

Codec Networks

Coding Threats. Decoding Solutions.

RETAIL & E-COMMERCE

Keep the Checkout Safe. Keep the Customer's Trust.

Web, mobile and API VAPT, payment integration security, privacy, brand protection and SOC for retail chains, marketplaces, D2C brands, quick commerce and omnichannel retailers

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, RBI payment rules, PCI DSS, consumer protection and DPDP



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 retail hit revenue and trust

Global and Indian data show the commercial stakes

US\$345 bn

India's projected e-commerce market by 2030 (IBEF)

59%

Of retail web traffic is malicious bots (Imperva, 2025)

£300 m

Estimated profit hit from the 2025 Marks & Spencer attack

6 hours

To report cyber incidents to CERT-In

What this means: retailers must harden storefronts, apps and APIs, isolate and monitor the payment page, stop account takeover and bots, protect customer data under DPDP, survive the festive peak and report incidents within six hours.

Sources: IBEF, Imperva Bad Bot Report 2025, Marks & Spencer statements, public reporting, CERT-In.

Who we serve across retail and e-commerce



Retail chains and supermarkets

Stores, POS, loyalty, supply chain



Online marketplaces

Sellers, catalogues, checkout, APIs



D2C brands

Storefront platforms, CRM, social commerce



Quick commerce

Dark stores, rider apps, 10-minute delivery



Omnichannel and fashion retail

Stores plus app, click-and-collect



Consumer electronics retail

High-value stock, EMI and BNPL checkout



Payments, loyalty and gift cards

Wallets, points, stored value



Retail technology and 3PL partners

Commerce SaaS, couriers, fulfilment

The threats that cost retailers the most

Six priorities from our 18-threat retail and e-commerce assessment



Payment page skimming

Scripts stealing cards at checkout



Account takeover and bots

Credential stuffing, scalping, scraping



Customer data breaches

CRM, cloud and API leaks



Festive-season DDoS and outages

Checkout down on the biggest day



Third-party and plugin compromise

Scripts, SaaS, partners and franchisees



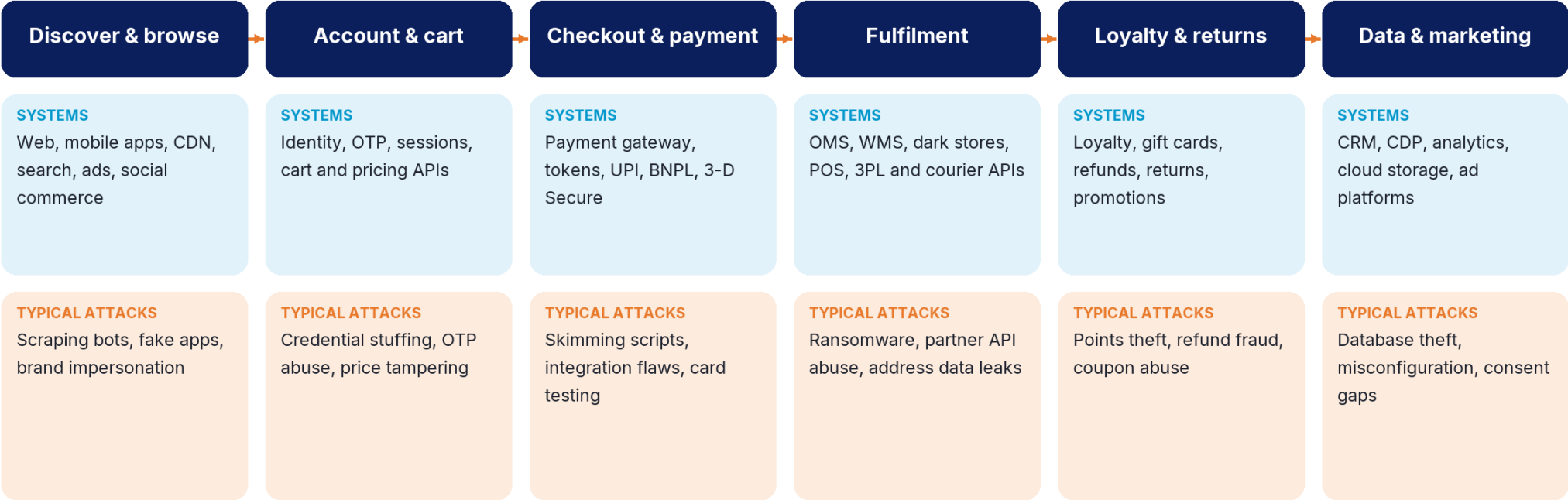
Slow detection & reporting

Missing the 6-hour window

Attacks target every step from browsing to delivery

Where Cyber Risk Sits Across the Retail and E-commerce Journey

Every step from browsing to delivery carries its own attack surface



In retail, an hour of checkout downtime in the festive peak is lost revenue—and a stolen customer database is lost trust.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, RBI payment rules, PCI DSS, consumer protection and DPDP

The rules and standards shaping retail 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. applications and cloud	CERT-In audit guidelines, 2025
No card data stored by merchants; tokenisation	Since Oct 2022; PA Directions Sep 2025	RBI PA guidelines and CoF tokenisation
Payment page script and cardholder data controls	Future-dated requirements since Mar 2025	PCI DSS v4.0.1
Grievance officer, disclosures, no dark patterns	Ongoing	E-Commerce Rules 2020; CCPA Guidelines 2023
Customer, loyalty and seller data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023
Information security good practice	Standards	ISO/IEC 27001; OWASP ASVS, MASVS, API Top 10

Key dates on the regulatory timeline

Regulatory and Standards Timeline Shaping Retail and E-commerce Cybersecurity

Consumer, payment, data and cross-sector cyber instruments that reach Indian retailers and platforms

● In force ● Upcoming (from Oct 2026)

2000	● Information Technology Act, 2000 enacted; CERT-In and data provisions added by the 2008 amendment
Jan 2018	● Legal Metrology (Packaged Commodities) amendments bring e-commerce listings under declaration rules
Feb 2019	● Press Note 2 of 2018: FDI conditions for marketplace e-commerce take effect
Jul 2020	● Consumer Protection Act, 2019 in force; Consumer Protection (E-Commerce) Rules, 2020 notified
Mar 2021	● RBI clarifies PA/PG guidelines: merchants may not store customer card credentials
Apr 2022	● CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India; ONDC pilot launched
Oct 2022	● RBI card-on-file tokenisation: no clear card data stored by merchants and aggregators
Aug 2023	● Digital Personal Data Protection Act, 2023 enacted
Nov 2023	● CCPA Guidelines for Prevention and Regulation of Dark Patterns, 2023 notified
Mar 2025	● PCI DSS v4.0.1 future-dated requirements, incl. payment page script controls, take effect
Jul 2025	● CERT-In Comprehensive Cyber Security Audit Policy Guidelines
Sep 2025	● RBI (Regulation of Payment Aggregators) Directions, 2025 consolidate PA rules
Nov 2025	● DPDP Rules, 2025 notified with phased commencement
May 2027	● Most DPDP Rules obligations, incl. consent and breach intimation, take effect

Sources: MeitY, CERT-In, RBI, Department of Consumer Affairs, DPIIT, PCI SSC. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

VAPT · Payments · Privacy · Brand & Fraud · Festive Readiness · Retail SOC

One partner from storefront to settlement



Web, Mobile & API VAPT

Storefront, app, API, POS, business logic



Payment Integration Security

Gateway, tokens, payment page, PCI DSS



Privacy & DPDP

Customer, loyalty and seller data



Brand & Fraud Protection

Fake apps, domains, loyalty and refund fraud



Bot, DDoS & Festive Readiness

Load and DDoS tests, bot management, drills



24/7 Retail SOC

Monitoring, fraud signals, threat hunting

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

D2C brands and single-format retailers

- Storefront, app and API assessment (B1)
- Payment integration and PCI scoping review (B2, B4)
- Cloud posture and secrets review (B3)
- Privacy quick assessment and policy pack (B6, B5)

Assurance

Regional chains and growing marketplaces

- Annual VAPT with retests (B1, B2)
- Payment page and tokenisation controls (B2, B4)
- Independent audit and PCI DSS readiness (B4, B5)
- 24x7 SOC with fraud signals (B7)

Continuous Resilience

National retailers, marketplaces and quick commerce

- Continuous testing and red teaming (B1, B10)
- Bot, DDoS and festive-readiness programme (B3, B10)
- Partner, seller and 3PL risk programme (B9)
- SOC with threat hunting and Board reporting (B7, B4)

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 and reporting support	B7, B8
No card data stored by merchants; tokenisation (RBI PA, CoF rules)	Payment integration and token reviews	B2, B4
Payment page and cardholder data controls (PCI DSS v4.0.1)	PCI DSS scoping, gap assessment, evidence	B4, B5
Grievance officer and disclosures (E-Commerce Rules 2020)	Platform governance and policy support	B5
No dark patterns in interfaces (CCPA Guidelines 2023)	Consent and interface review	B6
Customer, loyalty and seller personal data (DPDP)	DPDPA programme	B6
Quarterly incident disclosure, listed retailers (SEBI LODR)	Incident records, disclosure support	B4, B8

Five new case studies, five broken chains

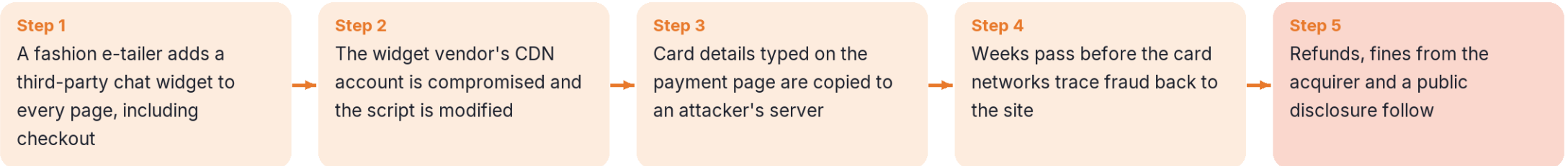
Illustrative composite scenarios written for 2026—not client engagements

1	The Script That Stole the Checkout	A compromised chat widget skims cards at checkout; script controls and tamper detection stop it	B2 · B9 · B4
2	The Festive Sale That Never Loaded	Scalper bots and DDoS take down a festive sale; resilience testing and bot management prevent it	B1 · B3 · B10
3	The Loyalty Points That Walked Away	Credential stuffing drains loyalty points into gift cards; MFA and redemption controls block it	B1 · B7 · B8
4	The Dark Store That Went Dark	A franchisee's VPN brings ransomware into WMS and dispatch; zero-trust access and backups contain it	B3 · B9 · B7
5	The Customer File on Sale	An open cloud bucket and leaked key expose 4 million records; posture review and DPDP readiness prevent it	B3 · B6 · B8

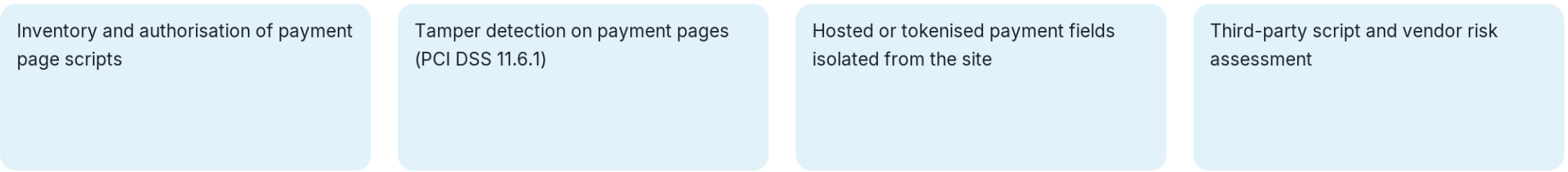
Example: breaking a payment page skimming chain

Case 1: The Script That Stole the Checkout

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: every script loaded on the payment page and who can change it, the isolation of card entry fields, tamper detection and alerting, the gateway and tokenisation integration, the vendor's own security, and whether the SOC would see data leaving the checkout.

Why retailers 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 OWASP, PCI DSS v4.0.1, RBI payment rules, CERT-In expectations and DPDP



Tests the whole chain

Technical, process and monitoring tests together



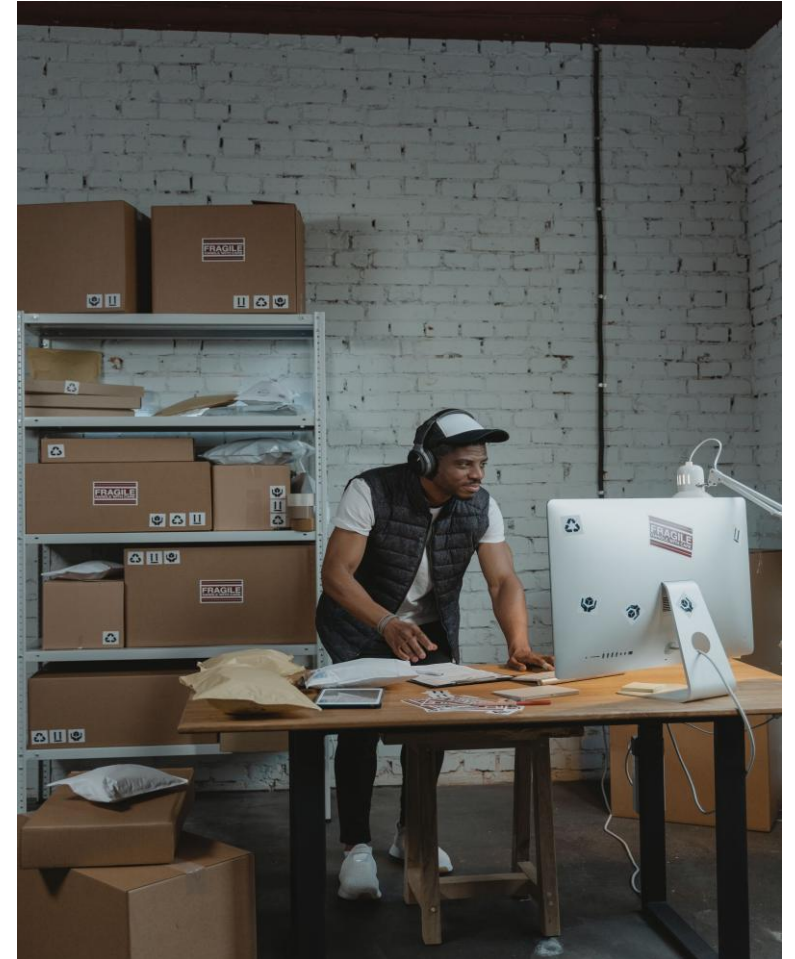
Full stack, one partner

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

Storefronts, apps and APIs, payment stack, cloud platforms, stores and dark stores, partners and sellers, and your sales 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.