

Wednesday, June 26, 2024

3:30 PM - 3:50 PM

Cybersecurity in the Age of AI: Fusing Zero Trust with Universal Confidential Computing

Dwayne Hoover

Vice President, Solutions Engineering

Anjuna Security

Abstract:

In an era marked by unprecedented data volumes and breakneck advancements in AI, government agencies face the dual challenge of harnessing this technology's unprecedented power while safeguarding sensitive information against never-ending and rapidly evolving threats.

This breakout session delves into the intersection of two cutting-edge concepts: Zero Trust Architecture and Universal Confidential Computing, offering insights into how they synergize to bolster the security posture of government AI initiatives. By adopting a Zero Trust – an approach that assumes that no entity, whether inside or outside the network, should be trusted by default – coupled with Universal Confidential Computing – a new technology category that offers cloud and application agnostic security and data privacy through a hardware-rooted trust – government agencies can establish a dominant security posture.

Join us as we explore practical strategies for implementing Zero Trust principles alongside Universal Confidential Computing to secure AI data processing and analysis workflows, ensuring data confidentiality, integrity, and privacy at every stage. Discover how this holistic approach empowers government organizations to embrace AI innovation with resilience, trust, and confidence, setting the stage for the future of the cyber mission.