IoT Automotive Cybersecurity

Cybersecurity in the IoT Automotive sector is one paramount. In this industry, cyber-attacks could have immediate implications on safety! Latest studies have shown that 37% of consumers would switch car brands to achieve improvements in autonomous driving and connectivity.

CHALLENGES

Security, physical safety and privacy concerns:
Hackers could potentially take control of safety-critical aspects of a vehicle's operation.
Personally-identifiable information could be stolen and breach consumer's privacy rights.

Increased varied technologies:
The number of sensors per vehicle has rapidly increased, which in turn, creates a higher number of entry points for potential cyber attacks.

Certification:
It is hard for consumers to evaluate whether a component is secure against cyber attacks.
A higher level of consumer trust could be gained through union – wide certification.
Different security standards may be applied to assess the security of IoT devices.

OPPORTUNITIES

65% of recent and intending car buyers have one or more connected car features in their current car

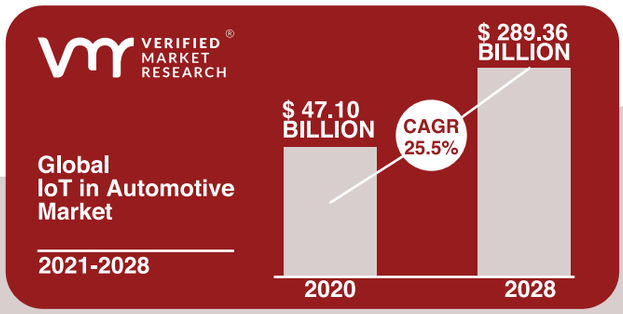
54% are concerned about data security and how their data might be used

19% of respondents have said that data privacy and data management concerns could prevent them from buying a connected car in future

25.5% IoT in Automotive Market size is projected to grow at a CAGR of 25.5% from 2021 to 2028

$47B IoT in Automotive Industry has been valued at USD 47.10 Billion in 2020

$289B IoT in Automotive Market size is projected to reach USD 289.36 Billion by 2028



HOW CAN *RED ALERT LABS* HELP YOU HAVE A MORE SECURE JOURNEY ?

We can train you

- By providing Cybersecurity trainings for Automotive IoT manufacturers, subjects as current market situation, incidents, threats and risks, regulation, standards and best practices are covered
- E.g. :Common Criteria for automotive applications and available protection profiles

We can support you

- To meet standards that you need
- During the full process of designing secure IoT components

We can evaluate your product security

- Through risk and cybersecurity threats analysis
- Through gap assessment and design reviews
- Through customized security assessment and penetration test campaigns for automotive components

We can accompany you in the certification process

- By assisting you in obtaining the certification you are targeting
- By providing a conformity assessment program for Automotive IoT, ensuring minimum risk exposure

WE MASTER *STANDARDS & REGULATIONS* THAT IMPACT YOUR INDUSTRY

- SPY Act (USA)
- UNECE WP.29
- BSI PAS 1885 (UK)
- C2C: Standards for V2X communication requiring Common Criteria
- ETSI ITS test specifications for V2X communications (103 096, 103 525 and 103 600 series)
- CCC: Standards for consumer device link to automotive
- ISO 16845 – Road vehicles — Controller area network (CAN) conformance test plan
- ISO 26262 – Road vehicles — Functional safety
- ISO/SAE 21434 – Road vehicles — cyber security engineering
- ISO 21448 — Road Vehicles — Safety of the Intended Functionality
- SAE J3101 – Hardware-Protected Security for Ground Vehicle Applications
- SAE J3061 – Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- 3GPP TS 33.536 Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services
- TISAX – Trusted Information Security Assessment Exchange
- IATF 16949 – Automotive Quality Management Systems

contact@redalertlabs.com
www.redalertlabs.com
Red Alert Labs
@RedAlertLabs
Aflortville (Paris Area) 94140, France

RED ALERT LABS
IoT Security