Wednesday, May 7, 2025
3:20 pm – 3:40 pm
Maneuvering the Domain: Deception-Enhanced Endpoint Defense for the Federal Enterprise

Rick Friend
Manager, Cybersecurity Solutions & Architecture
Merlin Cyber

Brian Recore
Cybersecurity Solutions Engineer
Merlin Cyber

Abstract:
Federal agencies face adversaries who increasingly bypass traditional EDR endpoint defenses by abusing techniques like syscall manipulation, credential harvesting, and Living-off-the-Land (LotL) binaries. These threats often operate under the radar, bypassing and exploiting traditional security control measures. While preventive controls remain essential, agencies must pair them with deception-based detection to impose costs on the adversary, buy time for defenders, and support timely corrective actions. This session focuses on how embedded endpoint deception—such as false credentials, decoy connections, and dissolvable identity traps—can expose malicious activity in real time and generate high-confidence alerts. Tailored for the mission needs of the Department of Defense and federal civilian agencies, the approach supports a layered defense strategy that enhances visibility, enables more agile response, and creates operational space to outpace the adversary.

Key Session Takeaways:

· Understand how attackers bypass EDR using techniques like syscall manipulation and credential harvesting—and why static defenses are no longer enough.
· Learn how endpoint deception enhances detection, using false credentials and decoy assets to expose attacker behavior without relying on signatures or agents.
· Explore agent and agentless deception technologies that adapt to each host without impacting performance or visibility.
· Discover how deception accelerates response, reduces dwell time, and supports faster, more confident deployment of corrective controls.