Codec Networks

Coding Threats. Decoding Solutions.

HOSPITALITY, TRAVEL & TOURISM

Protect the Guest. Protect the Brand.

Guest data protection, booking and payment security, Wi-Fi testing, SOC and brand monitoring for hotels, travel platforms, tour operators, restaurants and venues

What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

CERT-In, DPDP, RBI tokenisation and PCI DSS, immigration reporting and SEBI

How Codec Networks helps

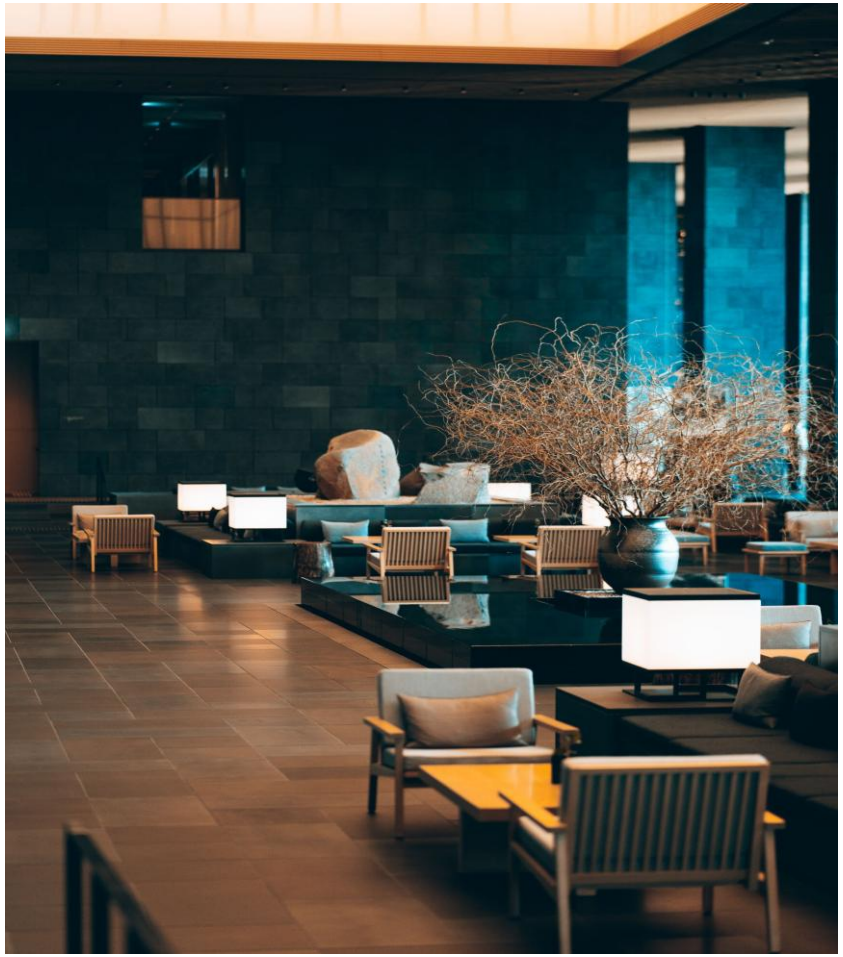
Services, bundles and packages built for the sector

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



Cyber incidents in hospitality expose guests and stop operations

Global incidents show the data and operational stakes

339 m

Guest records exposed in the Marriott Starwood breach (2018)

£18.4 m

UK ICO fine imposed on Marriott in 2020

9.95 m

Foreign tourist arrivals in India in 2024

6 hours

To report cyber incidents to CERT-In

What this means: hospitality and travel companies must know where guest identity and card data sit, secure booking and payment flows, lock down OTA and loyalty accounts, segment guest Wi-Fi and property systems, hold vendors to account, monitor around the clock and report incidents within six hours.

Sources: Marriott disclosures, UK ICO, Ministry of Tourism, CERT-In.

Who we serve across hospitality, travel and tourism

Hotel chains

Brands and management companies

Hotel owners

Owners, franchisees, boutique hotels

OTAs and booking platforms

Online travel, metasearch, aggregators

Tour operators

Inbound, outbound, destination management

Restaurants and QSR

Chains, cloud kitchens, delivery

Event venues

Convention centres, banquets, stadiums

Loyalty and travel tech

Loyalty, PMS, channel and payment vendors

Attractions and leisure

Parks, resorts, wellness, cruises

The threats that cost hospitality and travel companies the most

Six priorities from our 18-threat sector assessment

Guest data breaches

Passports, cards and stays exposed

Ransomware shutdowns

PMS, PoS and keys stopped at peak

Extranet and loyalty takeover

Guests defrauded in your name

Payment skimming and fraud

Booking engines and PoS targeted

Guest Wi-Fi attacks

Executives and delegates intercepted

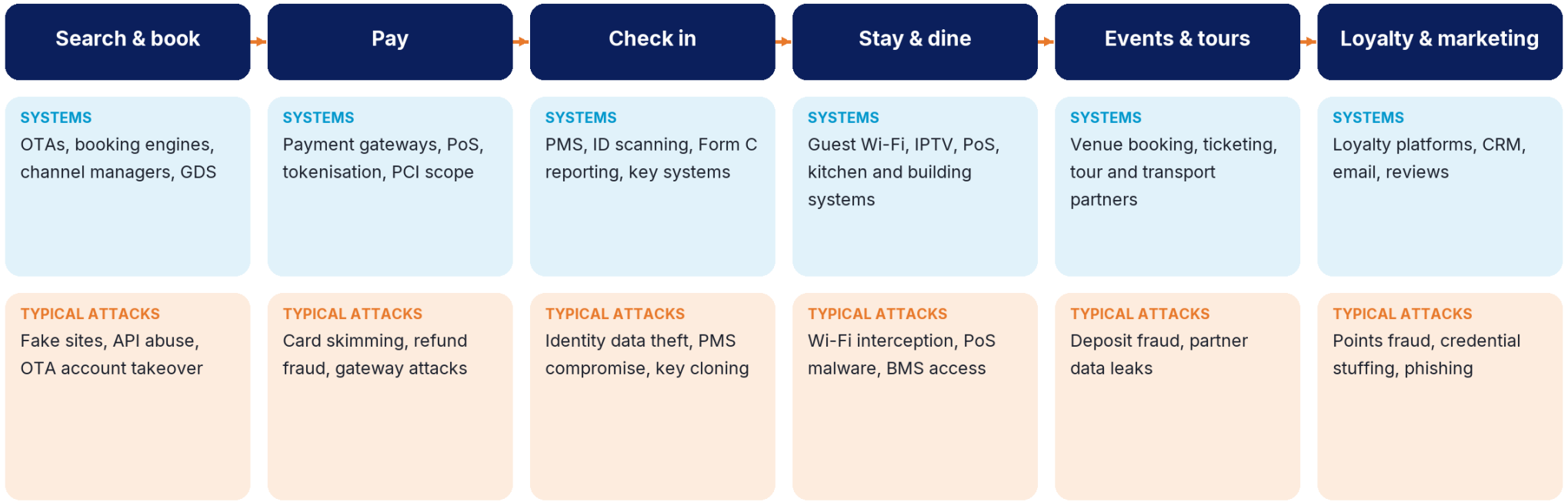
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage of the guest journey

Where Cyber Risk Sits Across the Guest Journey

Every stage from search to loyalty carries its own attack surface



A hotel that loses guest data loses trust across every brand it carries—guest data, payments and the networks guests touch must be protected together.

Source: Codec Networks analysis

Codec Networks

Codec Networks
Coding Threats. Decoding Solutions.

What regulators now expect

CERT-In, DPDP, RBI tokenisation and PCI DSS, immigration reporting and SEBI

Codec Networks
Coding Threats. Decoding Solutions.

The rules and standards shaping hospitality and travel 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
Guest, loyalty and employee data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
No merchant storage of card data; tokenisation	Since 1 October 2022	RBI card-on-file tokenisation
Payment environment controls	Ongoing; v4.0.1 current	PCI DSS v4.0.1
Form C reporting of foreign guests	Within 24 hours of arrival	Immigration and Foreigners Act 2025 and Rules
E-invoicing and room-rate slabs	Per GST notifications	GST law; 56th GST Council (Sep 2025)
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023

Key dates on the regulatory timeline

Regulatory and Standards Timeline Shaping Hospitality and Travel Cybersecurity

Payment, data, tax, immigration and cross-sector instruments and the incidents behind them

In force · Upcoming (from Oct 2026)

2000	Information Technology Act, 2000; amended 2008 with CERT-In and reasonable security practices
Nov 2014	Kaspersky publishes the Darkhotel report on hotel Wi-Fi attacks against executives
May 2017	Sabre discloses breach of its SynXis central reservations system affecting hotel card data
Nov 2018	Marriott discloses the Starwood reservation breach affecting ~339 million guest records
Oct 2020	UK ICO fines Marriott £18.4 million over the Starwood breach
Mar 2022	PCI DSS v4.0 published; v4.0.1 follows in June 2024
Apr 2022	CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Oct 2022	RBI card-on-file tokenisation: merchants may no longer store card data
Aug 2023	Digital Personal Data Protection Act enacted; GST e-invoicing threshold lowered to ₹5 crore
Sep 2023	Scattered Spider attacks disrupt MGM Resorts and Caesars in Las Vegas
Jul 2025	CERT-In Comprehensive Cyber Security Audit Policy Guidelines
Sep 2025	Immigration and Foreigners Act, 2025 in force; GST on hotel rooms moves to 5%/18% slabs
Nov 2025	DPDP Rules, 2025 notified with phased commencement
May 2027	**Most DPDP Rules obligations, incl. breach intimation, take effect**

Sources: MeitY, CERT-In, RBI, PCI SSC, CBIC, MHA, public incident reporting. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Guest data · Bookings & payments · Wi-Fi · SOC · Brand monitoring · Vendors

Codec Networks
Coding Threats. Decoding Solutions.

One partner from the booking engine to the guest room

Guest Data Protection

DPDP across PMS, OTA, payment and CRM

Booking & Payment Security

Booking engines, apps, APIs, PCI DSS

Wi-Fi Testing

Guest, conference, IoT and building systems

24/7 SOC

Properties, platforms and vendors monitored

Brand Monitoring

Fake sites, impersonation, leaked data

Vendor & Platform Assurance

PMS, channel and payment vendors

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services

- **B1** Cyber Assessment & VAPT Assurance
- **B2** Application, API & DevSecOps Security
- **B3** Cloud, Infrastructure & Zero Trust
- **B4** Regulatory Cyber Audit & Compliance
- **B5** GRC, ISO, SOC 2 & PCI DSS Maturity
- **B6** Data Privacy & DPDPA Program
- **B7** Managed SOC, MDR & Threat Monitoring
- **B8** Forensics, Incident Response & Malware RCA
- **B9** Third-Party & Supply-Chain Risk
- **B10** Cyber Simulation, Awareness & Tabletop
- **B11** Emerging Tech, AI & Web3 Security

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

Independent hotels, restaurants and tour operators

- Property IT and Wi-Fi assessment (B1)
- Booking and payment flow review (B2, B5)
- Backup and recovery review (B3)
- Policy, awareness and crisis plan pack (B5, B10)

Assurance

Hotel chains, QSR groups and venues

- Booking engine, app and API testing (B2)
- PCI DSS readiness and DPDP programme (B5, B6)
- Annual independent audit (B4)
- 24x7 SOC with brand monitoring (B7)

Continuous Resilience

Listed groups, OTAs and loyalty platforms

- Testing and red teaming (B1, B10)
- Loyalty and payment fraud analytics (B2, B7)
- SOC with threat hunting (B7)
- Board, regulator and owner 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 guidelines, 2025)	Independent IT and application audits	B4, B1
Guest, loyalty and employee personal data (DPDP)	DPDPA programme	B6
No card storage; tokenisation (RBI, 2022); PCI DSS v4.0.1	PCI DSS scoping, testing and readiness	B5, B2
Form C reporting of foreign guests (Immigration law, 2025)	Secure identity data handling	B6, B3
Quarterly incident disclosure, listed companies (SEBI LODR)	Incident records, disclosure support	B4, B8
Brand, owner and OTA security standards (contracts)	Standards audits and evidence packs	B5, B9

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Extranet Login That Robbed the Guests**	A phished OTA extranet account is used to defraud guests; MFA, monitoring and takedowns stop it	**B10 · B7 · B2**
2	**The PMS Vendor That Opened Every Door**	A cloud PMS vendor's compromised account leaks identity data; vendor assurance and minimisation limit it	**B9 · B6 · B7**
3	**The Deposit That Left With the Email**	A compromised mailbox diverts a MICE deposit; verification and monitoring stop it	**B10 · B7 · B2**
4	**The Points That Became Plane Tickets**	Credential stuffing drains loyalty accounts; bot management and anomaly detection catch it	**B2 · B7 · B6**
5	**The Resort That Ran on Paper**	Ransomware encrypts PMS, PoS and keys at peak season; segmentation and tested backups prevent it	**B3 · B7 · B10**

Example: breaking a phishing-to-guest-fraud chain

Case 1: The Extranet Login That Robbed the Guests

ILLUSTRATIVE ATTACK PATH

Step 1
A hotel's reservations desk is phished with a fake OTA 'guest complaint' email

→

Step 2
Attackers log in to the OTA extranet with the stolen credentials; there is no MFA

→

Step 3
They message upcoming guests through the platform asking for 'payment verification'

→

Step 4
Dozens of guests pay on a look-alike site before the hotel notices

→

Step 5
Refund disputes, OTA penalties, DPDP questions and a brand-trust crisis

WHERE CONTROLS BREAK THE CHAIN

- MFA and least privilege on every OTA and channel manager account
- Phishing simulation and reservations team training
- Monitoring of extranet logins and guest messaging anomalies
- Guest communication playbook and takedown of look-alike sites

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

Codec Networks

What we test: whether OTA and channel manager accounts enforce MFA and least privilege, whether reservations teams recognise OTA-themed phishing, whether extranet logins and guest messaging are monitored for anomalies, how fast look-alike payment sites can be taken down, and how the hotel communicates with affected guests in a tabletop exercise.

Why hospitality and travel 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, RBI tokenisation, PCI DSS v4.0.1, immigration reporting and brand standard expectations

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

Properties and brands, PMS and booking platforms, OTA and payment integrations, Wi-Fi and building systems, vendors with access, guest data and your 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.

Codec Networks
Coding Threats. Decoding Solutions.