AI is reshaping the automotive world, but demands the most effective security possible

Picture credit: AdobeStock

DRIVING FORWARD

Device Authority *outlines its vital security principles for the automotive industry*

Vehicles are fast becoming mobile computers communicating automatically with myriad external devices and services to deliver massive gains in efficiency, safety and consumer experience. But the cyber security threats are significant and constantly evolving. In mid-May, Device Authority was joined by distinguished speakers from its partners such as Microsoft, CyberArk, Entrust, Argus Cyber Security, PTC and Cumulocity for its summit in which connected cars was one of the main topics of talks and discussions. The consensus of experts from the event was that the following points are priorities

Compliance: vehicle security must comply with the mandatory United Nations Economic Commission for Europe (UNECE) WP.29 regulation and best practice standard ISO21434. These measures require threat analysis, and cover risk management and response, supply chains, post-production and life cycle security.

Vehicles must be secure by design, from factory to crusher: a holistic approach throughout the 15-20-year life cycle of each vehicle is required, covering every aspect of security – from design and development to production and operation.

The need for collaborative innovation: collaboration between innovators is necessary to create next-generation solutions for automotive cyber security. From global companies to smaller organisations with specialised expertise, a pooling of talent and insight is what will keep vehicles secure. With scaled quantum computers on the horizon, the automotive industry must prepare for the world of post-quantum cryptography. Innovation will be utterly essential to secure devices, applications and their data, using accurate inventories, crypto-agility and new technologies to automate processes.

Embed end-to-end security from the car to the cloud: security must cover the connected car's entire data ecosystem seamlessly. This requires successful integration of cyber security solutions. Perfectly-interlocking protection should extend to the cloud including the Vehicle Security Operation Centre (VSOC) and vehicle-to-cloud (V2C) communications.

Comprehensive threat detection: real-time monitoring, threat-detection and analysis is necessary to provide insights that power incident response automation. A good example is the implementation of Azure OpenAI Copilot to detect threats with a high level of accuracy, reducing response times and human involvement.

360° security visibility: organisations need to ensure that monitoring of connected vehicle security is comprehensive, using data connectors where necessary to encompass the cloud, VSOC and all applications used. This includes understanding the converging of IT and OT worlds which introduces new entry points for potential threats across connected cars, manufacturing floors, back-end services, and car dealerships.

Life cycle management tools: on-the-road security and compliance demand a full suite of solutions to manage requirements such as the US Software Bill of Materials. An intrusion detection and prevention system and solutions such as Microsoft Security Copilot to put the capabilities of AI into the hands of defenders. Given the complexity of the life cycle of a car, it's critical to introduce security from the start. Implementing a device twin can support and ultimately shorten the development cycle by automating and introducing new techniques or processes.

Agile and secure development cycles: the automotive industry is witnessing a shift towards new business models such as subscription and service-based, where cars can be upgraded with new features at any point. This evolution requires faster development cycles to meet regulatory requirements and the increasing complexity of vehicles. This push for quicker, higher-quality, and more secure development is now a major global issue for car manufacturers.

Consolidation is key: organisations are increasingly looking to consolidate security capabilities. It is estimated that, on average, there can be up to 70 different vendors needed to cover all aspects of security. By integrating and consolidating these solutions, CISOs can improve risk posture significantly. Tightly-connected and integrated solutions provide a major benefit, making the overall solution more secure and encompassing the entire ecosystem end-to-end ●