

Codec Networks

Coding Threats. Decoding Solutions.

AUTOMOTIVE & MOBILITY

Secure the Plant. Secure the Car.

Vehicle network testing, embedded and OTA security, plant OT security and charging API and cloud security for automotive and mobility companies

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

AIS 189/190, CERT-In, SEBI, DPDP and the global OEM rules



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 automotive stop plants, dealers and cars

Recent incidents show the operational and financial stakes

5 weeks

JLR production halted by a cyberattack (2025)

£1.9 bn

Estimated UK economic cost of the JLR attack (CMC)

15,000

Dealerships disrupted by the CDK Global attack (2024)

6 hours

To report cyber incidents to CERT-In

What this means: automotive companies must separate plants from corporate IT, secure the apps, APIs and OTA pipelines that reach vehicles, control suppliers, dealers and vendors, protect customer and vehicle data, monitor around the clock and prepare for AIS 189 and AIS 190.

Sources: Cyber Monitoring Centre (UK), public reporting on JLR and CDK Global, CERT-In, MoRTH.

Who we serve across automotive and mobility



Vehicle OEMs

Passenger, commercial, two- and three-wheelers



Component suppliers

Tier-1 and tier-2, electronics, castings



EV and battery makers

EV platforms, cells, packs, BMS



Charging networks

CPOs, OCPP backends, chargers



Dealers and distribution

DMS, finance, service, registration



Mobility platforms

Ride-hailing, leasing, subscriptions



Fleet and telematics

Fleet tech, logistics, public transport



Engineering services

Automotive ER&D and software partners

The threats that cost automotive companies the most

Six priorities from our 18-threat automotive assessment



Ransomware shutdowns

Plants, suppliers and dealers stopped



Supplier and platform outages

One partner's incident stops you



Remote vehicle access

Apps and APIs reaching the car



OTA and software supply chain

Tampered updates and pipelines



Charging and payment attacks

OCPP backends and card data



Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from design to the road

Where Cyber Risk Sits Across the Automotive Value Chain

Every stage from design to the road carries its own attack surface



In automotive, one weak link—a supplier, a dealer platform or an app API—can stop production or reach the car on the road.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

AIS 189/190, CERT-In, SEBI, DPDP and the global OEM rules

The rules and standards shaping automotive cybersecurity

Requirement	Frequency / deadline	Source
Vehicle cyber security management system	Type approval; phased from Oct 2026 (draft)	AIS 189 under CMVR; UN R155
Software update management system	Type approval; phased (draft)	AIS 190 under CMVR; UN R156
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
Independent cyber audits	Risk-based, incl. OT	CERT-In audit guidelines, 2025
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023
Customer, vehicle and driver data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Supplier information security	Per OEM contract	TISAX (VDA ISA); ISO/SAE 21434
Connected product security in the EU	Reporting from Sep 2026; full from Dec 2027	EU Cyber Resilience Act

Key dates on the regulatory timeline

Regulatory and Standards Timeline Shaping Automotive Cybersecurity

Indian instruments, vehicle standards and the global rules that reach Indian OEMs and suppliers

● In force

● Upcoming (from Oct 2026)

2000	● Information Technology Act, 2000 enacted; CERT-In and CII provisions added in 2008
2021	● UN Regulations R155 (cyber security) and R156 (software updates) take effect for new types in adopting markets
May 2021	● PLI for Advanced Chemistry Cell batteries approved (₹18,100 crore)
Sep 2021	● PLI for automobiles and auto components approved (₹25,938 crore)
Apr 2022	● CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Jul 2023	● SEBI LODR amendment: listed companies disclose cyber incidents quarterly
Aug 2023	● Digital Personal Data Protection Act, 2023 enacted
Sep 2024	● PM E-DRIVE scheme notified (₹10,900 crore) for EV adoption and charging
Dec 2024	● EU Cyber Resilience Act enters into force for products with digital elements
Jul 2025	● CERT-In Comprehensive Cyber Security Audit Policy Guidelines
Nov 2025	● DPDP Rules, 2025 notified with phased commencement
Jun 2026	● MoRTH draft notification to make AIS 189 (CSMS) and AIS 190 (SUMS) mandatory under CMVR in phases
Oct 2026	● Proposed first AIS 189/190 compliance date for new Level 3+ automated vehicle models
May 2027	● Most DPDP Rules obligations, incl. breach intimation, take effect
Dec 2027	● EU CRA essential requirements and CE marking fully apply

Sources: MoRTH, MHI, CERT-In, SEBI, MeitY, UNECE, EU Official Journal. AIS 189/190 dates are from the draft notification; confirm the final gazette.

Codec Networks

How Codec Networks helps

Vehicle · OTA · Plant OT · Charging · Suppliers and dealers · IT/OT SOC

One partner from plant floor to the road



Vehicle Network Testing

ECUs, CAN/Ethernet, telematics, TARA



Embedded & OTA Security

Firmware, secure boot, OTA pipeline



Plant OT Security

IEC 62443, segmentation, resilience



Charging API & Cloud

CPO backends, OCPP, apps, payments



Supplier & Dealer Risk

Tier-n suppliers, DMS, TISAX



24/7 IT/OT SOC

Plant, enterprise and vehicle cloud

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

Suppliers, dealers and charging start-ups

- IT and plant/backend assessment (B1)
- Backup and remote access review (B3)
- TISAX or OEM questionnaire readiness (B5)
- Policy and privacy pack (B5, B6)

Assurance

EV makers, charging networks and mid-sized suppliers

- Vehicle, charger or product testing (B1, B2)
- Plant segmentation and OT review (B3)
- Annual independent audit (B4)
- 24x7 IT/OT SOC (B7)

Continuous Resilience

OEMs, tier-1 majors and fleet platforms

- AIS 189/190 CSMS and SUMS programme (B4, B5)
- Continuous app, API and OTA testing (B2)
- Supplier and dealer risk programme (B9)
- SOC with vehicle-cloud monitoring (B7)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Vehicle cyber security and software update management for type approval (AIS 189/190, draft CMVR rules)	CSMS/SUMS readiness, TARA, vehicle and OTA testing	B4, B1, B2
Cyber incidents to CERT-In within six hours; 180-day logs (CERT-In Directions)	IT/OT SOC, IR retainer and reporting support	B7, B8
Risk-based independent cyber audits including OT (CERT-In audit guidelines, 2025)	Independent IT/OT audits	B4, B1
Quarterly cyber incident disclosure by listed companies (SEBI LODR)	Incident records and disclosure support	B4, B8
Customer, vehicle, driver and dealer personal data (DPDP)	DPDPA programme	B6
Global OEM, UN R155/R156, TISAX and EU CRA requirements	ISO/SAE 21434, TISAX and CRA readiness	B5, B9, B11
Card payments at chargers and dealers (PCI DSS)	Payment security review	B2, B5

Five new case studies, five broken chains

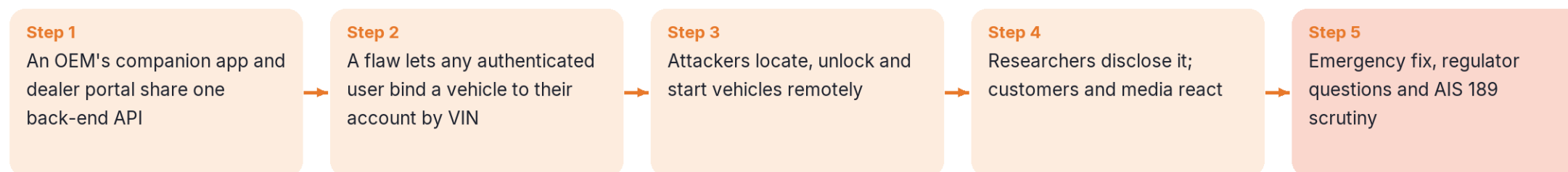
Illustrative composite scenarios written for 2026—not client engagements

1	The Five-Week Shutdown	Ransomware via a supplier's credentials stops every plant; segmentation and tested restarts prevent it	B3 · B7 · B10
2	The Dealer Platform That Went Dark	A DMS provider's incident puts dealers on paper; SaaS assurance and playbooks limit it	B9 · B2 · B10
3	The App That Unlocked Any Car	An API flaw lets attackers control vehicles by VIN; API testing and monitoring stop it	B2 · B11 · B7
4	The Charging Network Held to Ransom	A weak OCPP backend takes chargers offline; hardening and monitoring prevent it	B1 · B3 · B7
5	The Fleet That Drove Blind	A leaked API key exposes fleet data and immobilisers; cloud security and DPDP controls stop it	B2 · B6 · B7

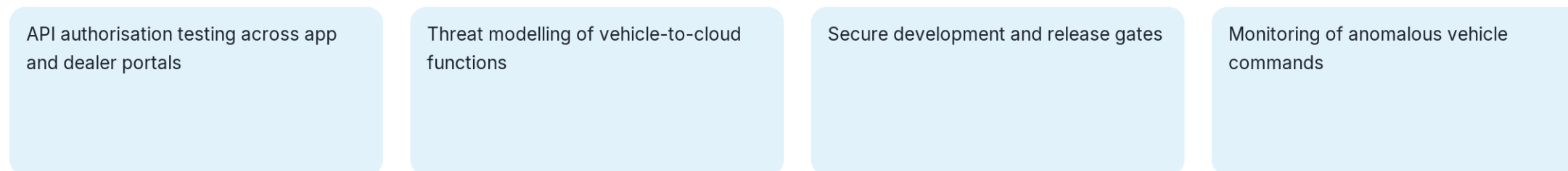
Example: breaking an app-to-vehicle attack chain

Case 3: The App That Unlocked Any Car

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: authorisation across companion apps, dealer portals and shared back-end APIs, vehicle binding and ownership transfer flows, rate limits and anomaly detection on vehicle commands, secure development and release gates, and incident response for a vehicle-affecting vulnerability.

Why automotive companies 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 AIS 189/190, ISO/SAE 21434, IEC 62443, TISAX, CERT-In expectations and your OEM customers' 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

Vehicles and ECUs, apps and APIs, OTA pipeline, plants, chargers, DMS and telematics platforms, suppliers and your homologation 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.