CASE STUDY

Securing the API-Driven Connected **Vehicle Ecosystem**

Overview of the Problem

APIs are pervasive throughout the automotive ecosystem, and play pivotal roles in ensuring secure operations across the entire automotive supply chain.

These chains are complex and consist of a network of suppliers who provide hardware, software, and infrastructure to automakers. The connectivity of these systems expands the manufacturer's attack surface, making APIs a prime target for both opportunistic and advanced persistent cyber threats. Regulations and industry standards are now driving manufacturers to take responsibility for the security of APIs across the lifetime of the vehicle and the span of the ecosystem.

Challenges faced by this leading global automobile manufacturer included:

- Lack of visibility into the security posture of thousands of APIs.
- Manual security reviews were failing to scale with the pace of development.
- The API threat landscape in automotive is vast and fast-moving; continuous monitoring and assessment are vital, not just periodic audits.
- Rising regulatory compliance demands - e.g. UNECE R155, ISO/SAE 21434, GDPR.

Industry:

Automotive Manufacture

Key Impacts:

- **Full security governance across 35,000 APIs and 5,000 developers**
- **Predictable API behavior and reduced false positives**
- **Enable compliance with UNECE R155 and ISO 21434**

The Solution: 42Crunch API Security Platform

After a rigorous selection process, 42Crunch was chosen as the only API security platform capable of addressing these challenges.

The platform capabilities include:

- **Enabling a security by design approach**: 42Crunch is embedded at every stage of the API lifecycle, from design in IDEs, through CI/CD security checks, to production firewalling enforcing security standards by design.
- **Automating security posture management**: The platform enables the automation of API contract testing, vulnerability scanning, and remediation guidance during development.
- **Scaling security enforcement**: 42Crunch's seamless integration with the auto-manufacturer's DevOps toolchain allowed the security program to be enforced at scale to address the needs of a complex API-based ecosystem.
- **Achieving predictable API behavior**: Continuous protection and enforcement of security policies on live API traffic and avoid the dangers of undefined APIs.

The Benefits

The positive outcomes reported from the 42Crunch deployment included:

- **Proactive risk mitigation** - led to a dramatic reduction in API vulnerabilities reaching production, through early detection and automated remediation.
- **Operational efficiency** - achieved via centralized, real-time visibility into the security posture of thousands of APIs across business units worldwide.
- **Regulatory and standards compliance** - including UNECE, ISO/SAE 21434, and GDPR is delivered as part of automated security audits and workflows, rather than through painful, manual reviews.
- **Scalability and flexibility** of cloud-native architecture and integration with existing IDE and CI/CD pipelines enabling security and development teams to "design security in" from the start, reducing bottlenecks and eliminating shadow APIs.

> Intentional design is fundamental to automotive software development, including automotive APIs, as the public would not tolerate a vehicle or APIs which are developed without an explicit design or focus on safety. 42Crunch's shift-left approach to API security aligns directly with intentional design practices.
>
> **Darren Shelcusky**
> Manager Vehicle and Connectivity Cybersecurity, Ford Motor Company

Conclusion

The deployment of the 42Crunch API Security Platform stands as a model for the automotive industry facing exponential API growth. This global auto-manufacturer was able to scale security enforcement to thousands of APIs and developers, ensuring APIs underpinning connected vehicles, mobile apps, and business platforms were secure, compliant, and resilient to an ever-evolving threat landscape.