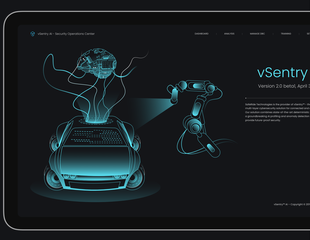
Business domain:
Automotive, Cybersecurity

Project type:
Web Application

Technologies:
React, NodeJS

vSentry

AI-enabled Web Application for Vehicle Monitoring and Preventing Cyberattacks



Business Overview

Cyber vulnerabilities are increasing rapidly with the growing number of internet-connected vehicles. Traditional security standards can't improve or deploy quickly enough to handle the increasing number of threats.

SafeRide is a provider of cyber anomaly detection and threat prevention solutions for vehicles powered by AI and machine learning. They offer in-vehicle cybersecurity for real-time, multi-layer monitoring of vehicle applications and networks. Their objective is to sell this as a comprehensive solution **called vSentry** that includes the installation of equipment, software, and staff training.

The client approached us to develop a web application that will secure the processes of connected apps and harness in-vehicle data, as well as uncover potential anomalies, threats, and insights systematically and to scale.

Challenge

Robust security and microservice base

The project required a strong security layer and a complete understanding of the vehicles' data encryption processes. To meet the client's needs, the NIX team set out to develop an application that will monitor the status of various vehicles, analyze incoming data, and prevent potential attacks or hacking attempts. We needed to implement a web application that would allow the handling of errors that come from the controller area network (CAN) bus vehicles in real-time.

** The CAN bus is a robust vehicle bus standard designed to allow microcontrollers and devices to communicate with each other's applications without a host computer.*

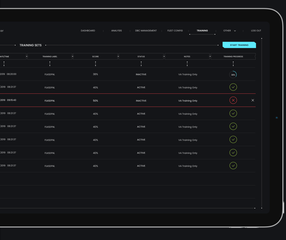
One of the requirements was that the app should support the microservice architecture, and we needed to realize how it should communicate with all other modules within a large system. Also, all the messages coming from the CAN buses must be stored on the application side, which implies a huge data stream.

The application needed to include two main modules:

- A message decoder from the communication matrix (or CAN matrix).
- An admin panel that displays all information and provides functionality for error analysis.

Solution

vSentry: high-integrity software powered by AI



The AI-based software establishes a baseline for vehicle behavior by training the machine learning model with a clean dataset. Once the baseline is established, the AI engine monitors data coming from vehicles on the road and identifies function anomalies as potential cyberattacks or malfunctions. Using raw vehicle data, it precisely **detects abnormalities and decreases the chances of false-positive alerts.**

For example, when a vehicle is attacked, vSentry channels information (different vehicle metrics) through the security software to a CAN bus that receives all incoming data. It reads a variety of signals and sends them to the cloud, where the AI engine analyzes the data and determines the type of cyber attack and its details. This information is then transmitted to a web application that depicts reports and metrics for further processing by a security analyst.

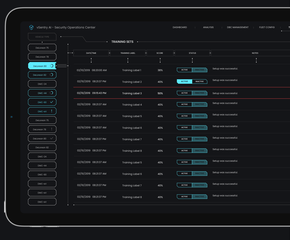
Moreover, the system includes various statistics, configurations, training, and other services.

To ensure resistance, sustainability, and the handling of high data load, we used a timescale database. Later we added modules that allowed us to:

- Add new CAN matrix structures to the system (different brands of machines, support for different structures);
- Train a third-party system to detect errors in the data flow;
- Aggregate general statistics by day and other filters.

The system's architecture consists of external and internal modules:

- Data acquisition module — responsible for collecting data and redirecting it to the system;
- AI Engine — responsible for analyzing the data and generating errors if discrepancies are found in the data.



Our solution is valuable to customers in two scenarios:

- Providing intrusion detection for vehicles that have no embedded intrusion detection and prevention system (IDPs) installed. In this scenario, the client's AI solution is a cost-effective way to detect cyberattacks with little or no changes to the vehicle hardware.
- Providing an additional layer of detection for IDPS-enabled vehicles to address zero-day vulnerabilities.

Outcome

A cost-effective way to detect and prevent cyber attacks

The client received a **high-security web application** that ensures vehicle safety while protecting personal data and privacy in real-time. In combination with AI machine learning and deep learning frameworks, vSentry allows for monitoring vehicle applications and networks, as well as discovering the onset of unknown threats and anomalies.

Client's testimonial

Noam Shalit
COO at SafeRide Technologies

*"We didn't have enough manpower or the capacity to complete a specific project, so we hired NIX to augment our staff. We started in April 2019, and we've been working with NIX on an ongoing basis. Headed by a knowledgeable project lead, **the team is experienced and professional.** The project manager heads the staff and demonstrates a really high level of expertise. We've been impressed by the NIX team's expertise and we plan to continue working with them".*

Team: 6 experts

Project Manager, Business Analyst,
Backend Developer, Frontend Developer,
QA Engineer, UI/UX Designer

Tech stack:

React, NodeJS, HTML, WebSocket, Jest,
PostgreSQL, InfluxDB, Apache Kafka,
Redis, Redux, Redux-Form, Streem, Doker,
Swagger, Kubernetes, Nginx

Contacts:

+1 727 256 3558
ask@nix-united.com
www.nix-united.com