Tuesday, June 25, 2024

10:40 AM - 11:00 AM

Navigating the Risks: Strengthening DoD Supply Chains Against AI-Induced Vulnerabilities

Jeremy Newberry

Cyber Security Solutions Architect

Merlin Cyber

Abstract:

The rapid integration of Generative AI (GenAI) within the Department of Defense (DoD) presents novel vulnerabilities, particularly in the areas of supply chain management. This session will address the dual-edge nature of AI deployment in defense contexts, highlighting how the automation and data-processing capabilities of AI can inadvertently expose the DoD to new forms of cyber threats. Specifically, we will explore the unique risks that Generative AI introduces to the supply chain, including data poisoning, model theft, and adversarial attacks, which can all undermine the integrity and security of critical defense operations.

Our discussion will pivot to robust remediation strategies tailored to the defense sector's needs, emphasizing alignment with the Zero Trust architecture and the implementation of stringent NIST cybersecurity frameworks. We will outline advanced methodologies for auditing and monitoring AI systems within supply chains to detect and mitigate risks early. Further, the presentation will explore the deployment of decentralized ledger technologies (DLTs) to enhance transparency and traceability in AI-driven processes, thereby securing the provenance of data and AI models used across the DoD.