

Karamba Security Invited to Join Auto-ISAC Industry Alliance and Present its Cyberattack Prevention at First Annual Summit

BLOOMFIELD HILLS, Mich. and HOD HASHARON, Israel — Dec. 12, 2017 – [Karamba Security](#), the world leader in automotive cyberattack prevention, has been invited to join the [Automotive-Information and Sharing Analysis Center](#) (Auto-ISAC) and will present end-to-end prevention and real-time forensics data at its first annual [Auto-ISAC Summit](#).

CEO and Co-founder Ami Dotan joins cybersecurity experts from leading automakers and tier-1 suppliers and representatives from the National Highway Traffic Safety Administration (NHTSA), the Federal Trade Commission (FTC) and Department of Homeland Security (DHS) for the two-day “Start Your Engines” conference in Dearborn, Michigan, Dec. 13-14, 2017. His presentation will include a demo of a car attack, end-to-end prevention and real-time forensics data.

Karamba will present and demo its market-leading capability to block hacking attempts with zero false positives and produce forensics data that is critical to security bug remediation by vendors who are not deploying Karamba’s Autonomous Security in their cars.

“Karamba enables the industry to meet NHTSA and DOT guidelines for car cybersecurity by providing a cyberhealth view of the entire fleet and detailed forensics data about blocked cyberattacks. When Karamba’s software prevents a hacker’s exploit, it sees the attempt and reports on the blocked vulnerabilities. When shared with Auto-ISAC subscribers, the industry can use these threat alerts and forensics data to remediate security bugs in cars that are not protected by Karamba’s software,” said Ami Dotan.

The reported data to Auto-ISAC members provides a fleet view for the carmakers, with a drill down to the cars attacked, prevention methods and forensics data about the vulnerability that hackers tried to exploit, but which were blocked by Karamba’s software.

As an industry-led alliance, Auto-ISAC relies on members to develop best practices to enhance cybersecurity awareness and collaboration across the global automotive industry. Karamba Autonomous Security is key in enabling Auto-ISAC members to prevent attacks with zero false positives and assure consumer safety.

Heuristic-based security leads to false positives. It’s not sufficient to minimize the number of false positives as a single error could cost lives. In this talk, Dotan will explain how to overcome these challenges with deterministic security that hardens the vehicle’s ECUs based on factory settings blocking any deviation in commands as a hacking attempt.

This enables automakers and tier-1 providers to comply with regulations and guidelines defined in the [Automated Driving Systems \(ADS\): A Vision for Safety 2.0](#), the [SELF DRIVE Act](#) passed by the U.S. House of Representatives and similar guidelines emerging worldwide.

Auto-ISAC was formed in August 2015 by automakers to establish a global information sharing community to address vehicle cybersecurity risks. Auto-ISAC operates a central hub for sharing, tracking and analyzing intelligence about cyber threats, vulnerabilities and incidents related to the connected vehicle.

Currently, Auto-ISAC Members account for more than 99 percent of light-duty vehicles in North America, with over 30 global OEM and supplier members. Building upon the success of this collaboration, Auto-ISAC recently expanded membership to heavy trucking OEMs and their suppliers, as well as the commercial vehicle sector—including fleets and carriers.

Auto-ISAC as well as Karamba will be at [CES® 2018](#) January 9-12, 2018, in Las Vegas, Nev. Karamba Security will showcase its capabilities working with leaders in the global automotive supply chain. From its suite at the Bellagio Hotel, Karamba will conduct joint demonstrations with partners who include Honeywell, IAV, Alpine and FEV to engage with conference-goers on cybersecurity vulnerabilities and how organizations can work together to secure the automotive industry. To schedule a private demo email: ces@karambasecurity.com.

Since coming out of stealth at the end of March 2016, Karamba Security has been actively engaged with 16 different car makers and tier-1 providers on hardening their ECUs of choice.

In November of 2017 Karamba Security was named by CNBC to its list of most innovative startups. In addition, Karamba Security was unanimously recognized with TU-Automotive's Best Cybersecurity Product/Service for 2017 and the 2017 North American Frost & Sullivan Award for Automotive New Product Innovation.

More information is available at www.karambasecurity.com.

Resources

[Autonomous Security](#)

[Karamba Security Approach](#)

About Karamba Security

Karamba Security provides industry-leading cybersecurity solutions for connected and autonomous vehicles. Its SafeCAN and Carwall software provide end-to-end in-vehicle security by authenticating communications, including OTA updates, with zero network overhead and by hardening the car's safety ECUs from attempts to manipulate or compromise their commands and hack into the car. Together, the products prevent cyberattacks with zero false positives, no connectivity requirements and negligible performance impact. In one year, Karamba has engaged with 16 OEM and tier-1 customers, received a total investment of \$17 million. The company has been recognized in 2017 with TU-Automotive's Best Cybersecurity Product/Service and the North American Frost & Sullivan Award for Automotive New Product Innovation. More information is available at www.karambasecurity.com.