Wednesday, June 3

12:50 pm – 1:10 pm

AI-Driven Threat Detection at the Speed of the Network: A Live End-to-End Demo

Aaron Boteler

CTO

CloudCurrent

Evan Powell

Founding CEO

Deep Tempo

Abstract:

Modern adversaries move faster than signature-based and rule-driven defenses can react, and they move through networks: hybrid IT, OT, and cloud environments whose operational reality is invisible to most detection stacks. This session demonstrates how a fully integrated, AI-native detection and visualization pipeline closes that gap in real time, grounded in the network and operational picture that makes findings actionable.

Evan Powell (DeepTempo) and Aaron Boteler (CloudCurrent) walk attendees through a live demonstration running against a realistic simulated network environment purpose-built for this talk. DeepTempo's LogLM, a vertical foundation model trained exclusively on security telemetry, ingests raw telemetry from hybrid IT, OT, and cloud environments to produce high-fidelity behavioral findings such as reconnaissance, lateral movement, C2 activity, and exfiltration, without signatures, without rules, and without per-environment retraining.

Those findings are passed through CloudCurrent's VStrike fusion layer, which correlates them with network topology and multi-source telemetry to place every detection in its operational context: which assets, which segments, which mission systems, and which adversary pathways are actually in play. The enriched, network-aware findings are then surfaced through Vigil (vigilsoc.org), an open-source platform started by DeepTempo,

delivering fully interactive visualizations that let operators step through attack timelines, map activity to MITRE ATT&CK, and understand not just that an attack occurred but where on the network, how it propagated, and why it matters to the mission.

Attendees will leave with a clear picture of how AI-native detection, network-grounded fusion, and open cyber visualization combine into a practical, deployable stack that DoD and government cyber teams can evaluate, adopt, and extend today.

Key takeaways:

* How foundation models detect adversary intent, not just anomalies, across encrypted IT and OT traffic

* How the VStrike fusion layer grounds AI findings in network topology and operational context, turning detections into mission-relevant intelligence

* How open cyber visualization (Vigil) gives operators a continuous operational picture of adversary activity across the network

* A proven, deployable stack aligned with DISA and U.S. Cyber Command modernization priorities