

# Securing Automotive SaaS at VAIVA

Success Story: VAIVA GmbH



VAIVA GmbH is an independent subsidiary of the Volkswagen Group that has emerged as a pioneering force in safety technologies, contributing to the vision of reducing the impact of serious accidents to nearly zero by making assisted and autonomous driving safe. Founded in 2009, VAIVA began specializing in the virtual design of function algorithms for integral safety in the automotive industry. Today they offer safety solutions across various mobility-driven industries, especially Automotive, Defence and Agriculture.

VAIVA's mission is to make autonomous driving not just revolutionary but safe, not only increasing road safety but protecting lives every day. The company stands as a testament to how focused innovation, agile methodology, productivity-enhancing technologies and strategic partnerships can shape the change in the mobility industry and thus the future.

As tecRacer, we're proud to work with such a visionary company and support at making a difference and set the foundation for a secure platform, providing safe mobility.

## Project Goals

VAIVA's ICASIS, a powerful simulation platform to generate images and data from virtual cameras and sensors in the vehicle interior, was gaining traction, but their AWS infrastructure had grown organically into a complex environment, focussing on the product vision instead of the infrastructure and platform. Manual processes bottlenecked growth, disaster recovery was not fully established, and as an automotive SaaS provider, zero tolerance is allowed when it comes to insecurity. They needed expertise in both AWS and automotive platform application layer security. The product idea is there and a first implementation existed. tecRacer arrived to build the foundation and enhance the security of the platform around the innovative product.

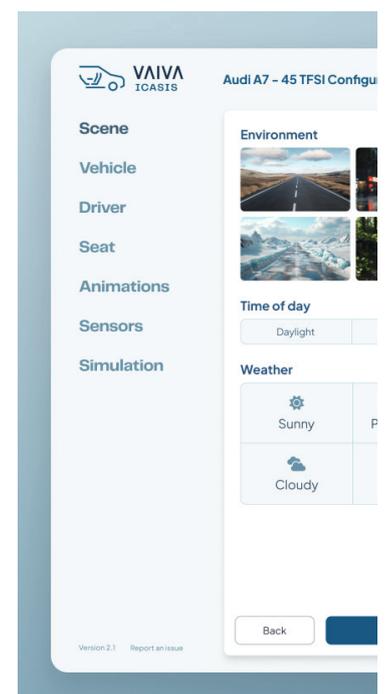
## tecRacer's Contribution

We began with understanding, not implementation. Through collaborative workshops and a comprehensive AWS Well-Architected Framework Review, we analyzed their architecture, workflows, and processes. Using PASTA and STRIDE threat modeling, we mapped real attack vectors specific to their platform and automotive context.

**Building the Foundation:** We implemented a secure landing zone using AWS Control Tower and customized Account Factory for Terraform. Each new account came preconfigured with security services, proper IAM roles, and compliance guardrails. Service Control Policies encoded security rules at the organizational level, while AWS Identity Center provided centralized access management. Our SSM Parameter-based solution enabled secure cross-account communication.

**Hardening the Application:** We refactored ICASIS's Infrastructure-as-Code for the multi-account environment, hardened ECS clusters, implemented comprehensive key management through KMS, and designed OIDC-based authentication avoiding long-lived credentials. An OWASP Top 10 analysis secured their APIs and development pipeline.

**Operational Excellence:** We developed comprehensive backup and disaster recovery strategies, established centralized logging with Security Hub and GuardDuty, designed secure VPC architectures with AWS IPAM, and prepared complete operational documentation for managed services transition.



**Knowledge Transfer:** Throughout the engagement, we maintained comprehensive documentation covering architecture decisions, security boundaries, operational procedures, and compliance frameworks. Multiple knowledge transfer sessions ensured VAIVA's team understood both the „what“ and the „why.“

### Used tools

AWS Control Tower and Organizations for governance, Identity Center for authentication, Account Factory for Terraform for automation. Security Hub, GuardDuty, KMS, and AWS Backup for defense in depth. Amazon ECS, RDS, Route 53, VPC, and IPAM for the application platform. GitLab with secure OIDC integration, OpenTofu as infrastructure source of truth. All guided by AWS Well-Architected Framework, PASTA/STRIDE threat modeling, and OWASP security principles.

### Result

VAIVA now operates on a secure, automotive-ready AWS foundation. Their multi-account architecture provides strong security isolation while automated provisioning enables rapid scaling. Comprehensive threat mitigation has significantly reduced risk, and robust backup strategies ensure business continuity.

Developers work efficiently within proper guardrails, productive without compromising security. The documented processes and knowledge transfer let VAIVA's team own their infrastructure and evolve it as they grow. Most importantly, customers and regulators have confidence in their platform's security posture, supporting VAIVA's growth in the competitive mobility market.

What began as an infrastructure challenge became strategic transformation, from organic growth to security-first architecture, positioning VAIVA for sustainable success in automotive safety innovation.

tecRacer combined deep AWS expertise with automotive industry understanding to deliver transformative results through collaborative partnership, comprehensive security practices, and thoughtful automation.

### Project Timeline

01.01.2025-31.06.2025

### Customer Perspective

**Frank Pirnay, Principal DevOps**

*“With the right partner like tecRacer, building secure applications becomes efficient — and automation at every step is the key. It streamlines processes, reduces risk, and ensures quality without slowing innovation.”*



### This is tecRacer

tecRacer stands for deep AWS expertise, a clear focus, and a partnership-driven mindset.

As the only AWS Premier Tier Services and Advanced Tier Training Partner in the DACH region, we support companies on their cloud journey – with pragmatic solutions, personal engagement, and a focus on real business impact.

Solution-oriented, passionate and with a healthy dose of pragmatism – this is how we create competitive advantages and ensure future security for our customers. With our team of experienced experts and a strong partner network.

Get to know our team, our values, and what drives us at [www.tecracer.com](http://www.tecracer.com) or contact us at [sales@tecracer.com](mailto:sales@tecracer.com).

