Tuesday, June 2

12:40 pm – 1:00 pm

Delivering Continuous ATO with Security Control Management

Kendall Moore

Co-Founder and CTO

Sicura

Abstract:

To counter fast-moving adversaries, security controls for mission-critical IT infrastructure must be continuously adapted to changes in the threat landscape, technology, and user actions. The federal government has traditionally relied on Authority to Operate (ATO) to keep pace with change, however, the process to obtain certification is often slowed by siloing between tools, fragmentation between security and DevOps teams, and over-reliance on manual workarounds to navigate the space between them. As teams navigate these challenges, the warfighter waits for delivery. Adding further challenges, systems often fall out of date in the three years between ATO exercises, increasing the risk of vulnerabilities and leaving warfighters unable to access the latest technology.

Security Control Management (SCM) provides a paradigm shift. By providing end-to-end compliance automation and integrating with key security and agile workflows, SCM transforms ATO certification from a static compliance exercise into a continuous cycle of enforcement, where the RMF becomes an agile workflow that delivers for the warfighter at the pace of the mission.

DevOps engineer Kendall Moore lived these challenges while obtaining ATO for complex infrastructure at NSA, and supporting key intelligence community contracts. These experiences led him to become the co-founder of Sicura, a platform purpose-built to deliver SCM in highly-secure environments.

In this talk, Moore will detail his lived experience navigating the back-and-forth between security and engineering teams that slowed down the ATO process, and the real-world consequences that slowed down delivery when mission engineers were prevented from working until ATO was complete.

Moore will also break down how SCM delivers Continuous ATO (cATO). Moore will cover key pillars of SCM and how these automate steps of the RMF. These include customizable security policies that map ATO requirements with specific system attributes, artifact delivery that integrates with DevOps workflows and existing GRC tools such as eMASS, automated remediation, continuous monitoring, and flexible deployment across hybrid and airgapped environments. Additionally, Moore will provide examples and outcomes from real use cases of cATO deployment, including with US Army DevCom.

Attendees will leave this talk with perspective on how cATO can accelerate certification timelines from months and years to days and weeks, while reallocating engineering labor toward mission critical problem solving. Moreover, they will have a framework to reset expectations for compliance as a process that hardens infrastructure every day, not only during certification exercises.