Karamba Security to Demonstrate Embedded Security for the Enterprise Blind Spot at Black Hat 2019 and DEFCON 27

Las Vegas, August 7, 2019 – Karamba Security, a world leader in automotive and enterprise edge cybersecurity, will introduce the Connected Products Security Forum and showcase cybersecurity technologies in the exhibitor hall (Booth IC2116) at Black Hat USA in Las Vegas on August 7-8. Karamba will also host a traffic light challenge (CTF) at DEF CON 2019, also in Las Vegas, on August 8-11.

"Black Hat and DEF CON are the perfect settings to talk in-depth about the danger these IoT-enabled blind spots can pose to today's enterprises," said Ami Dotan, CEO and co-founder of Karamba Security. "Connectivity is unavoidable in today's world. But companies can – and should – protect themselves from the dangers posed to the corporate network and to business continuity by the thousands of now connected devices. Newly-connected end-points like printers, routers, IoT edge servers, VoIP equipment and smart TVs are all access points for attackers."

Karamba recently commissioned a study that found that 64% of respondents don't think IoT devices are protected, thus indicating the need for embedded cybersecurity in connected systems. During sessions and appearances at Black Hat and Defcon, Karamba will discuss how IoT edge "blind spots" pose security threats and how Karamba's embedded technologies can protect products from cyber-threats. The company will highlight its success in securing connected vehicles and how this same technology is now being used to to protect all types of connected systems.

The recent news (dubbed "Urgent 11") that older versions of VxWorks are vulnerable to Remote Code Execution – a threat to potentially hundreds of millions of devices - is a great example of the enterprise blind spot. At Black Hat, the Karamba Team will be happy to discuss how Karamba XGuard could prevent attackers from exploiting such vulnerabilities in the OS, application or 3rd party libraries.

Karamba Security provides product vendors with built-in Day 1 and Zero-Day protection against remote code execution and fileless attacks. Karamba's security solution is built into the device before it ever leaves the factory and doesn't require any security updates during its lifetime. Built-in, embedded security allows devices to protect themselves against cyber threats.

Also at Black Hat, Karamba will launch the "Connected Products Security forum." The forum is the first of its kind and it will allow security experts from across a wide range of industries to share and learn the unique challenges of product security and to work together to build best practices that will enhance the security of our connected world.

If you'd like to meet with Karamba at Black Hat, register for the CPS forum, or try the hacking challenge at DEF CON, register here.

About Karamba Security

Karamba Security provides industry-leading embedded cybersecurity solutions for connected systems. Product manufacturers in automotive, Industry 4.0, IoT, and enterprise edge rely on Karamba's automated runtime integrity software to self-protect their products against remote code execution (RCE) cyberattacks with negligible performance impact.

After 32 successful engagements with 17 automotive OEMs and tier 1s, product providers trust Karamba's award-winning solutions to increase their brand competitiveness and protect their customers against cyberthreats.

More information is available at www.karambasecurity.com and follow us on Twitter @KarambaSecurity.

Karamba Security Business Contact:
Amir Einav, VP of Marketing
amir.einav@karambasecurity.com
+1-214-620-7320

Karamba Security Media Contact:
PAN Communications,
Kyle Tildsley
Karamba@pancomm.com
+1-617.502.4300