

Codec Networks
Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · HOSPITALITY, TRAVEL & TOURISM

Protect the Guest. Protect the Brand.

Guest data protection, booking and payment security, Wi-Fi testing, SOC and brand monitoring for hotel chains and owners, online travel agencies and booking platforms, tour operators, restaurant and QSR chains and event venues.

- Guest Data Protection
- Booking & Payment Security
- Wi-Fi Testing
- 24/7 SOC
- Brand Monitoring
- Vendor & Platform Assurance

THE CHALLENGE

Guests trust you with their passports, their cards and their plans.

Hotels, travel platforms and venues hold passports, card data and travel patterns across PMS, OTA, payment, loyalty and Wi-Fi systems run largely by vendors. Marriott's Starwood breach exposed about 339 million guest records, and the 2023 attacks on MGM Resorts and Caesars shut down hotel operations in Las Vegas.



What keeps leadership teams awake

- Guest identity and card data breaches
- Ransomware halting check-in, PoS and keys
- OTA, extranet and loyalty account takeover
- Payment skimming and refund fraud
- Guest Wi-Fi and venue network attacks
- CERT-In, DPDP, PCI DSS and Form C obligations

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

The rulebook has changed

Instrument	What it means for you
CERT-In Directions and audit guidelines (2022, 2025)	6-hour incident reporting, 180-day logs; risk-based independent cyber audits covering IT, cloud and applications
DPDP Act and Rules (2023, 2025)	Notices, safeguards, retention limits and breach intimation for guest and loyalty data; most obligations from May 2027
RBI tokenisation · PCI DSS v4.0.1	No storage of card data by merchants since October 2022; PCI DSS for booking, PoS and payment environments
Immigration law 2025 · GST · SEBI LODR	Form C reporting of foreign guests within 24 hours; e-invoicing; quarterly cyber incident disclosure for listed companies

OUR SERVICE OFFERINGS

One partner from the booking engine to the guest room

Built around our primary proposition for the sector: **Guest data protection, booking and payment security, Wi-Fi testing, SOC and brand monitoring.**

Guest Data Protection

- DPDP programmes for guest, loyalty and employee data
- Data mapping across PMS, OTA, payment and CRM systems
- Identity document and Form C data handling reviews
- Breach readiness and intimation playbooks

Booking & Payment Security

- Booking engine, app and OTA API testing
- PCI DSS v4.0.1 scoping and readiness
- Tokenisation, gateway and PoS integration reviews
- Refund and chargeback fraud controls

Wi-Fi Testing

- Guest and conference Wi-Fi penetration testing
- Segmentation and client isolation reviews
- Rogue access point and captive portal testing
- IPTV, IoT and building system exposure reviews

24/7 SOC

- Monitoring across properties, platforms and cloud
- Extranet, loyalty and payment anomaly detection
- Vendor access monitoring
- 6-hour CERT-In reporting support

Brand Monitoring

- Look-alike domain and fake booking site detection
- Social media and review platform impersonation
- Takedown coordination
- Dark web monitoring for guest and credential data

Vendor & Platform Assurance

- PMS, channel manager and payment vendor assessments
- Contract clauses for breach notification and audit
- Franchise and owner security standards
- Joint incident exercises with vendors

Who we serve: hotel chains and management companies · hotel owners and franchisees · online travel agencies and booking platforms · tour operators and destination management companies · restaurant and QSR chains · event venues and convention centres.

BUNDLED SERVICE MODELS

Packaged for how hospitality and travel companies buy

Eleven Codec Networks bundles apply directly to hospitality, travel and tourism companies:

- **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

Foundation

Independent hotels, restaurants and tour operators

- Property IT and Wi-Fi assessment
- Booking and payment flow review
- Backup and recovery review
- Policy, awareness and crisis plan pack

Assurance

Hotel chains, QSR groups and venues

- Booking engine, app and API testing
- PCI DSS readiness and DPDP programme
- Annual independent audit
- 24x7 SOC with brand monitoring

Continuous Resilience

Listed groups, OTAs and loyalty platforms

- Continuous testing and red teaming
- Loyalty and payment fraud analytics
- SOC with threat hunting
- Board, regulator and owner reporting

Mapped to your obligations

Requirement	How we help	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

THE CODEC NETWORKS VALUE ADD

Why hospitality and travel companies choose Codec Networks

CERT-In empanelled

Independent audits recognised by regulators, brands, owners and partners.

Certified and accountable

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

Guest-journey testing

Booking engines, apps, OTA integrations, payments and Wi-Fi tested the way attackers use them.

Standards-mapped

Findings mapped to PCI DSS v4.0.1, DPDP, ISO/IEC 27001 and CERT-In expectations.

Full stack, one partner

Testing, privacy, SOC, brand monitoring and forensics connected from finding to closure.

Certified experts

CISA, ISO 27001 LA/LI, CEH, OSCP and CHFI professionals.

How we engage

Discover & scope

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.

Assess & test

Threat-led testing and regulatory audits executed by certified specialists.

Report in business terms

Findings, risk ratings and a compliance gap matrix for the Board and regulators.

Remediate

Practical, prioritised fixes with technology and compliance teams.

Validate & prove

Retesting and an evidence tracker for auditors, regulators and partners.

Monitor & improve

Managed SOC, recurring testing and quarterly governance reviews.

What you receive: executive summary for the Board or its committee · technical findings with evidence and CVSS ratings · compliance gap matrix · prioritised remediation roadmap · retest reports · audit evidence tracker · SOC dashboards and MTTD/MTTR metrics.



START WITH A SCOPING SESSION

Let's make your next peak season, audit and incident a non-event.

Tell us your properties, platforms, vendors and guest data flows. We will propose a practical assessment and assurance plan.

New Delhi

507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place, New Delhi – 110001

Gurugram

707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50, Gurugram – 122018, Haryana

Call

011 430 496 96 · 011 437 522 99
+91 99716 76124 · +91 88007 88220 · +91 88003 31124

Write

mktg@codecnetworks.com
www.codecnetworks.com

Codec Networks

Coding Threats. Decoding Solutions.

Secure Today. Innovate Tomorrow. Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Packages are proposed groupings of Codec Networks bundles, finalised through scoping. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Sources: Marriott disclosures, UK ICO, Ministry of Tourism, CERT-In. Confirm obligations against the official instruments.