



Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · SPACE, SATELLITE & GEOSPATIAL SERVICES

Secure the Ground. Protect Every Mission.

Ground infrastructure security, API and cloud testing, identity controls and supply chain assurance for satellite makers and operators, launch start-ups, ground station and teleport operators, satcom providers, earth observation and geospatial platforms and navigation vendors.

Ground Station Security

Satcom Networks

API & Cloud Testing

Identity & Access

Supply Chain Assurance

24/7 SOC

Coding Threats. Decoding Solutions.

www.codecnetworks.com

THE CHALLENGE

When space services are hacked, the damage lands on the ground.

India's space economy, valued at US\$8.4 billion in 2022, targets US\$44 billion by 2033, with about 440 space start-ups and 113 IN-SPACe authorisations by August 2026. ISRO reported over 100 cyber attacks a day in 2023, and the 2022 KA-SAT attack showed how one ground network breach can disable tens of thousands of terminals.

What keeps leadership teams awake

- Ground stations reachable from the internet
- Mission control and command keys misused
- Terminal firmware wiped by one bad update
- Geospatial APIs leaking customer imagery
- Untrusted components in the satellite bus
- Privileged access shared with vendors



US\$44 bn

Space economy target for 2033

~440

Space tech start-ups on the DPIIT portal

113

IN-SPACe authorisations to 52 private entities

6 hours

To report cyber incidents to CERT-In

The rulebook has changed

Instrument	What it means for you
Indian Space Policy 2023 and IN-SPACe NGP (2023–2024)	Authorisation of satellites, launch, ground stations and foreign satellite capacity by IN-SPACe
Telecom Act 2023 and Telecom Cyber Security Rules (2023–2024)	Satcom licensing, spectrum and security conditions; incident reporting by telecom entities
CERT-In Directions and audit guidelines (2022, 2025)	6-hour incident reporting, 180-day logs in India, risk-based independent audits including OT
Geospatial rules and DPDP Act (2021–2027)	Sensitive attribute rules for maps and data; safeguards and breach intimation for personal data

One partner from ground station to API

Built around our primary proposition for the sector: **ground infrastructure security, API and cloud testing, identity controls and supply chain assurance.**

Ground Station & Teleport Security

- Antenna, baseband and modem network tests
- Mission control and TT&C reviews
- Segmentation of ground networks
- Range and test facility OT reviews

Satcom Network Security

- Hub, NMS and gateway assessments
- Terminal firmware and update checks
- Management VPN and access reviews
- Licence security condition support

API & Cloud Testing

- EO tasking and delivery API testing
- Geospatial and location platform VAPT
- Cloud ground segment and GSaaS reviews
- Tenant isolation and abuse testing

Identity & Access Controls

- Privileged access for operators
- Command and key custody reviews
- MFA and vendor access brokering
- Joiner, mover and leaver checks

Supply Chain Assurance

- Component and software supplier reviews
- SBOM and software integrity checks
- Integrator and vendor access reviews
- Contract security clauses

24/7 SOC & Response

- Ground network and NMS monitoring
- Cloud, API and identity alerts
- 6-hour CERT-In reporting support
- Ground segment incident forensics

Who we serve: Satellite operators and manufacturers · launch service start-ups · ground station and teleport operators · satellite communications providers · earth observation and geospatial data platforms · navigation and location-solution vendors.

Packaged for how space and geospatial firms buy

Eleven Codec Networks bundles apply directly to satellite makers and operators, launch firms, ground station and satcom providers and geospatial platforms:

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

Space start-ups and geospatial platforms

- API and web platform test
- Cloud ground segment review
- Location data privacy check
- IR retainer

Assurance

Satellite operators and ground station firms

- Ground network VAPT
- Privileged access review
- CERT-In empanelled audit
- 24x7 managed SOC

Continuous Resilience

Satcom providers and large space groups

- Red team of ground and NMS
- Supply chain assurance
- ISO 27001 and telecom rules
- SOC with OT and NMS

Mapped to your obligations

Requirement	How we help	Bundle
Authorisation for space objects and ground systems (IN-SPACE NGP)	Authorisation security review	B4, B5
Licence security conditions for satcom services (DoT)	Gateway and network assessment	B1, B3
Incidents to CERT-In in six hours; 180-day logs (CERT-In)	SOC, IR retainer, reporting support	B7, B8
Risk-based independent audits incl. OT (CERT-In guidelines 2025)	CERT-In empanelled audit	B4
Sensitive attributes kept off maps (Geospatial Guidelines 2021)	Data handling and API review	B2, B6
Safeguards and breach intimation for location data (DPDP Act)	DPDPA programme	B6
Supplier and component assurance where contracts require it	Supply chain assessment	B9

Why space and geospatial businesses choose Codec Networks

CERT-In empanelled

Independent audits that customers, partners and CERT-In guidelines expect.

Ground to cloud

Antennas, mission control, satcom networks, cloud and APIs in one scope.

Safe, authorised testing

Agreed windows that never put live passes or services at risk.

Certified and accountable

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

Full stack, one partner

Testing, audit, SOC and forensics connected from finding to closure.

Certified experts

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

How we engage

Discover & scope

Ground stations, mission control and command keys, satcom hubs and terminals, cloud ground segment, EO and location APIs, privileged and vendor access, suppliers and the obligations that apply to you.

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 pass, launch and terminal update a non-event.

Tell us your satellites, ground stations, networks, platforms, data and obligations. We will propose a practical testing, audit and monitoring 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: IN-SPACe Decadal Vision and PIB (October 2024), Lok Sabha reply on space start-ups (August 2026), CERT-In Directions (2022). Confirm obligations against the official instruments.