

Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · TEXTILES, APPAREL & CONSUMER MANUFACTURING

Ship Every Season. Keep Every Design.

ERP and e-commerce security, IP protection, 24x7 SOC, privacy and supplier assurance for textile mills, garment and footwear exporters, consumer products manufacturers, brand owners and their D2C arms.

ERP & E-commerce Security

IP Protection

24/7 SOC

Privacy & DPDP

Supplier Assurance

Buyer Questionnaire Readiness

THE CHALLENGE

In textiles and apparel, a cyber incident is a missed season.

India's textile sector employs more than 45 million people directly, and the country is the world's second-largest footwear producer. Factories run on ERP, PLM and e-commerce platforms, ship to brands that audit their vendors and increasingly sell direct to consumers. VF Corp's 2023 incident disrupted fulfilment and exposed data on about 35.5 million consumers.

What keeps leadership teams awake

- Ransomware stopping shipments in peak season
- Export proceeds diverted by email fraud
- Designs and tech packs leaking to competitors
- Credential stuffing and skimming on D2C sites
- Brand security questionnaires and audits
- CERT-In reporting, SEBI disclosure and DPDP



35.5 mn

Consumers affected by
VF Corp's December
2023 incident

US\$100 m

Sales Hanesbrands lost
to ransomware in one
quarter (2022)

45 mn+

People directly employed
in India's textile sector

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
SEBI LODR · Companies Act	Listed companies disclose cyber incidents quarterly; Boards accountable for risk
DPDP Act and Rules (2023, 2025)	Safeguards for consumer, loyalty and worker data; most obligations from May 2027
Buyer, tax and product rules	Brand security questionnaires; GST e-invoicing above ₹5 crore; BIS QCOs; EU CRA

One partner from design to doorstep

Built around our primary proposition for the sector: **ERP and e-commerce security, IP protection, SOC, privacy and supplier assurance.**

ERP & E-commerce Security

- ERP, PLM and order-management configuration and access reviews
- Web, API and mobile testing of D2C sites and apps
- Buyer portal, EDI and marketplace integration testing
- Payment, checkout and third-party script controls

IP Protection

- Classification of designs, tech packs and costing data
- DLP and shared-drive monitoring
- Contractor and leaver access controls
- Forensic readiness for IP disputes

24/7 SOC

- Monitoring across plants, offices and cloud
- Account takeover and fraud pattern detection
- BEC and look-alike domain monitoring
- 6-hour CERT-In reporting support

Privacy & DPDP

- Consumer, loyalty and CRM data mapping
- Worker and employee data safeguards
- Consent, notices and retention controls
- Breach intimation workflows

Supplier Assurance

- Assessment of job-workers and tier-2 suppliers
- Contract security and notification clauses
- Supplier onboarding and recertification
- Joint supplier incident exercises

Buyer Questionnaire Readiness

- Mapping of brand security questionnaires to ISO 27001
- Evidence packs reusable across buyers
- Independent assessment reports for buyers
- ISO 27001 and PCI DSS readiness

Who we serve: spinning and weaving mills · processing and job-work units · garment and home textile exporters · footwear manufacturers · consumer products manufacturers · brand owners and licensees · D2C and e-commerce arms.

Packaged for how manufacturers and brands buy

Eleven Codec Networks bundles apply directly to textile, apparel and consumer manufacturing 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

Mills, job-workers and single factories

- IT and plant assessment
- Backup and recovery review
- Email security and BEC controls
- Policy pack and buyer questionnaire support

Assurance

Exporters and multi-unit manufacturers

- ERP, PLM and portal testing
- IP protection programme
- Annual independent audit
- 24x7 SOC

Continuous Resilience

Brand owners, listed groups and D2C businesses

- Continuous web, API and app testing
- Supplier assurance programme
- SOC with fraud and brand monitoring
- DPDP programme and Board reporting

Mapped to your obligations

Requirement	How we help	Bundle
Cyber incidents to CERT-In within six hours; 180-day logs	SOC, IR retainer and reporting support	B7, B8
Risk-based independent cyber audits (CERT-In guidelines 2025)	Independent IT and plant audits	B4, B1
Quarterly cyber incident disclosure by listed companies (SEBI)	Incident records, disclosure support	B4, B8
Consumer, loyalty, employee and worker personal data (DPDP)	DPDPA programme	B6
Brand vendor codes and security questionnaires (buyer contracts)	ISO 27001 and questionnaire readiness	B5, B9
Card payments on D2C sites and apps (PCI DSS v4.0.1)	PCI DSS readiness and testing	B5, B2
Connected consumer product security (EU CRA, from Sep 2026)	Product and firmware security assessment	B2, B11

Why manufacturers and brands choose Codec Networks

CERT-In empanelled

Independent audits recognised by regulators, buyers and partners.

Certified and accountable

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

Buyer-ready evidence

Findings and evidence packs mapped to brand questionnaires and ISO 27001.

Season-aware delivery

Testing and changes planned around sampling, shipment and sale calendars.

Full stack, one partner

Testing, SOC, forensics, privacy and supplier risk connected from finding to closure.

Certified experts

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

How we engage

Discover & scope

Factories and units, ERP, PLM and e-commerce platforms, buyers and their requirements, job-workers and suppliers, consumer data and your audit and shipment 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 buyer audit, season and incident a non-event.

Tell us your units, systems, buyers, suppliers and channels. We will propose a practical, season-aware 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: VF Corporation Form 8-K/A (2024), Hanesbrands Q2 2022 results, Ministry of Textiles, CERT-In. Confirm obligations against the official instruments.