



AUTOMOTIVE

Cybersecurity Services for Connected & Autonomous Vehicles

Securing vehicles across their full lifecycle: compliance, engineering and operations



Compliance

- ✓ ISO/SAE 21434 implementation
- ✓ UNECE R155/R156 (CSMS Support)
- ✓ EU Cyber Resilience Act (CRA) readiness
- ✓ CSMS/ ISMS definition & audits
- ✓ Training & process deployment



"We support you at
homologation and regulation"



Engineering

- ✓ TARA (Threat Analysis and Risk Assessment)
- ✓ Secure-by-Design & Secure Coding
- ✓ Code Reviews & security audits
- ✓ Security Testing (pentesting, buzzing, vulnerability analysis)



"We help to build
secure products"

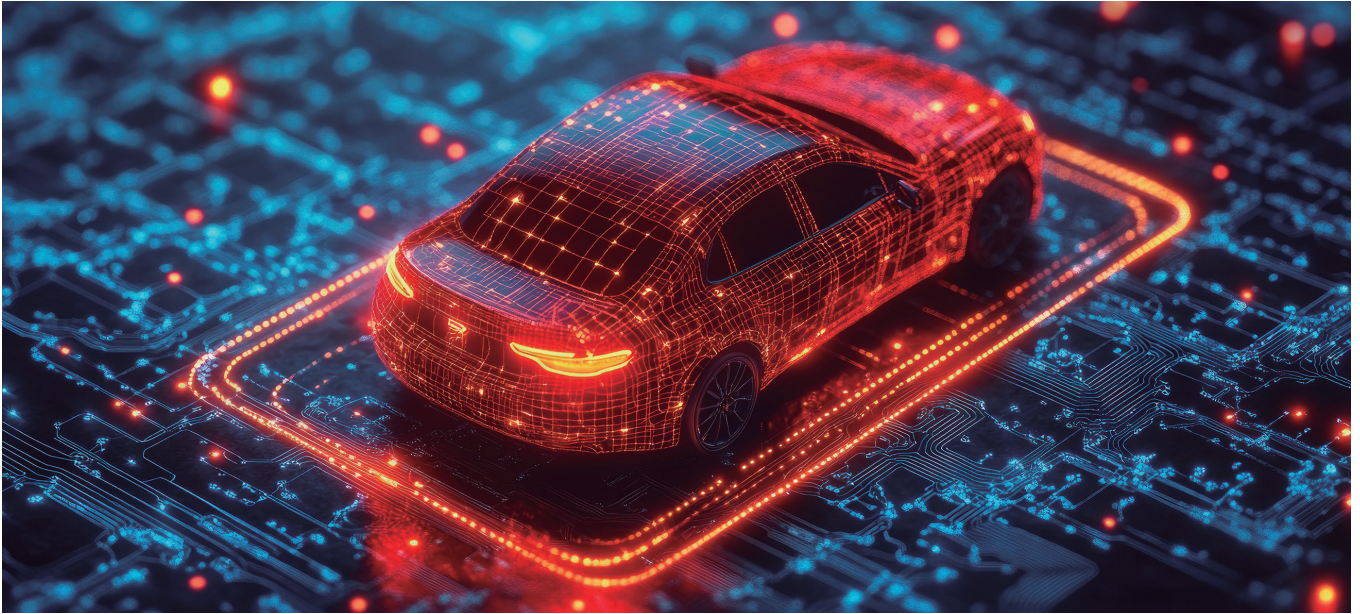


Operations

- ✓ PSOC (Product Security Operations Center)
- ✓ Vulnerability Management (lifecycle)
- ✓ Incident response & forensic analysis
- ✓ Threat Intelligence (incl. dark web monitoring)
- ✓ Continuous compliance (R155 + CRA)



"We support you during
the full life-cycle"



GMV Laboratory

- Complete technical audits, fuzzing and intrusion testing.
- Wireless network and in-vehicle communication attack-surface analysis.
- Ethical hacking: reverse engineering, tampering, forensic analysis.
- Scope: ECUs, ZCUs, gateways, HPCs, full vehicle, E2E platform and apps.

Trusted across the industry

- 20+ years working with OEMs and Tier 1 suppliers on connected-vehicle applications.
- 24/7 vulnerability management and incident response via GMV-CERT (cert.gmv.com).
- Automotive-specific certifications and quality standards.



GMV CYBERSECURITY DIFFERENTIATORS

Cross domain expertise | Experience in regulated environments | Hands-on experience at secure software development and penetration testing.