End-to-End Vehicle Security from NTT DATA and Swimlane

Introduction

The automotive industry is rapidly modernizing, driven by the latest innovations in connected and software-defined vehicles. This interconnectedness also means vehicle systems are increasingly vulnerable to internet attacks. Due to the complexity of autonomous vehicles, strict safety regulations, and numerous variants, it can take weeks or even months to roll out security updates. That kind of delay almost guarantees damage from an attack. That's why responding quickly and effectively to security incidents isn't just important but also essential to minimize financial, resource, and reputational harm.

To address this critical need, Swimlane and NTT DATA collaborated to develop a customized automation solution for a leading Premium OEM. This case study tells the story of the NTT DATA-built solution for autonomous vehicle security powered by the Swimlane Turbine AI automation platform.

CYBERSECURITY CHALLENGES

Complex real-time detection and response

Real-time detection and response to in-vehicle cyber threats are absolutely critical, yet they often prove to be immensely complex. This difficulty stems from fragmented security systems and the rapidly evolving methods used by attackers. Such complexity directly increases an organization's risk exposure, making it challenging for traditional security operations to effectively manage and mitigate threats.

Slow response threatens vehicle safety

Standard incident response plans are essential for vehicle fleets; however, implementing them in the automotive industry presents significant challenges. Car security updates are highly complex and intricately tied to strict safety rules and legal requirements. This means rolling out a fix can take weeks or even months. That slow timeline clashes dramatically with the urgent need to respond to a cyberattack in just minutes or hours to prevent widespread damage. This big difference creates a real dilemma. To close this critical gap, a new approach introduces the idea of response levels: immediate (Level 1) and intermediate (Level 2). These levels focus on quick actions, such as containing attacks or temporarily isolating affected services. They're vital for speeding up responses while keeping vehicles safe and stable, offering a proactive way to counter evolving threats, unlike slower, traditional vulnerability fixes.

Data overload delays threat detection

Connected vehicles generate massive amounts of real-time cybersecurity data, which can easily overwhelm traditional security teams. The sheer volume clogs systems, significantly delaying threat detection and response. Furthermore, strict data protection rules, such as GDPR, require the real-time anonymization of vehicle data. This makes transferring and processing it even more complicated before analysis.

In-vehicle networks are vulnerable

Automotive communication protocols, such as Controller Area Network (CAN), Local Interconnect Network (LIN), or FlexRay, as well as Automotive Ethernet, were not designed with built-in security. This fundamental lack leaves in-vehicle communications inherently vulnerable to cyberattacks and potential data compromise. Data transmissions between various vehicle components and external systems are, therefore, susceptible to a wide range of cyber threats, requiring robust protective measures.

AI HYPERAUTOMATION SOLUTION

AI-powered real-time threat analysis

Swimlane Turbine uses unique Active Sensing Fabric technology to quickly process vast data streams for intelligent threat prioritization and rapid anomaly detection. This fabric ingests millions of alerts daily from harder-to-reach telemetry at cloud-scale, automating critical security data analysis. It reduces reliance on manual security operations, allowing security teams to focus on critical incidents and ensuring seamless scalability without increasing headcount.

Achieve vehicle communication and compliance

Swimlane Turbine integrates NTT DATA's in-vehicle and OEM backend security sensors, enabling end-to-end continuous monitoring and proactive incident response for connected vehicle cyber threats. It provides automated compliance enforcement, ensuring adherence to evolving industry regulations, and implements a Zero-Trust security approach to safeguard data exchanges across all vehicle networks

Rapid threat response and management

Turbine's AI automation drastically cut threat response times. It automatically neutralizes threats, minimizing impact through streamlined incident workflows. It seamlessly integrates with existing automotive infrastructure to build a more resilient security posture against evolving threats.

OUTCOMES

Risk mitigation & brand protection
Reduced exposure to cyber threats, safeguarding brand reputation and customer trust.

Operational cost efficiency
Automated security tasks, reducing the need for extensive personnel and manual processes.

Future-proofing cybersecurity strategy
Gained a scalable, AI-driven security approach adaptable to evolving automotive technologies.