C VISION INTERNATIONAL

AGENDA

The Innovation/Security Tradeoff: How to Defend the AI Software Supply Chain

Executive Dinner

Click Here to Register

THE INNOVATION/SECURITY TRADEOFF: HOW TO DEFEND THE AI SOFTWARE SUPPLY CHAIN

June 10, 2026
5:30 PM-9:00 PM
Eastern Time

AI is redefining how software gets built and how it's attacked.
Engineering teams are shipping more code than ever, with some engineers pushing 10–20 commits per day and AI tools pulling dependencies faster than any security review can keep pace. The productivity gains are real. So is the expanding attack surface that comes with it.
Threat actors have recognized this too. Recent AI-assisted attacks have shown how easily the supply chain can be compromised. In the case of Trivy, an open source vulnerability scanner was turned into a credential harvesting tool through a single malicious AI bot commit. The software supply chain is the target, and the attack surface is compounding with every sprint.
Join Chainguard and AWS for a closed dinner conversation on what a secure-by-default AI supply chain looks like across the SDLC, and what it takes to prevent malicious code from entering your production environment.

TOGETHER WITH

Chainguard aws