Wednesday, August 20, 2025

3:10 PM - 3:30 PM

Modernizing RMF Compliance Through Automation and Agentic AI

Johann Detweiller

CISO

stackArmor

Fawad Siraj

Co-Founder and CTO

stackArmor

Abstract:

Meeting RMF requirements under NIST SP 800-37 Rev. 2 remains a significant challenge for Army cybersecurity teams, often requiring manual, time-consuming documentation efforts and ongoing control validation across complex environments. These burdens not only slow down system authorization but also strain limited security resources post-deployment.

A modernized approach is emerging: one that integrates authorization artifacts as code, aligns with DevSecOps pipelines, and embeds compliance directly into infrastructure deployment. By automating the generation and maintenance of critical documentation—such as System Security Plans (SSPs) and control implementation statements—teams can reduce errors, increase traceability, and maintain alignment with evolving configurations.

Furthermore, the integration of agentic AI enables intelligent, continuous monitoring tasks across the system lifecycle, dramatically reducing the need for manual oversight or expanded workforce support. By autonomously validating system changes, performing real-time risk assessments, and generating audit-ready evidence, agentic AI minimizes the human effort required to maintain RMF compliance. This not only ensures sustained alignment with control baselines but also mitigates the need to hire additional personnel for routine compliance tasks. To build confidence and trust in agentic AI, its actions are fully traceable, auditable, and aligned with established RMF workflows—providing transparency and assurance to cybersecurity teams and authorizing officials. The result is a leaner, more efficient security operation that maintains readiness and compliance while allowing existing teams to focus on mission-critical objectives.