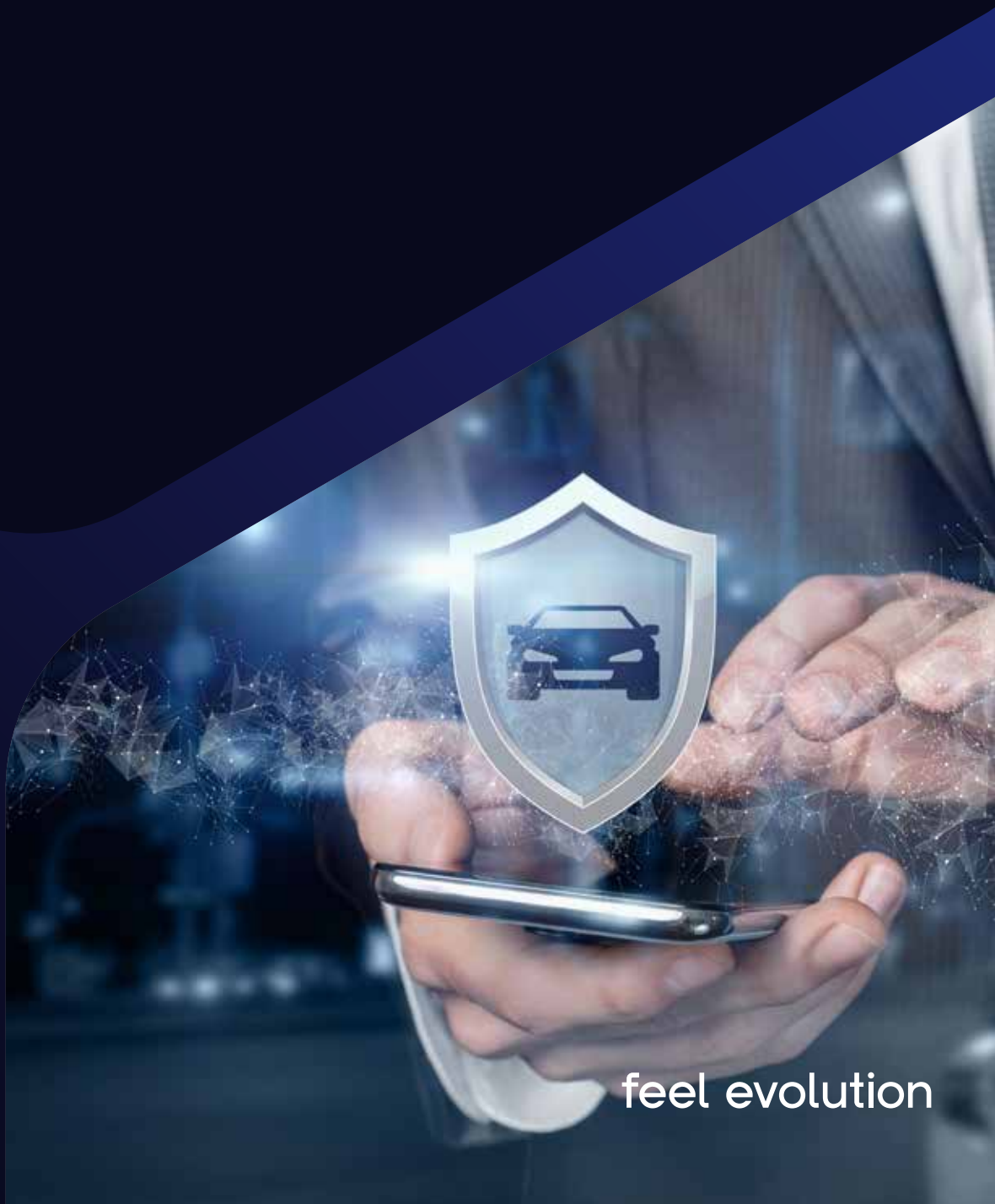
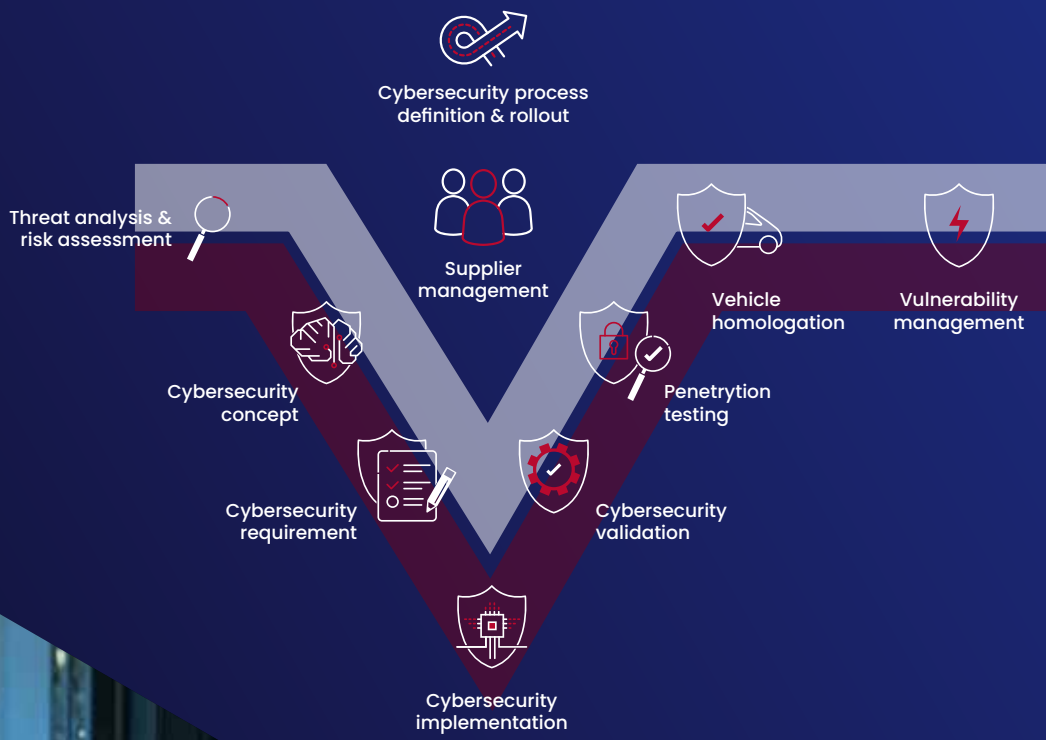
FEV.io

Cybersecurity solutions

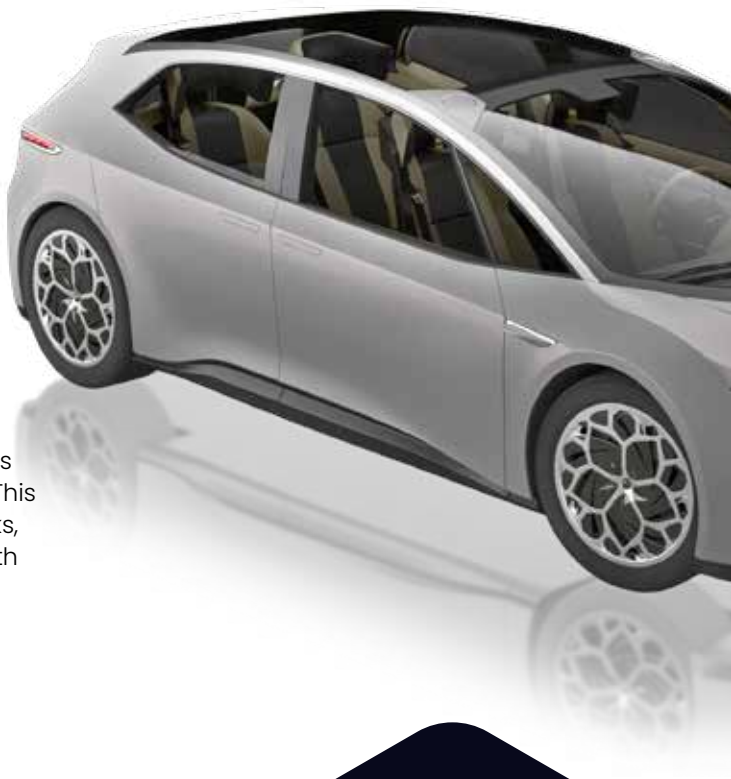


feel evolution

FEV Cybersecurity Services stands at the forefront of smart car cybersecurity. Our V Cycle approach encompasses every stage of cybersecurity development – from initial design to final deployment and homologation. We specialize in creating tailor-made solutions that address the unique challenges of the smart car market. Our team of experts employs the latest technologies and methodologies to ensure your smart car products are not just innovative but also secure against evolving cyber threats.



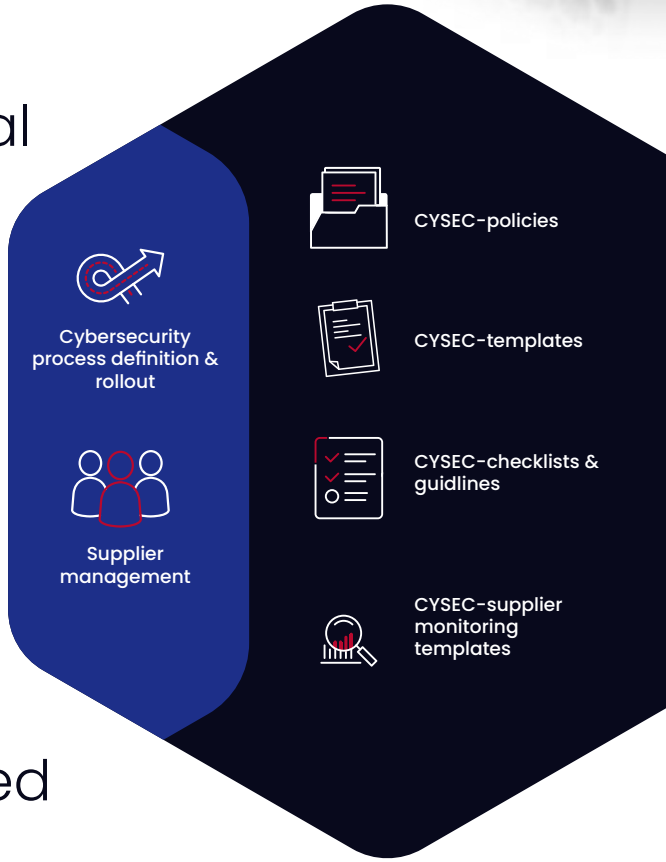
Connected vehicle infrastructure security



Our expertise extends beyond basic cybersecurity measures to encompass the entire connected vehicle infrastructure. This includes robust protection for in-vehicle systems, IT networks, cloud-based services, and mobile applications. Our in-depth experience ensures a multi-layered security strategy, safeguarding every aspect of connected vehicle technology against cyber threats and unauthorized access.

Process definition and global standards compliance

Our cybersecurity process definition and rollout are grounded in adherence to global standards like R155. We provide detailed process documents, templates, checklists, and guidelines, all compliant with international regulations. Our approach includes state-of-the-art supplier monitoring and management, ensuring that every aspect of your supply chain meets the highest cybersecurity standards.

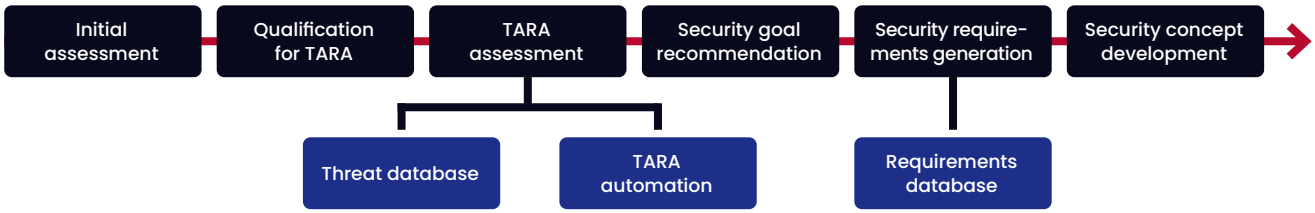


Advance threat identification with automated TARA methodology

FEV automated TARA methodology revolutionizes threat identification and risk analysis. This advanced, autonomous system minimizes the need for manual effort, employing sophisticated algorithms to automatically detect and analyze potential cyber threats.

Benefits

1. Improved efficiency
2. Consistency and accuracy
3. Enhanced coverage
4. Proactive risk management
5. Data-driven decision making
6. Cost effective
7. Scalability
8. Continuous monitoring and updates

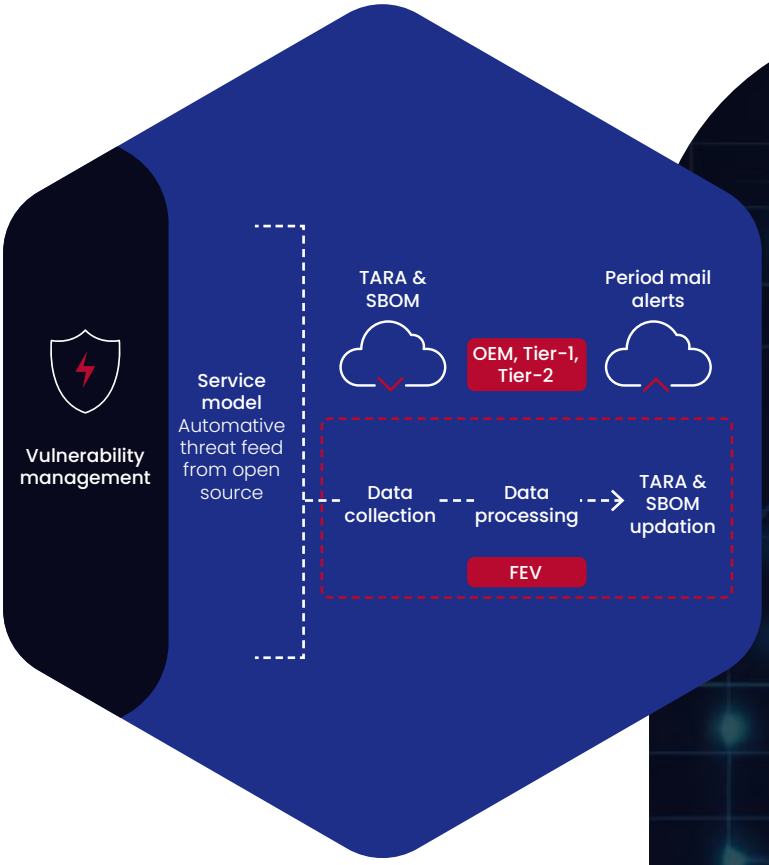


Expertise in cybersecurity requirements and Control

Our vehicle domain knowledge helps to bring out precise cybersecurity requirements for connectivity, powertrain, body, chassis, ADAS functions. This helps to improve security as well as safety of these sub systems on connected vehicle.

Continuous monitoring and incident response

Our services include ongoing monitoring, vulnerability management, and a rapid incident response mechanism. Our state-of-the-art Vehicle Security Operations Center (VSOC) and comprehensive incident response playbooks ensure that we are always prepared to respond to and mitigate any cybersecurity incidents, maintaining the integrity and security of your systems at all times.



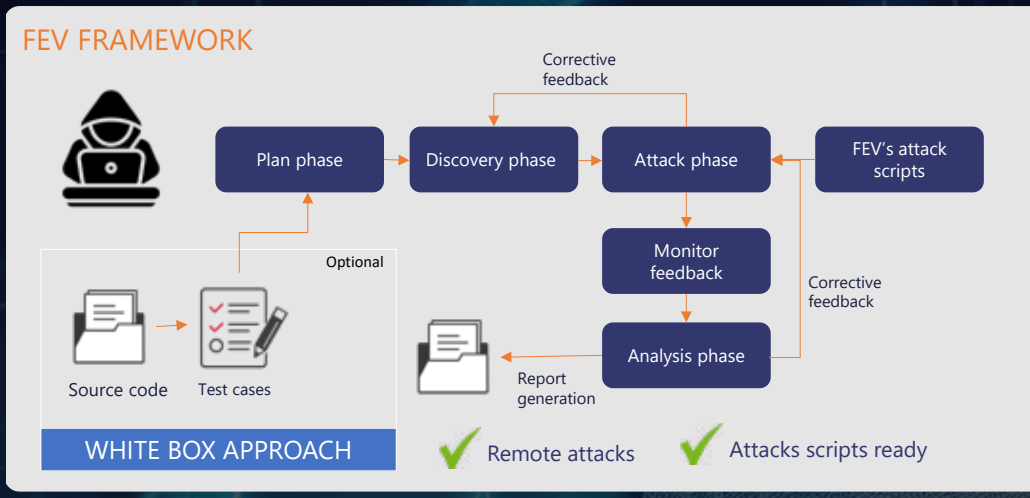
FEV PEN test LAB

PEN test LAB capable to execute all advance HW/wireless attacks

- Side channel analysis and exploit secure debug port
- Fault injection and steal ECU proprietary information
- Designed custom HW for SCA and fault injection
- Custom HW designed for radio frequency transmission devices
- Firmware extraction and malware injection
- PCB reversing and hardware manipulation
- LAB infrastructure designed for advance HW attacks

Specialized HW (custom made) and experienced professional to Execute HW Attacks

Penetration testing



FEV follows both white and black box approach for penetration testing

Offerings	Penetration testing
1 Penetration testing (white, grey and black box)	Automotive (4-W, 2-W, ECU's), medical, industrial, IOT, OT devices
2 Penetration testing: app and Cloud	Connected cloud and eco system, infrastructure Mobile app, smart apps

Vehicle level

FEV covers all interfaces at vehicle Llevel such as wireless, local I/O, software components

Wireless component
Long radio
- LTE/UMTS/GSM (cellular)

Short radio
- Keyless lock/unlock (RF/LF)
- Bluetooth (4.2/5.0/5.1) , NFC
- Wifi (WPA/WPA2)/ wifi-AP
- Sensors/camera

Ecosystem interfaces/ chargers
- Vehicle to vehicle/ app's
- Wireless charger
- Vehicle charging point
- Vehicle to cloud interface

Cockpit (head unit and telematics)
Software components
- Web browser
- Third tarty apps
- Connected car services (app)
- Android auto/car play

GPS Navigator

USB

Local I/O
In-vehicle network
- CAN/CAN-FD
- Diagnostics (UDS)
- Ethernet
- OBD-II

Hardware, component, device level

FEV covers hardware attacks, binary reversing and all interfaces associated with devices

Hardware attacks
Attack on debug interfaces
- Bypassing JTAG/ SWD locks
- UART/SPI/I2C
- Firmware extraction through UART/SPI/ from IC

Side channel and fault injection
- Clock glitching
- Voltage glitching

Reverse engineering
- Binary analysis
- Reversing protocol (UART/SPI/I2C/IVN)
- PCB reversing

Software
- OS: Linux, RTOS, BareMetal
- Architecture: AUTOSAR, NON-AUTOSAR

Local I/O
- In-vehicle network: CAN/CAN-FD, ethernet, OBD-II, diagnostics (UDS)
- USB

Wireless Component
- Wifi (WPA/WPA2)/ Wifi-AP
- Bluetooth, NFC
- Zigbee
- LF/RF

Regional offices India

Technical center
Pune, A-21, Talegaon MIDC
Pune Maharashtra 410507
P +91-2114 666 000
marketing-india@fev.com

Smart mobility center
Survey 2, Hissa No 7/1, Baner
Pune Maharashtra 411045

Software center
9th floor
IIT Madras Research Park
Kanagam road, Taramani
Chennai, 600113

Vehicle development center
H Block, Plot no, C-181
MIDC, Chinchwad,
Pune Maharashtra 411019

Software center
350 Ramprika Tower
Himmat Nagar, Tonk Road
Jaipur, Rajasthan 302018

Project office
1117, Logix office tower
Sector-32
Noida, Uttar Pradesh 201301

Headquarter FEV Europe

FEV Group GmbH
Neuenhofstraße 181
52078 Aachen · Germany
P +49 241 56890

Follow us on social media

www.fev.io