Thursday, August 21, 2025

9:00 AM - 9:20 AM

***AI-Driven Security Fortification and Attack Surface Reduction***

**Russ Andersson**

COO

RapidFort

Abstract:

AI is creating a multi-pronged software security challenge because it is being used to exploit software vulnerabilities, while at the same time, AI coding assistants are increasing the volume of software that must be defended. AI code is not inherently more insecure, merely the volume of it is significantly increasing code base sizes, quickly, often without adequate oversight, and thus increases attack surfaces, which leads to security risks and CVE exploitation. RapidFort's experience founding the concept and tooling enabling Flow Defending highlights four developments relevant to AI coding and its implications for AI:

AI Weaponization is Increasing the Threat Landscape: AI is increasing the rate, severity and volume at which software vulnerabilities can be exploited. Software vulnerability exploits have increased 400% year over year and are now the primary attack vector for cloud software. We will profile industry statistics that illustrate this trend.

Increased Volume & Velocity Code Releases

AI Vibe Coding is increasing the volume of code being developed, potentially overwhelming security teams. We will profile industry statistics that illustrate this trend.

Vulnerability Remediation Windows are Shrinking:

Because adversaries weaponize vulnerabilities in 72 days but companies patch in 45 days, this gap provides a window of opportunity responsible for 84% of breaches. Time is everything in cybersecurity.

The need for Flow Defending:

Flow defending is a term whereby security defenses are built into the software development workflow using highly automated, and often AI-based, tooling to protect and patch software before it gets deployed thus closing the software window. It is the complement to the so-called Vibe coding enabling AI-generated software to be secured rapidly. State-of-the-art tooling, often AI-based, is able to examine workloads to prioritize and remediate risks automatically.

To address these challenges, and the evolving AI driven threat landscape, RapidFort integrates AI-driven vulnerability intelligence directly into SDLC workflows, enabling teams to tame AI's output, focus on true mission-critical risks, and maintain a near-zero CVE state from code commit through live container runtime.