critical software



CASE STUDY | AUTOMOTIVE

SDV Compliance with SPDX 3.0

How a global automotive OEM achieved software supply-chain transparency and regulatory compliance.

The challenge

Modern vehicles integrate millions of lines of code across multiple ECUs (in some instances, more than 70 ECUs in a single vehicle), making software provenance, vulnerability response, and audit readiness difficult to manage at scale. The OEM needed a more robust way to trace software components, build environments, and security status across the vehicle platform, while preparing for increasingly stringent regulatory expectations – these also include the prevention of contributions from individual contributors & partners located in specific regions deemed as adversarial.

© Critical Software

The solution

The OEM adopted an SPDX 3.0-based architecture to represent the vehicle software stack as a structured, machine-readable system rather than a set of static SBOM files. This approach allows proving due diligence while responding to compliance audit requests by governmental entities, through improved traceability across software components, build metadata, vulnerability information, and assets used in the development.

Key implementation elements included:

- Core Profile: linked the software stack to the vehicle identity and supported end-to-end traceability.
- Build Profile: captured cryptographically guaranteed contributor info (commit signing), compiler toolchains, build environments, and build location data to strengthen provenance records; import & include SBOM & compliance statements from tier 1 suppliers.
- Security Profile: provided up-to-date exploitability status to respond to legal requirements and help teams prioritize relevant vulnerabilities.
- AI/Dataset Profile: documented model lineage and training data provenance for ADAS-related functions.

© Critical Software

CASE STUDY | AUTOMOTIVE:

SDV COMPLIANCE WITH SPDX 3.0

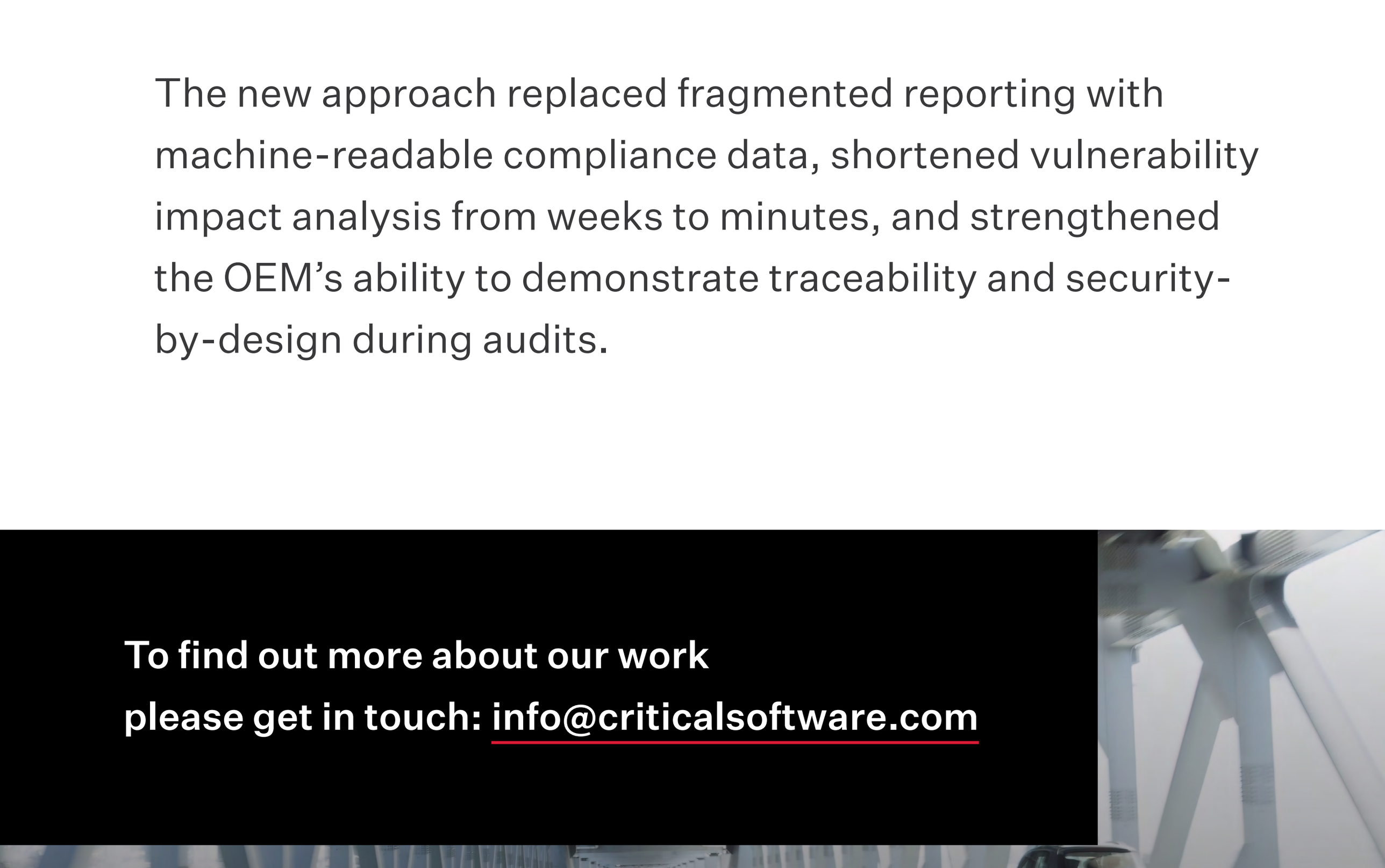
High-risk areas

SPDX 3.0 addresses the most exposed areas of the vehicle stack: communications and infotainment systems, where foreign adversarial exploit injection and data sovereignty are primary concerns; zonal controllers, which require faster visibility into security and patch status; OTA updates, where software must be validated as secure before deployment; and ADAS AI models, where dataset and model provenance require full traceability.

A story of success

The new approach replaced fragmented reporting with machine-readable compliance data, shortened vulnerability impact analysis from weeks to minutes, and strengthened the OEM's ability to demonstrate traceability and security-by-design during audits.

To find out more about our work
please get in touch: info@criticalsoftware.com



critical software