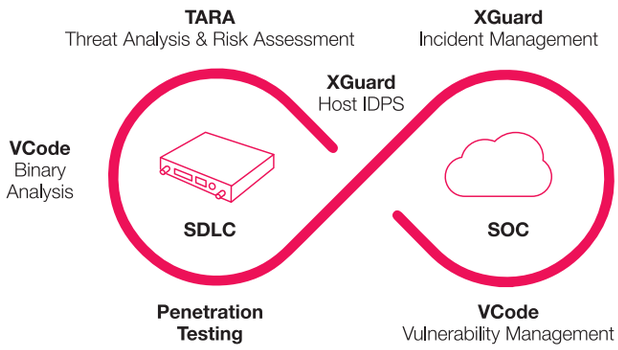
Accelerate ISO/SAE 21434 Compliance

Karamba Security

With market adoption of electric and software-defined vehicles, Karamba's End-to-End Product Security Portfolio enables OEMs and Tier-1 suppliers to comply with the ISO/SAE 21434 cybersecurity standard and with the UN R155 regulation, without affecting R&D processes, start of production schedules and post-production operational processes.

Karamba's portfolio enables its customers to discover, mitigate and manage security vulnerabilities in their ECUs and vehicle types, for faster compliance with the cybersecurity standard, without putting a burden on R&D, supply-chain vendors, or fleet managers.

Karamba's End-to-End Product Security



Discover.

Karamba's products and services discover vulnerabilities and threats during the product development lifecycle, without interfering with R&D or supply-chain processes.

- ✓ **Threat Analysis and Risk Assessment (TARA)**
  Karamba's product security experts identify risks in the ECU and vehicle type architecture and design. The uncovered issues and vulnerabilities are prioritized and mitigated according to risk and likelihood to be exploited, in order to enable OEMs and suppliers to focus only on the highest risk issues and minimize development and SOP impact.
- ✓ **VCode – Binary Analysis Software**
  VCode software enables OEMs and suppliers to assure supply chain security. Within minutes, VCode scanning uncovers security vulnerabilities, misconfigurations, and other security issues in suppliers' and home-grown binaries. The discovered issues are prioritized based on the software bill of materials (SBOM), which is automatically created by VCode software. VCode covers AUTOSAR, QNX, Linux, and Android operating systems.
- ✓ **Penetration Testing**
  Karamba's pentesting service identifies security issues in ECUs and the entire vehicle architecture, to enable OEMs and suppliers to remediate critical security issues before production. We perform interface fuzzing, binary research and reverse engineering and have completed dozens of pentests to ECUs such as in-vehicle inverter, battery management system, infotainment, telematics, gateway and ADAS, as well as complete EV vehicle types.

Mitigate.

ECUs and vehicle types should be protected against exploiting zero-day and known vulnerabilities, to reduce remediation time, and remove urgency in security patching, against known and newly reported threats.

✓ **XGuard Software**

- Karamba's award-winning Host IDPS software hardens the ECU against malware and in-memory attacks, thanks to binary whitelisting and control flow software integrity. It ensures deterministic protection and continuous monitoring of the ECU.
- XGuard complements secure boot mechanisms with runtime firmware protection.
- Seamless to R&D: Karamba's XGuard software is applied to the ECU firmware during build (no source code required), without requiring any change to R&D processes or validation plans.
- Karamba's XGuard covers 13 different operating systems and over 7 CPU architectures. Its negligible performance impact enables OEMs and suppliers to protect the ECU, as-is.

Manage.

Karamba's XGuard Monitor and VCode Vulnerability Management System offer Continual Security for OEMs and suppliers, and enable them to focus on vulnerabilities that matter most.

✓ **VCode Vulnerability Management System (VMS)**

Consolidating vulnerabilities from multiple data sources, such as AutoISAC alerts, security attacks, bug bounty and white hat hackers' disclosures. VCode VMS prioritizes all issues by blast-radius analysis, severity, and exposure to exploits.

✓ **XGuard Monitor**

XGuard's backend engine receives high-fidelity alerts from XGuard agents and matches them to automatically created baselines on vehicle and fleet levels. The baselining and anomalies are created by utilizing an unsupervised machine learning engine, in order to eliminate needs for manual settings. This enables automatic adjustments to new features, which are dynamically delivered to software defined vehicles.

Karamba Security

Drive Innovation with Confidence

www.karambasecurity.com | contact@karambasecurity.com

Israel office Tel: +972 9 88 66 113
USA office Tel: +1 833 4KARAMBA
Germany office Tel: +49 172 3991 036