Tuesday, June 2

3:20 pm – 3:40 pm

Dominate the Digital Disconnected Edge with Zero Trust and Identity Security

Andrew Whelchel

Lead Solutions Engineering - Federal

Saviynt

Abstract:

Deploying modern zero trust today demands more than just MFA and microsegmentation to meet today's mission at the disconnected edge. Zero Trust for accelerating the mission becomes an even greater challenge in a contested and disconnected environment, where the tyranny of distance (or just disconnection) stretches normally resilient systems to their limits. Identity security, when enabled with AI (artificial intelligence), enables scalable Zero Trust authorization access for users and non-person entities (NPEs) across connected and DDIL environments down to OT endpoints.

By delivering Zero Trust via AI-enabled identity security for C2 and joint all-domain operations missions, organizations gain benefits as they leverage identity security to enable missions and defend against cyber threats across disconnected and DDIL environments. These organizations reap mission benefits from device and user trust validation at the edge, mitigating contested security risks and ensuring mission continuity. These benefits result from using identity security with AI in the DDIL environment, enabling accelerated risk reduction and executing a compressed time-to-enforcement for zero-trust policies.

Delivering Zero Trust at the edge outcomes requires an identity security solution with an AI platform that is ready to deploy at the edge, can extend to edge OT endpoints, and operate using a rapidly deployable ICAM platform. When deployed with these key elements, they gain several capabilities, including:

- Enable distributed identity access using DDIL-enabled ICAM with AI-enabled identity security.

- Establish data and attribute-based edge policy enforcement for C2 and Joint All-Domain Operation mission applications.
- Provide continuous authentication service with strong MFA (using CAC where available) to sustain the mission while connected and disconnected.
- Assure auditability and deferred synchronization during disconnected state, as mission networks adapt and ensure safety and security before reconnection.

To ensure the mission at the edge's needs are met, identity security with AI must be delivered as an ICAM solution down to the person, NPE risk reduction, and OT edge cyber protection. When integrated and optimized, these elements will improve the speed of action for onboarding mission personnel and non-person entities and ensure data-centric protection of mission partner resources. These outcomes will be in addition to providing operational capability to ensure audit compliance even when disconnected, and information assurance before connecting to the enterprise network. As part of this session, attendees will learn about key capabilities, including accelerated identity security-based onboarding in a disconnected environment, managing data-centric edge policy enforcement, providing continuous authentication services with MFA when disconnected, and assuring audit requirements in any environment, connected or not.