XGuard®

Vehicle Host IDPS

Karamba Security

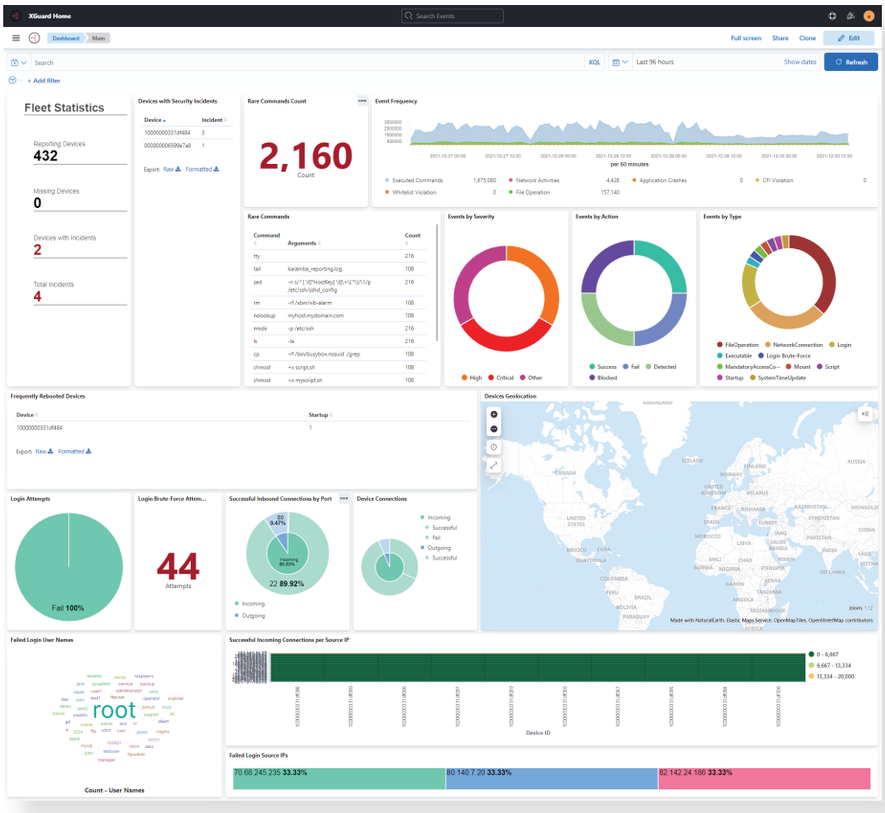
Seamlessly Applied ECU Hardening and Unsupervised Machine Learning

OEMs and Tier-1 suppliers are responsible for their vehicles' and ECUs' resiliency against cyberattacks.

XGuard software is automatically applied to the ECU firmware, hardens it, and detects attack attempts. XGuard expedites OEMs' and suppliers' compliance with the ISO/SAE 21434 standard without affecting their engineering and validation processes.

What is XGuard?

Karamba Security's XGuard is an embedded software agent and a cloud-based backend. XGuard agents deterministically prevent malware and fileless attacks. The backend engine detects anomalous behavior and provides high fidelity alerts about suspicious devices.



Seamless Integration

XGuard agents are integrated as part of the firmware build toolchain. No source code is required, development processes are untapped, and the agent is seamlessly integrated with the ECU binaries.

Verification & validation are likewise unchanged. The product software image is tested with XGuard embedded into it, without requiring changes to test plans, as XGuard doesn't change product functionality.

Karamba Security

Negligible Performance Overhead

The XGuard agent is designed for embedded systems, with low CPU and memory consumption. The agent takes up to 5% CPU overhead, 5% memory size, and 10% of the flash size.

XGuard Backend: Unsupervised Machine Learning

XGuard's backend has a set of predefined monitored behaviors, observes a huge number of events across the entire fleet and uses adaptive unsupervised machine learning to find anomalies that indicate threats. This allows Vehicle Security Operations Center (VSOC) teams to focus on highlighted anomalies and to determine incidents' root cause.

XGuard's backend engine specializes in detecting "unknown threats". For example: insider threats (someone who has valid credentials to the system yet has malicious intent) and advanced persistent threats.

XGuard unsupervised machine learning automatically adjusts to a wide variety of ECU behaviors and fleet deployments without requiring any developer intervention.

Broad Threat Coverage

XGuard software enables OEMs and Tier-1 suppliers to assure their customers a high level of protection against cyberattacks.

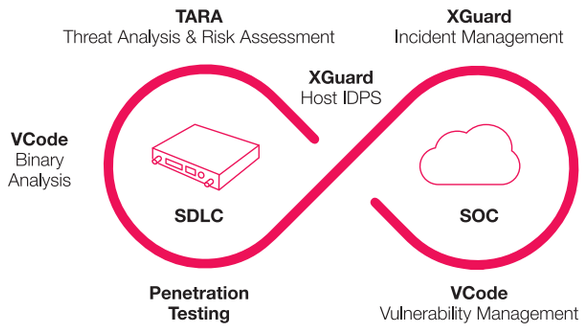
- Malware is deterministically detected as foreign code which wasn't part of the original build, and is prevented from executing.
- Fileless attacks, which exploit in-memory vulnerabilities such as buffer overflow, are deterministically detected and prevented by utilizing Karamba's patented Control Flow Integrity (CFI).
- The backend analytics engine identifies and alerts on a significant number of hacking attempts such as password guessing, privacy violations, and rogue devices.

ISO/SAE 21434 and UN R155 Compliance

Software Integrity, security event logging and an update mechanism form the cornerstone of many cyber-related regulations in various industries.

Automotive OEMs and suppliers, who must meet the ISO/SAE 21434 standard and UN R155 regulation, use XGuard for achieving compliance. The software, which is seamlessly integrated, and auto-adapts to fleet behavior, addresses the UN R155 requirements for software integrity, OTA updates, authentication, and logging, without taking an extra toll on R&D, or requiring changes to the ECU architecture.

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