Tuesday, May 6, 2025
10:40 am – 11:00 am
An AI Application's Journey to Production: Software Supply Chain Fundamentals

Connor Wynveen
Solutions Engineer
Chainguard

Abstract:
Speed and security are often at odds. Early prototype efforts typically prioritize functionality to quickly demonstrate mission value. In an era with unprecedented access to data, data scientists and developers have an incredible ability to build applications that empower analysts and decision makers, support wargaming simulations, and address a plethora of other critical use cases.

Open-source software is ubiquitous, comprising roughly 80% of many application code bases. While these building blocks accelerate time-to-mission value, a significant majority of security vulnerabilities are found within them. This can lead to the misconception that open source is inherently insecure. But what if open-source software isn't fundamentally flawed—instead, the challenge lies in how we integrate and manage it?

This presentation will follow the lifecycle of a notional Retrieval-Augmented Generation (RAG) AI application, demonstrating how a few intentional choices and best practices can mean the difference between an application successfully fielded in production and one that gets trapped in a security risk reduction black hole. We will focus on the following software supply chain security fundamentals:

1. Using minimal, hardened, multi-stage container images: Learn how using minimal and hardened multi-stage container images can reduce known vulnerabilities (CVEs) by 90-99%

2. Dependency management: Explore current open-source consumption practices, the challenges they bring, and the solutions available today to mitigate these risks

3. Release cadence: Understand why regularly rebuilding your application is a critical capability and how establishing a consistent release cadence can drive both speed and security