Tuesday, June 25, 2024

2:20 PM - 2:40 PM

Accelerate your Generative AI using ZSP Identity Security to Reduce Risk and Speed the Mission

Andrew Whelchel

Senior Solution Engineer

Saviynt

Abstract:

At the speed of rapidly shifting AI models and data, the challenge remains for the joint mission on how to leverage generative AI in way to reduce risk and accelerate the mission. Generative AI, like machine learning and other AI models, depend on untampered data to ensure outcomes meet the needs of the mission. Risk further exists for outcome manipulation with improper access to models and training data pools.   To assure the success of the generative AI mission, identity security, particularly assurance of zero standing privilege, is crucial to the mission. Identity security when aligning with the generative AI tools and data ensure that the training data, models and AI response outcomes operate with reduced risk and speed of the mission. When employing zero standing privilege with generative AI systems, it empowers risk reduction for operators working with AI data and models as well as assures minimal access for NPE agents doing continuous deployment of the AI system.

This session will enable integration of zero standing privilege into generative AI environment to provide speed of access via governed service agent access and facilitate insider threat mitigation resulting in generative AI that is focused on the success of the joint mission.

Attendees of this session will learn and apply new capabilities including:

- Learn the approaches to apply zero standing privilege against service principals and other NPE agents for access enforcement and insider threat mitigation in Azure OpenAI environment.
- Develop methods for implementation controls for zero standing privilege using identity security in your generative AI environment.
- Experience demonstration of existing operational zero standing privilege capabilities protecting service principals to rapidly mitigate cyber and insider threat risks against Azure OpenAI and similar environments.