Wednesday, June 3

3:20 pm – 3:40 pm

From Automation to Autonomy: Governing Agentic AI in Defensive Cyber Operations

Jason Malnar

Lead Cybersecurity Solutions Architect

Merlin Cyber

Abstract:

DISA has identified a critical challenge: while agentic AI has the potential to transform defensive cyber operations, the industry lacks proven standards for interoperability, secure integration, and governance. Merlin Cyber addresses this gap with a lab-validated Autonomous SOC architecture that operationalizes agentic AI across real-world, multi-vendor environments.

This solution moves beyond rule-based automation by deploying an AI SOC analyst capable of ingesting threat intelligence, executing cross-platform threat hunts, enriching findings, assessing severity and blast radius, and generating response recommendations. In testing within a federal lab environment, the system reduced threat detection-to-response time from hours to under five minutes while decreasing analyst triage workload by up to 80%.

The architecture integrates multiple security platforms—including EDR, orchestration, threat intelligence, asset intelligence, and ITSM—through API-driven interoperability and a normalized data model. This enables agents to operate consistently across heterogeneous environments, including multi-EDR deployments.

To align with Zero Trust principles, all agent actions are governed through least-privilege access using scoped API credentials and strict tenant-level authorization boundaries. Autonomous actions are controlled through a Just-in-Time (JIT) human authorization gate, supported by a pre-defined action framework and AI-generated rationale for every recommendation. All decisions and actions are logged end-to-end, producing an auditable chain aligned to NIST 800-53 (AU, SI, IR) controls.

This session provides a practical, implementation-focused perspective on agentic AI—demonstrating how interoperability, authorization, and governance challenges can be solved today using commercially available technologies. Merlin Cyber's approach offers DISA a validated model for securely adopting agentic AI within high-stakes operational environments.