VCode VMS

Vulnerability Management System

Karamba Security

Manage Your Vulnerabilities, Automatically

Automated system to manage OEM and Tier-1 supplier vulnerabilities, for cost-effective compliance with the ISO/SAE 21434 standard and the UN R155 regulation

The automotive industry faces strict regulations. UN R155 requires software defined vehicles to be type approved, and the ISO/SAE 21434 standard describes the detailed set of processes required and the expected supporting documents, specifically for continual vulnerability management. Managing cybersecurity vulnerabilities, threats and incidents is a cumbersome process that involves disperse parts of the organization, as well as supply chain providers. It's a costly effort, which lengthens the remediation and validation process, and may have significant compliance and time-to-market consequences.

Karamba Security's VCode Vulnerability Management System enables OEMs and suppliers to discover, mitigate and manage security vulnerabilities, alleviate the issues associated with those processes and provide the evidence needed for the type approval process.

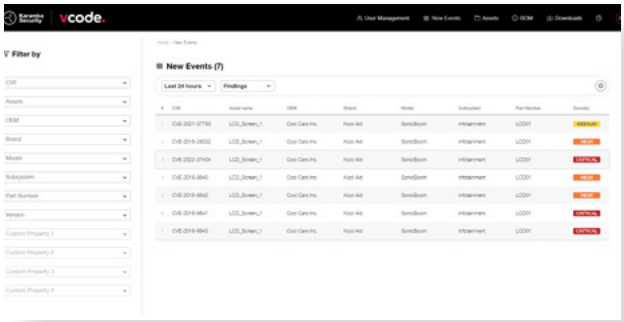
VCode VMS allows OEM and supplier security teams to manage their vulnerability assessment and prioritization process in a central location, creating a common language for all internal and third-party stakeholders, i.e. product security experts, SOC analysts, R&D architects, developers, quality assurance, validation, homologation, and management teams.

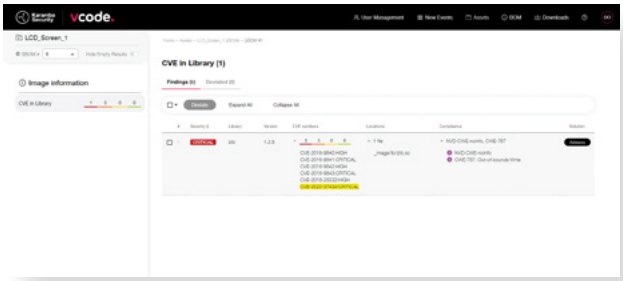
At the base of the system is a detailed, hierarchical software/firmware component inventory, creating a software bill of materials (SBOM) for ECUs and vehicle-types.

The system enables handling a range of security issues: code vulnerabilities, weaknesses, misconfigurations, and CVEs from various sources across the product lifecycle. Sources may include NVD and other public CVE databases, penetration testing reports, threat analysis and risk assessment (TARA) reports, binary scanning results, bug bounty and information disclosure reports, threat intelligence sources like Open-Source Intelligence (OSINT), and other feeds.

Analyze Blast Radius

Easily provide accurate impact analysis reports, mapping issues to system impact, across multiple product lines and software versions.



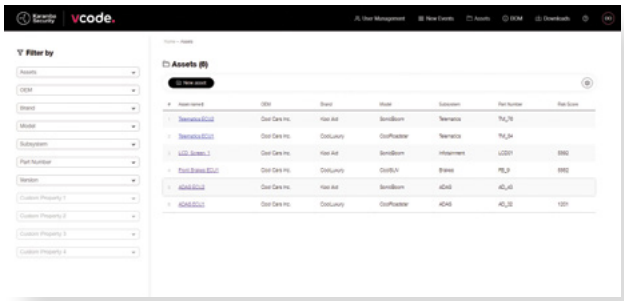


Exploitability and Remediation Analysis

Provide in-depth reports of security incidents, including affected software libraries, their locations, and exploit impacts.

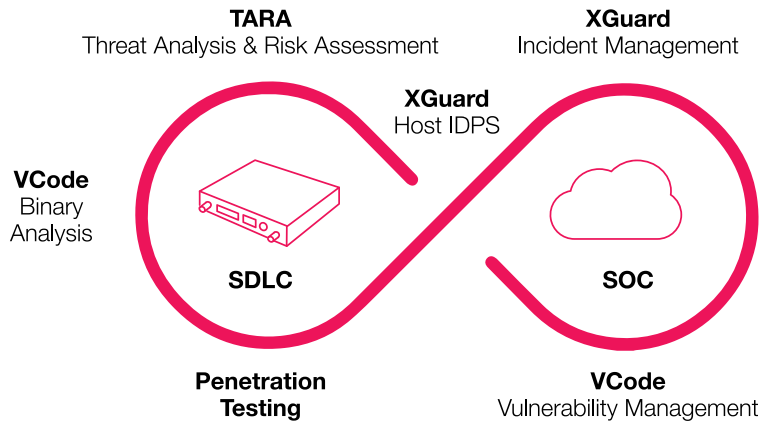
Assets Database

Show all software assets by vehicle type and ECU, for fast investigation processes.



Karamba's End-to-End Product Security Portfolio enables electric and software-defined vehicle (EV and SDV) OEMs and Tier-1 suppliers to comply with the ISO/SAE 21434 standard and with the UN R155 regulation, without interfering with R&D schedules or post-production operations.

Karamba's End-to-End Product Security



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