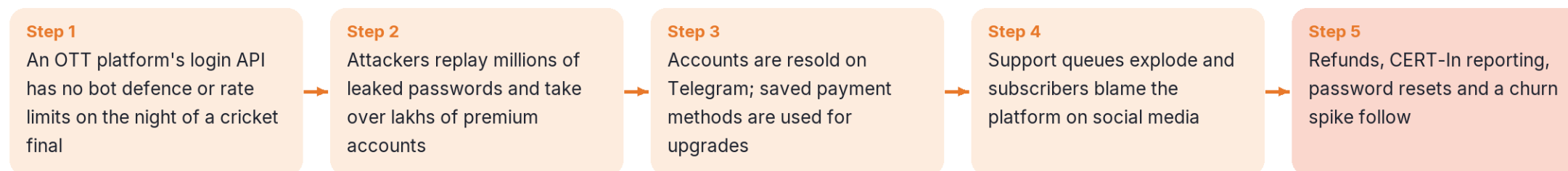
Illustrative composite scenarios written for 2026—not client engagements

1	The Final That Doubled as a Password Test	Credential stuffing takes over lakhs of OTT accounts on match night; bot defence and SOC stop it	B2 · B7 · B3
2	The Screener That Reached Telegram First	A phished dubbing vendor leaks unreleased content; vendor controls and watermarking break the chain	B9 · B3 · B8
3	The Ransomware That Took the Channel Off Air	An exposed gateway lets ransomware reach playout; segmentation and SOC limit it	B3 · B7 · B8
4	The Anchor Who Never Said It	Deepfakes and a hijacked channel push a scam; monitoring and account controls stop it	B10 · B3 · B7
5	The Tournament API That Leaked Its Players	An open player API and DDoS hit an esports final; testing and privacy controls prevent it	B2 · B6 · B7

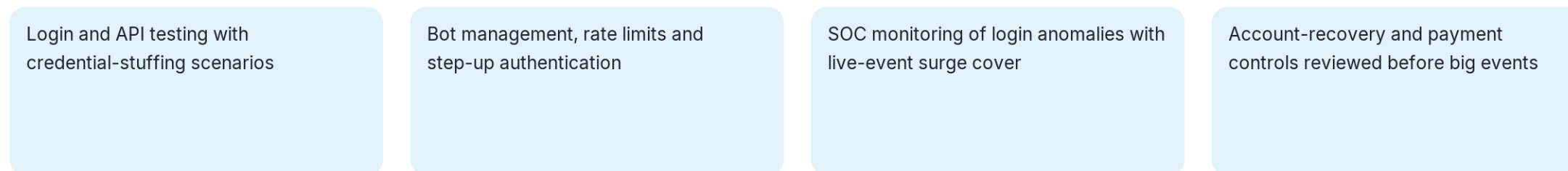
Example: breaking a credential-stuffing chain

Case 1: The Final That Doubled as a Password Test

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 login and account APIs resist automated password replay, whether bot defence and rate limits hold at live-event load, whether step-up checks protect payments and profile changes, whether the SOC sees takeover patterns in real time, and how leadership handles subscribers, press and CERT-In reporting in a tabletop exercise.

Why media businesses and platforms 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, the IT Rules, TRAI audit expectations, the Online Gaming Act and ISO/IEC 27001



Tests the whole chain

Technical, process and monitoring tests together



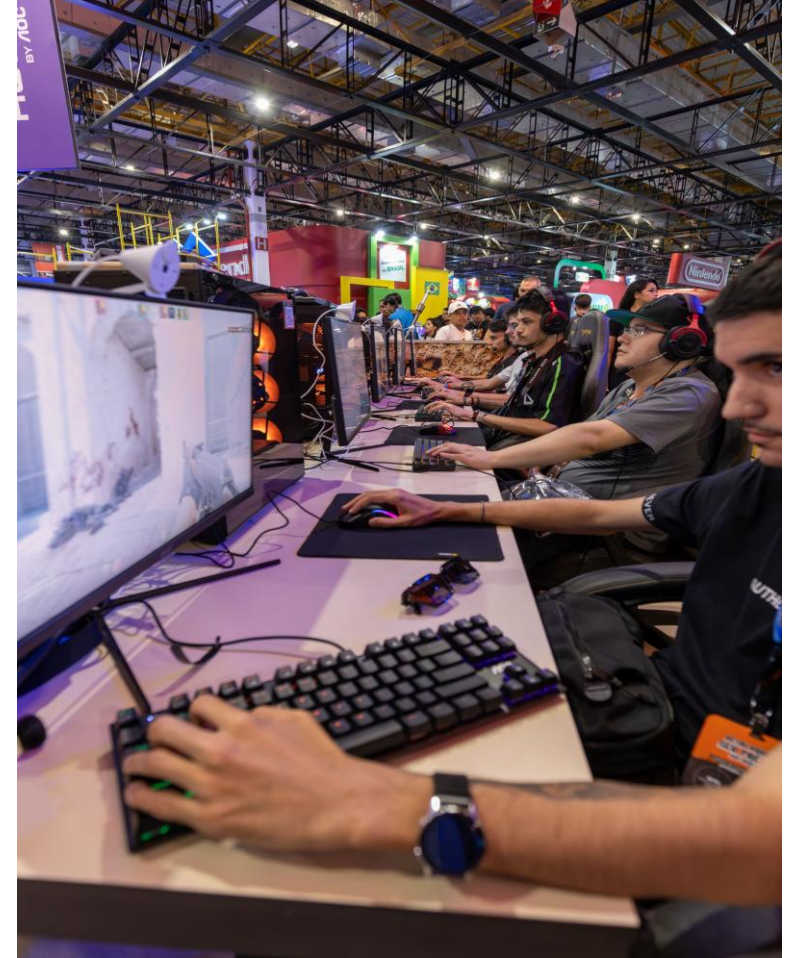
Full stack, one partner

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

Broadcast and newsroom systems, OTT and gaming platforms, apps and APIs, content supply chain and vendors, ad tech, cloud estate and your release and event 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.