Global Automotive Partners Collaborate to Keep Hackers Out of Cars; Joint Solutions to be Demoed at CES 2018

BLOOMFIELD HILLS, Mich. and HOD HASHARON, Israel — Dec. 18, 2017 – Karamba Security, the world leader in automotive cyberattack prevention, today announced that it will be part of a collaboration of global automotive players to secure connected and autonomous vehicles. The collaboration secures cars from known and unknown vulnerabilities that can be weaponized by adversaries in cyberattacks.

US-based Honeywell, Japan-based Alpine, Germany-based IAV and Israel and US-based Karamba Security are partnering to create multi-layered solutions to secure cars. Each partner brings to bear its own unique expertise and technology to respond to existing and evolving attack methods and vectors.

Demonstrations at CES will feature:

- Preventing cyberattacks on vehicles, with zero false positives, provided by Karamba Security
- Reporting the attack attempts to an OEM Security Operations Center (SOC), provided by Honeywell
- Hardening infotainment systems according to factory settings and preventing changes, i.e. malware, provided by Alpine, and by Karamba Security
- Engineering and integration services provided by IAV demonstrating a driving car secured by Karamba Security software, with reports and alerts transmitted to a SOC managed by HP Enterprise

Honeywell – Anomaly Detection, Exploit Prevention and SOC Analysis
Together with Karamba, the two companies will identify and validate, in runtime, software commands and data generated by more than 100 million lines of code governing modern vehicle operation. Honeywell's Intrusion Detection software monitors in-vehicle network communications and anomalies, while Karamba Security's ECU software prevents an attack on the vehicle. Detected anomalies and prevented exploit attempts are transmitted in either real-time or via a scheduled download to Honeywell security centers for analysis and remediation.

IAV – Intelligent Safety Analysis and Authentication of Vehicle Users
With the risks of cybersecurity threats that modern data connections are open to, IAV, in partnership with Karamba Security, has created an Automotive Security Defense Center to showcase how these attacks can be prevented to protect the connected vehicle. The prototype continuously monitors the vehicle for OEM and fleet operators to detect and avert attacks, analyzes weak points and any issues noted by OEMs to close

security gaps, and incorporates routine software updates. The demo at CES will illustrate a hack attempt and how it can be prevented.

Alpine – Resiliency of Infotainment System to Ransomware Attack
By integrating Karamba's Carwall product Alpine and Karamba assure that the infotainment system is resilient to attacker attempts to hack the system. To demonstrate this capability, the companies have introduced a vulnerability into the system. The demo toggles between a vulnerable system and one with protection applied. The exploit results in a ransomware attack which locks the system. The same exploit attempt will fail on the protected browser, and a detailed incident report is sent to Karamba's incident management server.

The automotive industry faces a multitude of pressing security challenges, most significant among them is authenticating car networks. There is an urgent need to authenticate in-vehicle communication to protect safety systems against hacks and to ensure that OTA updates are not used to deploy malware on targeted ECUs. Carmakers have been demanding suppliers authenticate in-car communications to protect vehicles against malicious messages sent by unauthorized Electronic Control Units (ECUs) or by physically hacking the car.

The collaboration aims to overcome industry barriers that have hindered progress to deploy stronger, layered defenses to assure consumer safety and help automakers and tier-1s meet regulatory compliance.

Regulations and guidelines are emerging worldwide such as those set out by the National Highway Traffic Safety Administration (NHTSA) and U.S. Department of Transportation (DOT)'s newly published federal guidance, Automated Driving Systems (ADS): A Vision for Safety 2.0, as well as the guidelines defined in the SELF DRIVE Act passed by the U.S. House of Representatives.

Visit Karamba at CES 2018 for more information about CES demonstrations. To schedule a private demo email: ces@karambasecurity.com.

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.