



RunSafe Security CEO Joseph M. Saunders to Address U.S. Connected Vehicle Rule at Automotive Cybersecurity Summit 2026

DETROIT, MI, UNITED STATES, July 22, 2026 /EINPresswire.com/ -- As the automotive capital of the world races to secure next-generation [Software-Defined Vehicles \(SDVs\)](#), RunSafe Security, the pioneer in cyberhardening and embedded system protection, will deliver critical insights at the upcoming Automotive Cybersecurity Summit 2026.

With model year production lines facing stringent new federal compliance benchmarks, RunSafe Founder and CEO Joseph M. Saunders will lead a vital session on BIS Connected Vehicle compliance. He will address how OEMs and Tier-1 suppliers can navigate new international software origin restrictions and shift automotive compliance from a point-in-time check to a continuous lifecycle culture.

What / Scheduled Sessions:

- Solo Keynote: "Meeting U.S. Connected Vehicle Rule Origin Requirements"
- Context: Joe will discuss the Bureau of Industry and Security (BIS) Connected Vehicle Rule. He will share technical strategies to rapidly map code provenance, generate automated, compliance-ready [Software Bills of Materials \(SBOMs\)](#), and purge foreign-adversary-linked components from deep within multi-tier supply chains.

Who:

- Joseph M. Saunders, Founder & CEO, RunSafe Security
- Automotive OEMs, Tier-1 suppliers, security engineers, and transportation policy experts.

When: July 29 – 30, 2026

Where: DoubleTree Suites by Hilton Hotel Detroit Downtown - Fort Shelby, 525 W Lafayette Blvd, Detroit, Michigan, 48226

Why It Matters to the Detroit Automotive Ecosystem:

Recent consumer data from the [2025 Connected Car Cyber Safety & Security Index](#) reveals that 65% of drivers believe remote hacking of a vehicle is possible, while 77% explicitly identify third-party components as a severe cyber risk.

As automotive architectures grow more complex, scanning and patching legacy C/C++ code is no longer enough. RunSafe protects vehicle software by deploying patented memory relocation techniques that immunize embedded systems against runtime exploits without requiring code rewrites, directly answering the call for Secure by Design automotive engineering.

RunSafe also provides build-time SBOMs, which are uniquely capable of capturing components in automotive software that binary analysis and scanning miss. Most software composition analysis tools are optimized for open-source detection and perform well on known OSS packages, but provide limited insight into proprietary or commercial components—which are exactly what BIS cares about. Build-time SBOMs instrument the build itself, recording exactly which source files, libraries, and toolchains contributed to the output while that information is still clear. In automotive software, where static linking and aggressive optimization strip away identifying signals, this timing difference is critical for BIS compliance.

Media Opportunities:

Joseph Saunders will be available for brief one-on-one interviews, technical deep dives, and on-camera commentary regarding the local and global economic impacts of the U.S. Connected Vehicle regulations. Press credentials can be coordinated via the contact below.

Kari Ritacco
RedIron PR
+1 703-928-9996
Kari@RedIronPR.com

This press release can be viewed online at: <https://www.einpresswire.com/article/928356797>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.