

# Sichere Bereitstellung von Automotive-SaaS für VAIVA

Success Story: VAIVA GmbH



Die 2009 gegründete VAIVA GmbH, eine unabhängige Tochtergesellschaft des Volkswagen Konzerns, hat sich als wegweisendes Unternehmen im Bereich Sicherheitstechnologien etabliert. Autonomes Fahren nicht nur möglich, sondern auch sicher zu machen, ist VAIVAs Mission. Dazu begann das Unternehmen mit der virtuellen Entwicklung von Funktionsalgorithmen für die integrale Sicherheit in der Automobilindustrie. Heute bietet VAIVA Sicherheitslösungen für verschiedene mobilitätsorientierte Branchen an, insbesondere für die Bereiche Automobil, Verteidigung und Landwirtschaft. Das Unternehmen zeigt beispielhaft, wie fokussierte Innovation, agile Methoden, produktivitätssteigernde Technologien und strategische Partnerschaften den Wandel in der Mobilitätsbranche gestalten können. tecRacer ist stolz darauf, mit einem derart visionären Unternehmen zusammenzuarbeiten und einen Beitrag zur Entwicklung einer sicheren Plattform für sichere Mobilität zu leisten.

## Gewachsene Strukturen bremsten Entwicklung und Sicherheit

VAIVAs leistungsfähige Simulationsplattform zur Erzeugung von Bildern und Daten aus virtuellen Kameras und Sensoren im Fahrzeuginnenraum – genannt „ICASIS“ – gewann zunehmend an Bedeutung. Die Amazon Web Services (AWS) Infrastruktur war jedoch organisch gewachsen und hatte sich zu einer komplexen Umgebung entwickelt, in der der Fokus eher auf der Produktvision als auf der Infrastruktur und Plattform lag. Manuelle Prozesse bremsten das Wachstum, ein vollständiges Notfallkonzept war nicht komplett implementiert, und als Anbieter eines Automotive-SaaS-Produkts gilt: Null Toleranz bei Sicherheitsrisiken. VAIVA benötigte daher Expertise in AWS-Infrastruktur und in sicherheitsrelevanten Aspekten der automobilen Platform Application Layer. Erste Umsetzungen und Ideen lagen bereits vor, doch um das Fundament zu schaffen und die Sicherheit der Plattform zu stärken, wurde tecRacer hinzugezogen.

## Projektleistung tecRacer

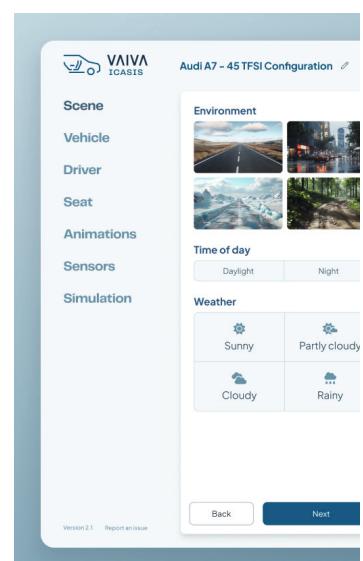
Das Team von tecRacer begann mit dem Verstehen der bestehenden Architektur, bevor etwas implementiert wurde. In gemeinsamen Workshops und einer umfassenden Überprüfung nach dem AWS Well Architected Framework analysierte tecRacer Architektur, Arbeitsabläufe und Prozesse. Mit PASTA und STRIDE Bedrohungsmodellierung identifizierten die Expertinnen und Experten reale Angriffsvektoren, speziell auf die Plattform und den automobilen Kontext zugeschnitten.

## Aufbau des Fundaments

tecRacer implementierte zuerst eine sichere Landing Zone auf Basis von AWS Control Tower und einer angepassten „Account Factory for Terraform“. Jedes neue Konto wurde mit Sicherheitsdiensten, passenden IAM Rollen und Compliance Richtlinien vorkonfiguriert. Organisationsweit definierte Service Control Policies stellen Sicherheitsregeln sicher, während AWS Identity Center ein zentrales Zugriffsmanagement bereitstellt. Die auf SSM Parametern basierende Lösung von tecRacer ermöglicht sichere Kommunikation zwischen Konten.

## Absicherung der Anwendung

tecRacer überarbeitete die bestehende Infrastructure as Code für die Multi Account Umgebung, härtete die Amazon Elastic Container Service (ECS) Cluster, implementierten ein umfassendes Schlüsselmanagement über Key Management Service (KMS) und entwickelten eine OpenID Connect (OIDC) basierte Authentifizierung, um langlebige Anmelddaten zu vermeiden. Eine Analyse nach OWASP Top 10 schützte ihre APIs und die Entwicklungspipeline.



## Betriebsstabilität, Qualität und Wissenstransfer

tecRacer entwickelte umfassende Strategien für Backups und Notfallwiederherstellung, richtete eine zentralisierte Protokollierung mit Security Hub und GuardDuty ein, entwarf sichere Virtual Private Cloud (VPC) Architekturen unter Nutzung von Amazon VPC IP Address Manager (IPAM). Während des gesamten Projekts wurde eine umfassende Dokumentation für den Übergang in den Managed Service Betrieb erstellt. Diese deckt Architekturentscheidungen, Sicherheitsgrenzen, Betriebsprozesse und Compliance-Rahmenbedingungen ab. Mehrere Wissenstransfersitzungen stellten sicher, dass das Team von VAIVA sowohl das „Was“ als auch das „Warum“ verstand.

## Eingesetzte Tools

- **Governance & Sicherheit**
  - AWS Control Tower, AWS Organizations, Identity Center, Security Hub, GuardDuty, KMS, AWS Backup
- **Plattform & Netzwerk**
  - Amazon ECS, RDS, Route 53, VPC, IPAM
- **Automatisierung & Entwicklung**
  - Account Factory for Terraform, GitLab mit sicherem OIDC, OpenTofu
- **Methodische Grundlagen**
  - AWS Well Architected Framework, PASTA/STRIDE, OWASP Prinzipien

## Vom Infrastrukturproblem zur strategischen Transformation

VAIVA arbeitet nun auf einer sicheren, für die Automobilindustrie geeigneten AWS-Grundlage. Die Multi-Account-Architektur gewährleistet eine starke Sicherheitsabschottung, während die automatisierte Bereitstellung ein schnelles Skalieren ermöglicht. Umfassende Maßnahmen zur Bedrohungsabwehr reduzieren Risiken, robuste Backup-Strategien sichern die Geschäftskontinuität. Die Entwickler-Teams arbeiten effizient innerhalb definierter Leitplanken – produktiv und ohne die Sicherheit zu beeinträchtigen. Die dokumentierten Prozesse und der Wissenstransfer ermöglichen dem VAIVA-Team, die Infrastruktur eigenständig weiterzuentwickeln. Kunden und Regulierungsbehörden haben Vertrauen in die Sicherheitsarchitektur der Plattform – ein wesentlicher Faktor für VAIVAs Wachstum in einem wettbewerbsintensiven Markt. Was als Infrastrukturproblem begann, wurde zu einer strategischen Transformation: Von organisch Gewachsenem hin zu einer Security First Architektur, die VAIVA in Position bringt für langfristigen Erfolg in der automobilen Sicherheitsinnovation. tecRacer kombinierte fundierte AWS-Expertise mit Branchenverständnis, um durch partnerschaftliche Zusammenarbeit, umfassende Sicherheitsmaßnahmen und durchdachte Automatisierung nachhaltige Ergebnisse zu erzielen.

### Projekt Dauer

01.01.2025-31.06.2025

### Ansprechpartner beim Kunden:

**Frank Pirnay, Principal DevOps**

*„Mit dem richtigen Partner wie tecRacer wird das Entwickeln sicherer Anwendungen effizient. Dabei ist die Automatisierung in jedem Schritt der Schlüssel. Sie verschlankt Prozesse, reduziert Risiken und stellt Qualität sicher, ohne Innovation zu bremsen.“*



## Das ist tecRacer

tecRacer steht für tiefgreifende AWS-Expertise, eine klare Spezialisierung und ein partnerschaftliches Selbstverständnis.

Als einziger AWS Premier Tier Services und Advanced Tier Training Partner in der DACH-Region begleiten wir Unternehmen bei ihrer Cloud-Transformation – pragmatisch, persönlich und mit echtem Wirkungstreiber im Fokus.

Lösungsorientiert, leidenschaftlich und mit einer gesunden Portion Pragmatismus – so schaffen wir Wettbewerbsvorteile und sorgen für die Zukunftssicherheit unserer Kunden. Mit unserem Team aus erfahrenen Experten und einem starken Partner-Netzwerk.

Erfahren Sie mehr über unser Team, unsere Werte und was uns antreibt auf [www.tecracer.com](http://www.tecracer.com) oder nehmen Sie unter [sales@tecracer.com](mailto:sales@tecracer.com) Kontakt mit uns auf.

