

Codec Networks

Coding Threats. Decoding Solutions.

INSURANCE INTERMEDIARIES & INSURTECH

Every Policy You Sell. Secured End to End.

Cyber audits, IRDAI-aligned assessments, API security, claims platform testing and vendor risk for intermediaries and insurtechs

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

IRDAI's 2026 Information and Cyber Security Guidelines



How Codec Networks helps

Services, bundles and packages built for the sector



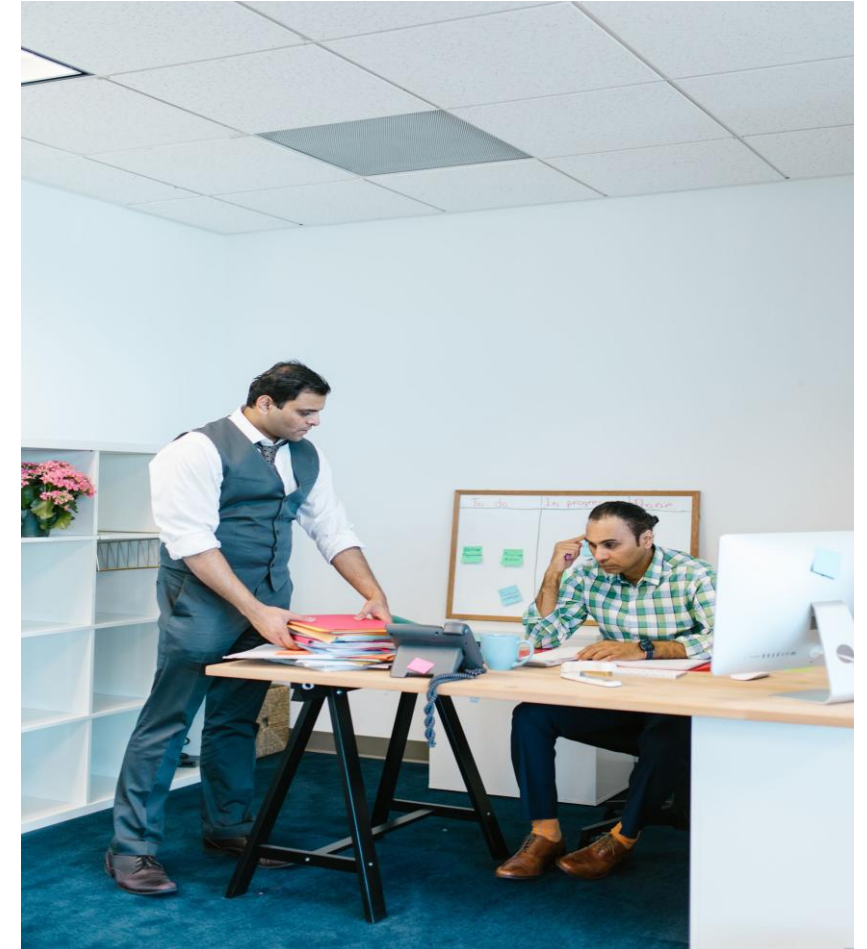
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



A new rulebook for intermediary cybersecurity

IRDAI's April 2026 guidelines cover brokers, corporate agents, web aggregators and TPAs

6 Apr 2026

IRDAI's revised guidelines issued,
covering intermediaries

6 hours

To report cyber incidents to
CERT-In

6-monthly

External PT by CERT-In
empanelled auditors

30 days

To submit compliance reports
after audit (as reported)

What this means: intermediaries must now commission audits by CERT-In empanelled auditors, test internet-facing systems every six months, control vendors and cloud providers, and report incidents within six hours—while insurers scrutinise them as distribution partners.

Source: IRDAI Information and Cyber Security Guidelines, 2026 (6 April 2026), as reported in public sources.

Who we serve across intermediaries and insurtech



Insurance brokers

Direct, reinsurance and composite



Corporate agents

Banks, NBFCs and companies



Web aggregators

Comparison and lead platforms



Third-party administrators

Health claims and cashless



Insurance repositories

e-insurance accounts and e-policies



Digital insurance platforms

Insurtech and embedded insurance



Distributor networks

POSPs and agent platforms



Claims and survey partners

Surveyors and loss assessors

The threats that cost intermediaries the most

Six priorities from our 18-threat intermediary assessment



Customer data leakage

KYC, health and lead data exposed



Broken APIs

Quote, policy and claims data for anyone



Phishing & fake sites

Your brand used against your customers



Premium diversion & BEC

Payments sent to fraudsters



Ransomware

Claims processing and servicing stop



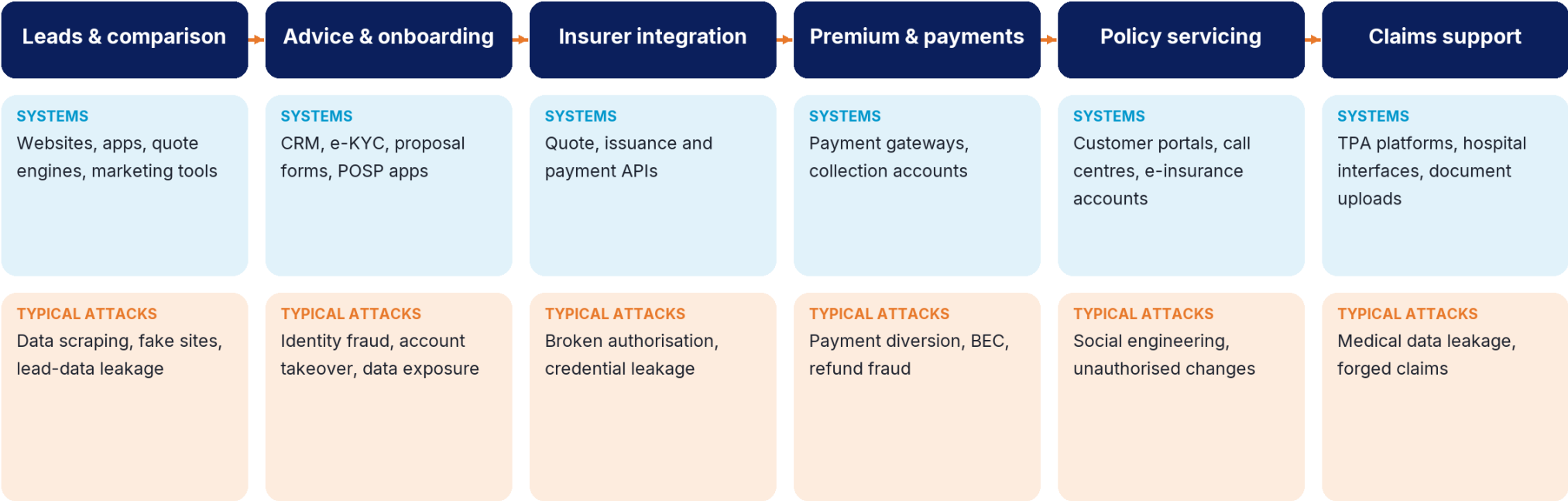
Slow detection & reporting

Missing the 6-hour window

Attacks target every step from lead to claim

Where Cyber Risk Sits in the Intermediary Journey

Every step between a lead and a settled claim carries its own attack surface



Each step touches an insurer's systems—intermediary security is insurer security.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

IRDAI's revised guidelines apply to intermediaries from FY 2026-27

IRDAI 2026—and what it asks of intermediaries

Requirement	Frequency / deadline	Source
Scope	Brokers, corporate agents, web aggregators, TPAs	IRDAI 2026 guidelines
Cyber security audit	By CERT-In empanelled auditors (as reported)	IRDAI 2026 guidelines
Compliance report	Within 30 days of audit completion (as reported)	IRDAI 2026 guidelines
External penetration testing (grey/white box)	At least every six months, CERT-In empanelled	IRDAI 2026 guidelines
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions; IRDAI 2026
Cloud providers	MeitY-empanelled with STQC audit status	IRDAI 2026 guidelines
Vendor contracts	Right-to-audit; sub-outsourcing approval	IRDAI 2026 guidelines
DPDP safeguards and breach intimation	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Key dates on the regulatory timeline

Regulatory Timeline for Intermediary Cybersecurity

Key IRDAI and cross-sector instruments shaping intermediary cybersecurity

● In force ● Upcoming (from Oct 2026)

Apr 2022	●	CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Apr 2023	●	IRDAI Information and Cyber Security Guidelines, 2023, covering intermediaries
Aug 2023	●	Digital Personal Data Protection Act, 2023 enacted
Nov 2025	●	DPDP Rules, 2025 notified with phased commencement
Apr 2026	●	IRDAI Information and Cyber Security Guidelines, 2026 issued (6 April)
FY 2026-27	●	Compliance with the 2026 guidelines required from the current financial year
May 2027	●	Most DPDP Rules obligations, incl. breach intimation, take effect

Sources: IRDAI, CERT-In, MeitY. Confirm timelines against the official IRDAI circular.

Codec Networks

How Codec Networks helps

Cyber audits · Platform assessments · API security · Claims testing · Vendor risk · SOC

One partner from lead to claim



IRDAI Cyber Audits

Gap assessment, empanelled audit, compliance report



Platform Assessments

Websites, apps, distributor portals, e-KYC



API Security

Quote, issuance, payment and claims APIs



Claims Platform Testing

TPA portals, hospital interfaces, uploads



Vendor Risk

Cloud, SaaS and KYC vendors, contracts



24/7 SOC & Response

API abuse signals, brand monitoring, IR

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 brokers and corporate agents

- Gap assessment (B4)
- Annual audit and report (B4)
- Six-monthly external PT (B1)
- Policy pack and awareness (B5, B10)

Assurance

Aggregators, TPAs and growing platforms

- Audit support and closure (B4)
- App, API and claims testing (B2)
- Cloud and DPDPA (B3, B6)
- 24x7 managed SOC (B7)

Continuous Resilience

Large intermediaries and insurtechs

- Red teaming and simulations (B1, B10)
- Vendor and partner assurance (B9)
- SOC with API abuse signals (B7)
- AI and chatbot security (B11)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Audit by a CERT-In empanelled auditor; compliance report within 30 days of audit completion (IRDAI 2026, as reported)	Audit, compliance report and closure tracking	B4
External penetration testing at least six-monthly, grey or white box	Scheduled PT with retest	B1
Cyber incidents to CERT-In within six hours	IR retainer, playbooks and reporting support	B7, B8
Secure applications and APIs connected to insurers	Application and API security testing	B2
MeitY-empanelled CSPs with STQC audit status; data erasure on exit	Cloud review against IRDAI requirements	B3
Vendor right-to-audit, sub-outsourcing approval, supervised privileged access	Vendor risk programme	B9
DPDP safeguards for customer and health data	DPDPA programme and DLP review	B6

Five new case studies, five broken chains

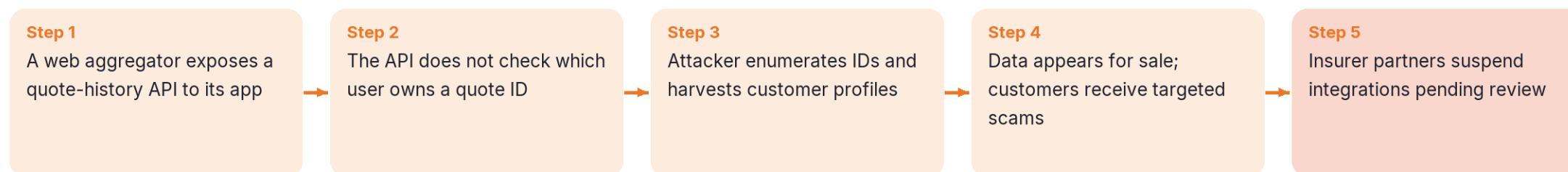
Illustrative composite scenarios written for 2026—not client engagements

1	The Quote API That Answered Everyone	An aggregator API leaks customer profiles; authorisation testing and rate limits prevent it	B2 · B7 · B6
2	The Broker's Premium Account Switch	BEC diverts a client's premium; MFA, DMARC and call-back checks stop it	B10 · B7 · B8
3	The TPA Night Shift Ransomware	An unpatched gateway halts cashless claims; VAPT, SOC and backups limit the damage	B1 · B7 · B8
4	The POSP Logins Sold on Telegram	Phished distributor logins leak data; MFA, anomaly alerts and takedowns stop it	B2 · B7 · B10
5	The Chatbot That Revealed Policy Details	Prompt injection exposes customer data; AI testing and least privilege prevent it	B11 · B2 · B6

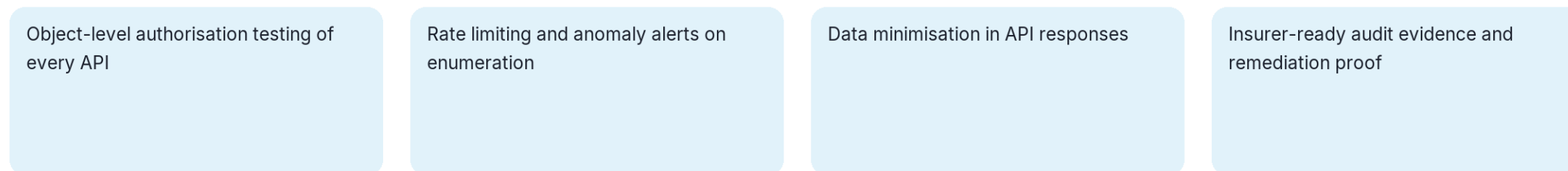
Example: breaking an API data-exposure chain

Case 1: The Quote API That Answered Everyone

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: object-level authorisation on every quote, policy and claims API, enumeration and rate-limit controls, minimal data in responses, anomaly alerts on bulk access and the evidence insurer partners will ask for.

Why intermediaries choose Codec Networks



CERT-In empanelled

For information security auditing services; NISAP empanelled for application audits



Certified

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



Regulation-mapped

Mapped to IRDAI's 2026 guidelines, CERT-In and DPDP



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

Intermediary type, insurer partners, platforms, APIs 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.