Luxoft
A DXC Technology Company

A Luxoft factsheet

Automotive Cybersecurity

Luxoft's Automotive Cybersecurity offering is a complete solution for automotive cybersecurity protection. Our robust service covers threat analysis, risk assessment, security engineering, vulnerability management and incident response support using the latest technologies. It also includes cybersecurity-specific testing activities such as penetration testing and fuzz testing. Our Cybersecurity Management System (CSMS) is certified by TÜV SUD and built using our automotive Cybersecurity experts who are certified by TÜV SUD and TÜV NORD. We can support automakers and their key partners with regulatory compliance, obtaining type approvals, and conducting audits and assessments that adhere to ISO 21443 and UNECE R155/R156.

The challenge

The software-defined vehicle has become a technology platform on wheels. As such, they feature a growing number of complex and integrated automotive systems that can be exposed to cyberattacks. These vulnerabilities present the risk of vehicle theft and malicious acts that can compromise critical safety functions and brand image. They can also reveal opportunities for hackers to unlock billable digital features and clone ECUs for financial gain. This means OEMs and Tier 1s require state-of-the-art security solutions and comprehensive testing abilities to mitigate these threats.

We help with critical challenges that include:

- Responding to emerging cyberattacks growing in complexity and posing increasing risks to vehicle security.
- Creating customized automotive cybersecurity solutions that can meet the specific requirements of your vehicle platform.
- Identifying cybersecurity vulnerabilities across vehicle components and systems, including hardware, firmware, wireless attack vectors, and wired vehicle networks.
- Support to obtain Vehicle Type Approval and make it easier to meet the requirements demanded of all vehicles produced from July 2024 onward.

Our solution

We ensure OEMs and Tier 1s can navigate the specific industry compliance and regulatory requirements while mitigating against escalating hacking threats. Through this service, we help stakeholders understand the severity and implications of cybersecurity vulnerabilities and remediate them – to protect your vehicles, customers, and brand reputation. Supported by our cybersecurity testing lab, we provide you with comprehensive testing and assessment of the security posture of vehicles on all levels, covering hardware, software, and communication networks.

Why work with us?

Benefits

- A proactive approach to identifying and mitigating cyber threats with complete automotive cybersecurity protection that covers all automotive domains.
- Assured compliance with industry standards and regulations, with support to grant Vehicle Type Approval.
- Meet compliance and standards faster and more efficiently by drawing on our preconfigured skills, certifications, and competency.
- Design and build the architecture for cybersecurity concepts and solutions that align with the specific needs of your vehicle platform.
- Enhance reputation and trust with a commitment to cybersecurity, using comprehensive testing to minimize the risk of potential threats and eliminate weaknesses in product design.

What makes us different?

- We leverage our deep industry knowledge to navigate your challenges and the regulatory landscape of the automotive sector.
- Our end-to-end understanding of every stage of automotive software development and validation, combined with specialist automotive cybersecurity skills and knowledge.
- Our Cybersecurity Management System (CSMS) is certified by TÜV SUD and is built by our automotive Cybersecurity experts who are certified by TÜV SUD and TUV NORD. We're compliant with the relevant industry standards and regulations, including UNECE R155 and R156 and ISO 21434.
- Our penetration test engineers have extensive background in automotive, with access to our advanced testing laboratories.
- We offer high scalability, global support, and localization capabilities for fast speed-to-market.

Our customers

The Challenge

A Tier 1 supplier had overlooked incorporating cybersecurity at the beginning of a development project and had challenges obtaining Type Approvals. With the end of the project approaching, the company needed to establish how secure it was.
After the OEM performed penetration testing, a large number of security vulnerabilities were identified.
The organization needed the support of an automotive cybersecurity partner to address these challenges.

The Solution

We performed cybersecurity management and engineering, in compliance with ISO 21434 and UNECE R155 CSMS regulations. We defined the development activities and participated in the cybersecurity development and testing activities.

The Results

After executing the test cases raised by the OEM's penetration testing, we helped ensure that our customer met the relevant cybersecurity requirements and was able to overcome their complex challenge.

For more information contact:

Khaled Naga
khaled.naga@dxc.com

Global Automotive
Cybersecurity Manager