MONITORING & INCIDENT RESPONSE

Introduction

By 2025, forecasts predict that there will be more than 450 million connected vehicles on the road. The increasing capabilities offered by connected computer systems enable a wide array of digital services and features.
Modern vehicles can have up to 100 embedded systems, which makes the vehicle a network on wheels.
The technological evolution, together with the expanding attack surface (remote interfaces), increases the number of vulnerabilities and techniques that are likely to be used by attackers to compromise a vehicle or the entire fleet.

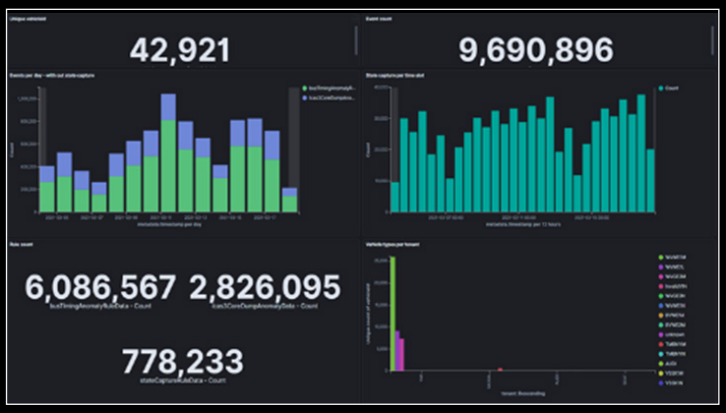
Challenges

Every component in a modern vehicle has at least dozens of open-source libraries, therefore, has thousands of known vulnerabilities and exploits.
Automotive companies are now required to implement vulnerability management processes to comply with the new regulations. The processes include monitoring and mitigation of cybersecurity vulnerabilities, not only for themselves but also for partners, third parties, and service providers during the entire supply chain and vehicle lifecycle (cross models, platforms, and versions).
The number of vulnerabilities and attacks increases every day. Therefore, manufacturers and Tier 1 suppliers must always have clear monitoring and visibility in order to make critical decisions in real time that prevents and minimizes the damage to the vehicle or driver.

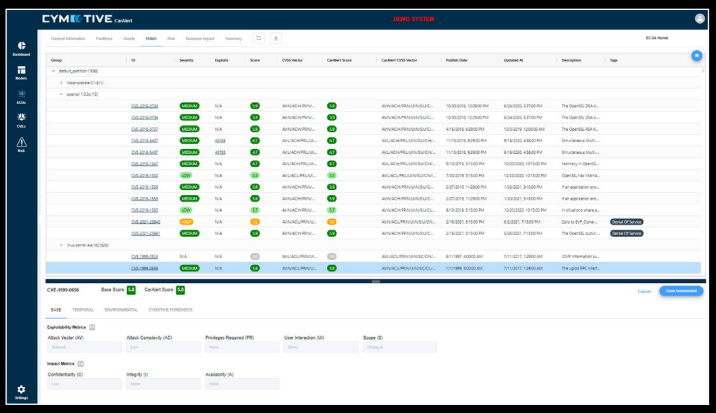
CYMOTIVE TECHNOLOGIES

The Solution

CYMOTIVE cyber automotive specialists and forensics team are researching how attackers and cyber criminals behave. The team detects and responds to cyberattacks in connected vehicles, services, and fleets by defining new cyber processes, building risk model methodologies and mitigation plans for its customers. The processes can be customized to the regulation standards in the relevant countries. Our Attack Research Lab (ARL) possess proven end-to-end incident detection and response capabilities. By elevating our vast knowledge of the attacker's perspective, we have established evidence-based detection mechanisms that use correlation rules, machine learning, and threat intelligence capabilities.



Vehicle Logs Analysis



CarAlert Vulnerability Dashboard

Our CarAlert system maps and manages vulnerabilities in the fleet level, including software packages and ECUs, measuring overall security and business implications to reach optimal decision making.
In order to detect, assess, and prioritize un-mitigated vulnerabilities, we collect data from several sources, such as the CarAlert system, IDS, threat intelligence, penetration testing, and others. The unique processes, together with the analysts' knowledge-base and unique experience, give us the ability to analyze the E2E perspective needed to mitigate vulnerabilities and to respond to cyber incidents.

CYMOTIVE TECHNOLOGIES