British Government Recognizes Karamba Security as Automotive Technology Innovator

Invited to 10 Downing Street as part of Israeli Technology Delegation

DETROIT & TEL AVIV, Israel, April 29, 2016 — The British Embassy in Israel has named Karamba Security to an elite group of technology innovators in recognition of its pioneering work to secure automobile electronics systems from cyberattacks.

Karamba Security joins a delegation of prominent Israeli automotive and transport companies who will be honored at a reception held Thursday, May 5 at the British Prime Minister's residence at 10 Downing Street.

The delegation will travel to the United Kingdom to meet with dozens of leading organizations in the industry, including representatives of car manufacturers Jaguar and Land Rover and heads of London's Transport Authority.

Fifteen start-ups were selected in the fourth **annual TeXchange 2016: Intelligent Mobility - Innovation in Action**, aimed at introducing British companies to Israeli innovation in intelligent mobility. TeXchange is run by the UK Israel Tech Hub at the British Embassy Israel, in partnership with the Institution of Engineering and Technology (IET). The competition this year focused on solutions for the automotive industry and smart cities.

Taking place at IET London: Savoy Place on May 4, guests will be given the opportunity to meet with Israel's most cutting-edge mobility innovators and engage with other British mobility stakeholders active in this space.

With autonomous driving on the horizon, cybersecurity will become as essential as seat belts and air bags. Last month, the FBI released a 2,000-word public service announcement warning of "remote exploits" in motor vehicles. The FBI's recent warning has highlighted the cybersecurity risks of the increasingly connected car. Analysts estimate that 20 percent of vehicles sold worldwide in 2015 included some form of embedded connectivity. Gartner predicts that by 2020, the number of connected cars sold globally will be 250 million. And IHS predicts that by 2022, 73 percent of passenger cars sold will be equipped with an Internet-based entertainment portal or Web-connected system for things like safety alerts. Something must be done to close the vulnerabilities to ensure the safety of vehicle operation.

Karamba Security was selected for its innovative approach to protect the connected car. Its solution hardens a car's externally connected controllers, or electronic control units (ECUs) open to the Internet, Wi-Fi or Bluetooth, etc. against hackers, sealing off a car's infotainment system, GPS device and roadside assistance program by making sure that no unfamiliar code is allowed to run. By blocking access to those entry points, it becomes much more difficult for an intruder to reach critical driving functions like the steering wheel, ignition and brakes.

“We make sure that only what’s part of the factory settings is allowed to run,” said Ami Dotan, Karamba’s co-founder and CEO. “Once we recognize foreign code, we just don’t let it run.”

Karamba is co-founded, in part, by cybersecurity experts that managed Check Point Software Technologies’ endpoint security research and development teams. Their expertise is helping Karamba develop solutions to harden the connected ECUs within automobiles to protect them from cyberattacks and ensure the car’s safe, ongoing operations.

To learn more, please visit www.karambasecurity.com.

Media contacts

Montner Tech PR
Deb Montner
dmontner@montner.com
+1-203-226-9290 x110