The Auto-ISAC Launches Automotive Threat Matrix (ATM) Tool to Enhance Vehicle Cybersecurity Governance

Advancing Cybersecurity of the Connected Vehicle across the Industry

WASHINGTON, DC, UNITED STATES, March 27, 2024 /EINPresswire.com/ -- The Automotive Information Sharing and Analysis Center (Auto-ISAC), renowned for its leadership in automotive cybersecurity information sharing, introduces the Automotive Threat Matrix (ATM). This innovative initiative marks a significant leap forward in bolstering the assessment of automotive threats and risks, as well as the classification and sharing of cyber threat intelligence across the automotive industry.

Crafted by esteemed automotive security subject matter experts from Auto-ISAC's Member and Partner network, the Automotive Threat Matrix (ATM) represents a pioneering effort. Modeled after the acclaimed MITRE ATT&CK™ framework, ATM offers a standardized taxonomy meticulously tailored for automotive-specific adversarial cyber tactics and techniques.

“In the realm of automotive cybersecurity, shared understanding accelerates industry maturation and speed of response to cyber-attacks, both of which are vital to staying ahead of emerging threats," stated Kevin Tierney, Chair, Auto-ISAC, and Chief Cybersecurity Officer at General Motors. "ATM represents a significant advancement in our ongoing mission to enhance automotive cybersecurity governance, providing stakeholders with a standard taxonomy to communicate and act more effectively."

What Can It Do?

• Expedited Threat Intelligence: ATM accelerates the categorization of vehicle-specific threat intelligence, facilitating the swift identification of emerging attack techniques targeting vehicles.

• Streamlined Governance: ATM enhances all aspects of automotive cybersecurity governance, encompassing threat assessment, intelligence sharing, incident response, compliance reporting, and execution of penetration testing.

• Compliance Abstraction: ATM serves as a useful abstraction for compliance reporting, aiding in fulfilling automotive cybersecurity regulatory requirements such as UN Regulation 155 and current as well as future legislative requirements.

• Enhanced Threat Detection: ATM, based upon real-world attacker tactics and techniques, can help identify attack paths and inform the design of intrusion detection systems.

ATM is available online at https://atm.automotiveisac.com/

The Auto-ISAC was formed by automakers in August 2015 to establish a global information-sharing community to address vehicle cybersecurity, and operates as a central hub for sharing, tracking, and analyzing intelligence about emerging cybersecurity risks. Its secure intelligence-sharing portal allows members to anonymously submit and receive information that helps them more effectively respond to cyber threats.

Auto-ISAC's 2024 Europe Cybersecurity Summit is scheduled for June 11-13, 2024, hosted by BMW in Munich, Germany. To register or become a sponsor of the Summit, please visit 2024 Europe Cybersecurity Summit.

Auto-ISAC members represent more than 99 percent of light-duty vehicles on the road in North America. Members also include heavy-duty vehicles, commercial fleets, carriers, and suppliers. For more information, please visit www.automotiveisac.com and follow us @autoisac.

Michael Shokouhi
Auto-ISAC, Inc.
michaelshokouhi@automotiveisac.com
Visit us on social media:
Twitter
LinkedIn
