Wednesday, May 7, 2025
11:20 am – 11:40 am
DevSecOps - Operationalized

Rich Streeter
Operations Director
Sertainty Federal Systems

Abstract:
DevSecOps brings software developers' skills and talents into the cybersecurity fight, which is a significant step forward. However, there are two key challenges.

First, developers have historically been excluded from cybersecurity efforts because protections—both culturally and technologically—have been primarily network-centric. Second, most cyber threats target networks and, more specifically, the data they store. This raises an important question: If DevSecOps efforts were 100% successful, what percentage of total cybersecurity threats would be mitigated? If network security and application development tools remain static, the answer is: not much. However, moving beyond legacy toolsets opens up far more promising possibilities.

The most powerful tool for cybersecurity and data protection is cryptography. Traditionally, cryptography has been the exclusive domain of network and system engineers. Developers, on the other hand, work directly with the data that requires protection—utilizing, transforming, and creating it. A fundamental truth in computing is that protected data must be decrypted when applications use it. Once an application completes its tasks, the responsibility for securing both the input and output data falls back to network or system resources, where encryption is applied. In essence, developers control the data, while network administrators protect it.

The problem? There is currently no widely implemented encryption technology that allows cryptographic protection to be applied effectively within applications. If such a technology existed, a broader concept of DevSecOps—one where developers play a direct role in data security—would already be the norm. Sertainty’s innovation changes this dynamic by enabling developers to integrate cryptographic protections directly into applications, making data security a core part of DevSecOps.

If application developers could take responsibility for protecting the data their applications use—both inside and outside of those applications—it would bypass many systemic cybersecurity vulnerabilities. Sertainty's technology presents the first real opportunity for developers to bridge this gap.

Bottom line: If we want to empower the application development community to solve long-standing cybersecurity challenges, we must provide them with the right tools. Giving developers the ability to secure both the input and output data they handle is the ultimate goal of DevSecOps—and the key to stronger cybersecurity.