

Codec Networks

Coding Threats. Decoding Solutions.

CLOUD, DATA CENTRES & HOSTING

Run the Cloud Others Trust. Prove It Every Day.

Cloud configuration reviews, virtualisation security, SOC, resilience and customer assurance for cloud, data centre and hosting providers

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 provider duties, MeitY empanelment and customer regulators



How Codec Networks helps

Services, bundles and packages built for the sector



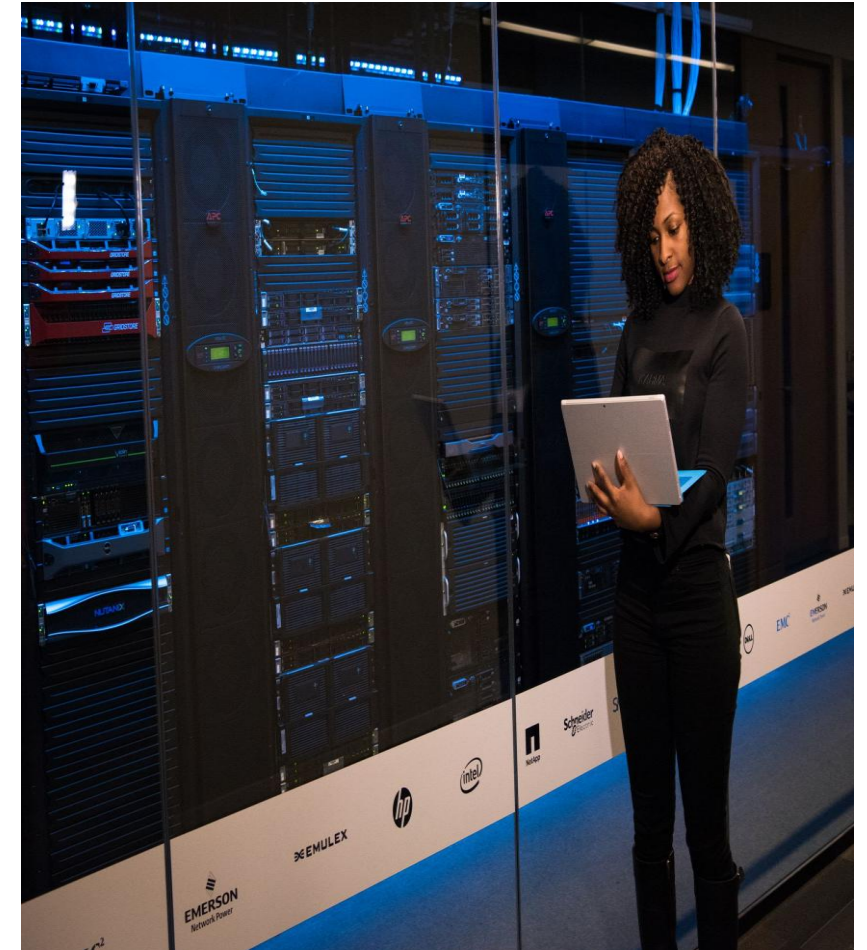
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Infrastructure providers carry specific duties

CERT-In names data centres, cloud and VPS providers directly

6 hours

To report cyber incidents to
CERT-In

5 years

Subscriber records kept by cloud
and VPS providers

180 days

ICT logs to be kept in India

May 2027

Most DPDP obligations take
effect

What this means: providers must protect shared hypervisors, control planes and facilities, keep subscriber records and logs as CERT-In requires, prove assurance to regulated customers and report incidents within six hours.

Sources: CERT-In Directions (28 April 2022), MeitY, SEBI, IRDAI.

Who we serve across cloud, data centres and hosting



Cloud service providers

IaaS and PaaS platforms



Colocation operators

Space, power and cooling



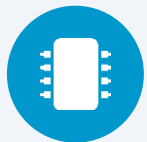
Managed hosting

Hosted and private cloud



VPS providers

Virtual and bare-metal servers



Edge and GPU clouds

AI and edge infrastructure



Sovereign and government cloud

Empanelled government platforms



Interconnection providers

Exchanges and cloud on-ramps



Backup and DR providers

Recovery services

The threats that cost infrastructure providers the most

Six priorities from our 18-threat cloud and hosting assessment



Hypervisor ransomware

Many customers down at once



Control-plane takeover

Consoles and APIs abused



Exposed out-of-band access

BMC and IPMI below the OS



Platform abuse

Criminal infrastructure on your servers



Facility OT compromise

Cooling and power as attack targets



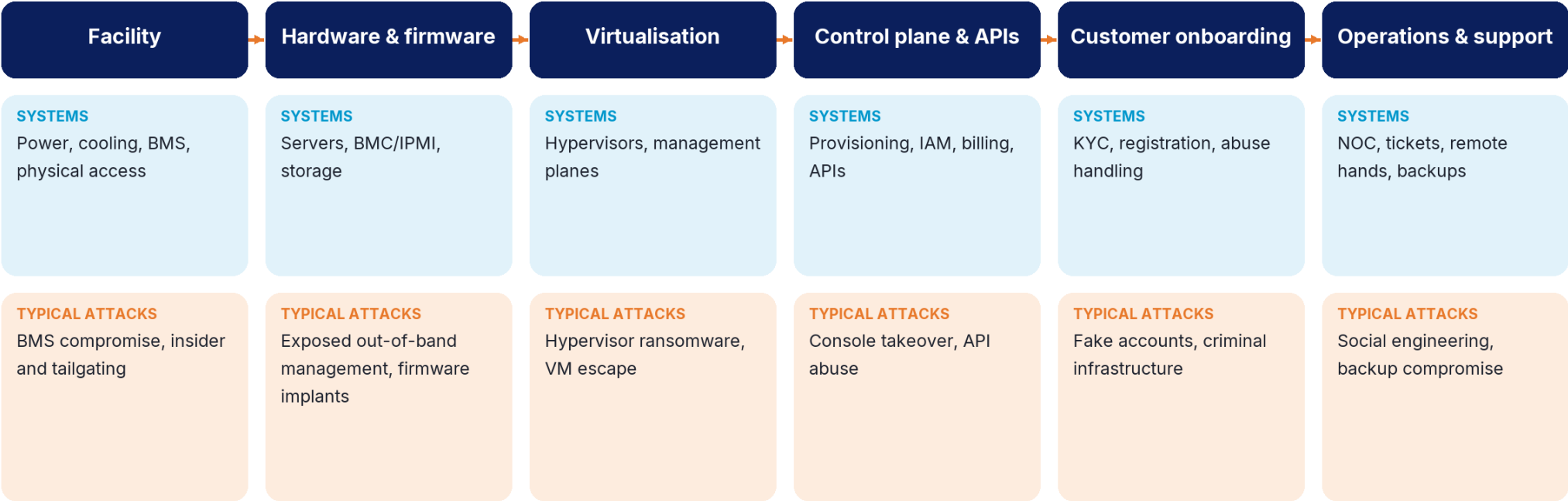
Slow detection & reporting

Missing the 6-hour window

Attacks target every layer from facility to console

Where Cyber Risk Sits in Cloud and Hosting Operations

Every layer from facility to customer console carries its own attack surface



Customers inherit the provider's facility, hypervisor and control-plane security—shared responsibility starts here.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In provider duties, MeitY empanelment and customer regulators

The rules that shape cloud and hosting security

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
Subscriber records (cloud, VPS, data centres)	5 years after cancellation	CERT-In Directions, 2022
Clock synchronisation	To NIC or NPL NTP servers	CERT-In Directions, 2022
Cloud services for government	Empanelment with STQC audit	MeitY
Cloud for SEBI-regulated customers	Per framework	SEBI cloud framework, 2023
Cloud for insurers	MeitY-empanelled, STQC audit status	IRDAI guidelines, 2026
Customer personal data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Key dates on the regulatory timeline

Regulatory Timeline Shaping Cloud and Data Centre Security

Cross-sector and customer-driven instruments

● In force ● Upcoming (from Oct 2026)

Apr 2022	●	CERT-In Directions: 6-hour reporting, 180-day logs, subscriber records for cloud and VPS providers
Sep 2022	●	CERT-In subscriber-registration requirements in force after extension
Mar 2023	●	SEBI framework for adoption of cloud services by regulated entities
Aug 2023	●	Digital Personal Data Protection Act, 2023 enacted
Nov 2025	●	DPDP Rules, 2025 notified with phased commencement
Apr 2026	●	IRDAI 2026 guidelines require MeitY-empanelled CSPs with STQC audit status
May 2027	●	Most DPDP Rules obligations, incl. breach intimation, take effect

Sources: CERT-In, MeitY, SEBI, IRDAI. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Cloud configuration · Virtualisation · SOC · Resilience · Assurance · Facility OT

One partner from facility to control plane



Cloud Configuration Reviews

Control plane, IAM, consoles, defaults



Virtualisation Security

Hypervisors, BMC, firmware, isolation



24/7 SOC

Platform, abuse, DDoS and OT monitoring



Resilience

Ransomware, DR and backup testing



Customer Assurance

ISO 27017/27018, SOC 2, empanelment



Facility OT Security

BMS, power, cooling, vendor access

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 hosting and VPS providers

- Control-plane VAPT (B1)
- Hypervisor and BMC review (B3)
- CERT-In record-keeping check (B4)
- ISO 27001 gap assessment (B5)

Assurance

Mid-sized clouds and colocation

- Virtualisation and isolation testing (B1, B3)
- Facility OT review (B3)
- ISO 27017/27018 and SOC 2 (B5)
- 24x7 managed SOC (B7)

Continuous Resilience

Large and sovereign cloud providers

- Red teaming and simulations (B1, B10)
- Empanelment and audit support (B4)
- SOC with platform signals (B7)
- Customer and Board reporting (B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Cyber incidents to CERT-In within six hours; 180-day logs (CERT-In Directions)	SOC monitoring, IR retainer and reporting support	B7, B8
Subscriber records for 5 years; clock synchronisation (CERT-In Directions)	Record-keeping and logging gap assessment	B4
MeitY cloud empanelment with STQC audit	Empanelment readiness and audit support	B4, B5
SEBI, RBI and IRDAI cloud requirements for customers	Customer assurance evidence and audits	B4, B5
Secure virtualisation and tenant isolation	Virtualisation and isolation testing	B1, B3
DPDP safeguards for customer personal data	DPDPA programme and data handling review	B6
Resilience and recovery commitments (SLAs)	DR, failover and ransomware simulations	B10

Five new case studies, five broken chains

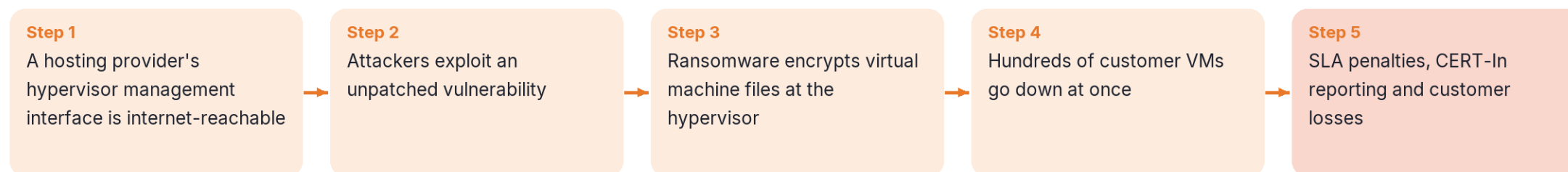
Illustrative composite scenarios written for 2026—not client engagements

1	The Hypervisor Ransomware Weekend	An exposed management interface lets ransomware hit every VM; isolation and backups limit it	B3 · B7 · B8
2	The VPS That Attacked a Bank	Fake-identity VPS hosts phishing; onboarding checks and records stop it	B4 · B7 · B2
3	The Out-of-Band Door Left Open	Exposed BMCs allow firmware tampering; isolated OOB networks prevent it	B1 · B3 · B7
4	The Snapshot That Went Public	A public-by-default share exposes data; secure defaults prevent it	B2 · B3 · B6
5	The Cooling System That Became a Cyber Incident	A compromised BMS overheats halls; OT segmentation prevents it	B3 · B7 · B10

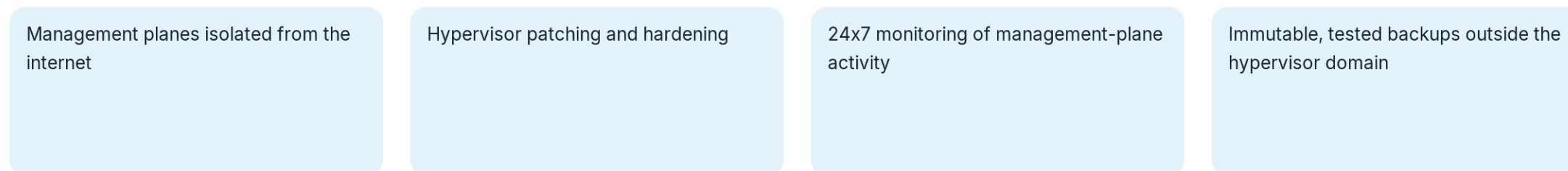
Example: breaking a hypervisor ransomware chain

Case 1: The Hypervisor Ransomware Weekend

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: internet exposure of management planes, hypervisor patch levels and hardening, monitoring of management-plane activity, and immutable backups outside the hypervisor domain, plus CERT-In and customer notification steps.

Why infrastructure providers 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 CERT-In, MeitY, customer regulator and DPDP requirements



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

Service model, facilities, virtualisation stack, customers 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.