Wednesday, February 16, 2022
3:40 PM – 4:00 PM
An Imminent Need to Secure the Federal Software Supply Chain

Bryan Whyte
Technical Presales Manager
Sonatype

Abstract:
The security landscape for the US Government is changing. Government agencies are increasingly embracing the concept of DevOps — The walls between IT operations and developers are torn down, wasteful practices ripped out, and collaboration at scale rewarded.

Enter open source development practices powering DevOps, and more and more, powering federal software supply chains. These free and readily available open source components allow agencies to save time and money, and in many cases improve quality. In today's world, understanding what's in your supply chain is critical to national security and part of President Biden's recent Cybersecurity Executive Order. Not all components are created equal. Open source and DevOps can give the federal government the power to keep up with the commercial industry, but not without proper controls.

As government developers and contractors work towards digital modernization goals, they are consuming hundreds of billions of open source components and containerized applications to improve processes and catch-up with their commercial counterparts. The good news: they help create efficiencies and enhance innovation within the government. The bad news: many of the components and containers they are using are fraught with defects including critical security vulnerabilities.

We're in the middle of a paradigm shift in how the federal government develops software and addresses the security issues and there is an imminent need to secure the federal software supply chain, it's time to shift left.

Join this session to learn more about:

- Why the time is now to shift left

- Best practices for digital modernization

- Key Findings from The 2021 State of the Software Supply Chain Report