Driving compliance:

Ensuring embedded software visibility in automotive manufacturing

KEY TAKEAWAYS

Enhanced visibility

Gain deeper insight into embedded software to ensure compliance and security.

Open source identification

SCANOSS detects undeclared open source and dependencies, reducing hidden risks.

Proactive compliance

Stay ahead of legal and regulatory challenges by addressing risks early.

THE SITUATION

Enhancing compliance visibility in automotive manufacturing

A software supplier for an automotive industry leader faced a critical challenge: ensuring compliance in the software they developed which included both native car apps (APPs) and Internal Combustion Engine (ICE) systems. Building on the base platform provided by the brand, they needed to ensure complete clarity about the software they were delivering back to the brand. This required identifying open source software (OSS) in use, scanning GitHub branches effectively, and implementing basic compliance policies to mitigate hidden risks. Additionally, they sought a comprehensive solution to address open source in AI-generated code and compliance challenges in a unified approach.

With undisclosed software posing risks such as hidden licence obligations and copyright violations, the stakes were high. The team needed to address several technical challenges to ensure compliance and minimise risks. This included defining which licences to check against specific policies, limiting scans to production dependencies impacted by an npm install, and generating comprehensive reports for AI functions integrated into GitHub Actions. Without a solution to these issues, the company risked compliance failures, legal consequences, and operational inefficiencies.

THE SOLUTION

Simplified compliance with SCANOSS

By leveraging SCANOSS's comprehensive License Dataset, the company gained the ability to find both declared and undeclared open source components, binaries, and dependencies, including critical C and C++ code. SCANOSS offered detailed insights into licences, copyrights, and attributions, enabling the company to address compliance requirements with precision and efficiency. The integration into GitHub Actions was enhanced with the ability to include, exclude, and explicitly configure the set of licences checked. Additionally, new Policy Check reports were delivered as Workflow Artifacts, allowing the team to download each Policy Check result in Markdown format—streamlining their workflows and ensuring accessible and actionable reporting.

> **Undisclosed software poses risks like hidden licence obligations and copyright violations—the stakes were high.**

THE OUTCOME

Compliance secured; risks mitigated

They achieved complete visibility into the embedded software within their products, ensuring full compliance with licensing obligations. This proactive approach eliminated legal and regulatory risks, safeguarded the company's reputation, and kept uninterrupted shipping timelines, reinforcing their position as an industry leader committed to quality and compliance.

In August, the partnership was established, and by October SCANOSS delivered a tailored solution after rigorous testing and software adjustments.fr. The seamless integration into their existing workflows ensured there was no disruption to their operations, allowing the team to maintain productivity without losing any working time. Within just three months, SCANOSS enabled the company to enhance compliance processes, achieve software transparency, and eliminate risks tied to embedded software.

Ready to enhance visibility, mitigate risks, and future-proof your operations?

sales@scanoss.com