Tuesday, January 28, 2025

2:10 PM – 2:30 PM

The ABCs of Software Supply Chain Security: Starting with XZ and Finding the Y

Connor Wynveen

Solutions Engineer

Chainguard

Abstract:

The software supply chain faces increasingly sophisticated attacks, from malicious backdoors in critical open-source projects to exploited vulnerabilities in widely used dependencies. High-profile incidents like SolarWinds, Log4Shell, XZ, and the recent npm compromise underscore a troubling trend: hidden threats are becoming harder to detect and mitigate.

For years, security professionals in the federal industry have asked, “Can you determine whether open-source contributors are linked to adversary nations or known threat actors?” The XZ backdoor turned this fear into reality. While solving the challenge of verifying every contributor is daunting, the question remains: what can we do today to protect our software supply chains?

This session emphasizes getting the basics (the ABCs) of software supply chain security right. We’ll dive into practical strategies for building truly minimal container images – ensuring they are up-to-date, secure by default, and with a minimal attack surface – so your organization spends less time patching vulnerabilities and more time mitigating risks.