Wednesday, June 3

9:00 am – 9:20 am

Beyond the API Key: Securing the Mission-Critical Shift to Autonomous AI

Brandon Iske

Principal Solutions Architect

Okta

Abstract:

As DoW races to integrate LLMs and autonomous agents into scientific workflows, traditional security is hitting a breaking point. Legacy API keys and manual OAuth flows weren't built for the speed of the mission—they create 'over-permissioned' risks that stall innovation and complicate audits in high-security environments.

This session introduces Cross App Access (XAA), an emerging identity-first standard that treats AI agents as first-class identities. By leveraging the Identity Assertion JWT Authorization Grant (ID-JAG) extension to OAuth 2.0, XAA replaces static permissions with dynamic, task-specific authority.

We will explore how a unified security fabric—integrating XAA with other industry standards like the Shared Signals Framework and Model Context Protocol (MCP)—dramatically reduces risk and time to respond to security challenges. Attendees will learn to eliminate the identity gap, ensuring that AI-driven discovery scales securely across the enterprise for both warfighters and their autonomous counterparts.