Tuesday, October 22, 2024

11:00 am - 11:20 am

Defend AI at the Hybrid DDIL Edge with ZSP Identity Security

Andrew Whelchel

Lead Solutions Engineering, Federal

Saviynt

Abstract:

The joint multi-domain environment in the pacific region carries new and more complex challenges. In meeting these challenges, defense organizations bring a new pace of AI innovation to mission systems at the edge faster than ever before. These AI capabilities, though offering potential for operational advantage, come with new risk challenges that must be addressed to maintain the drive at the speed of the mission. These AI mission assets when equipped with zero standing privilege (ZSP) identity security provides the operator the ability to mitigate the risk of AI at the edge while still leveraging that AI asset for operational overmatch.

Essential to the success of AI assets at the edge is not just about the execution of AI itself, but rather about application of ZSP identity cyber protection to the AI asset for maximum force multiplier impact. As part of the hybrid edge capability, the ZSP identity cyber protection ensures speedy and secure zero standing privilege access to accelerate AI at the edge while supporting disconnected (DDIL) scenarios.

Meeting challenges of AI cyber protection at the edge requires ZSP identity cyber protection with durable disconnected survivability (DDIL) that is available from cloud to the tactical edge. The ZSP identity security enables edge AI capabilities in the joint domain theater including:

• Provide access authorization to data sets, AI hyperparameters and AI analytics products operating at the tactical edge

• Enable cyber risk remediation through removal of access authorization due to cyber threat or end of mission

• Provide durable ICAM services enabling access to AI edge services and data even in

disconnected environments.

The capabilities included and described as part of this session include ZSP identity security capability details, DDIL ICAM architecture and operational use case scenarios to hasten the assurance of success of the edge AI mission.