Wednesday, October 23, 2024

4:00 pm - 4:20 pm

Hitchhikers Guide to API Security for AI Based Apps

Paul Deakin

Principal Solutions Engineer

F5

Abstract:

As AI workloads increasingly rely on APIs for seamless integration and functionality, ensuring their security, monitoring, and discovery becomes critical. APIs serve as the backbone for data exchange, model deployment, and real-time decision-making in AI systems. However, this creates unique challenges across the DoD such as safeguarding sensitive data, mitigating potential attack vectors, and managing complex API ecosystems.

In this presentation, we will explore why DoD environments need robust API security measures, effective monitoring to ensure performance and compliance, and reliable discovery methods to track and manage evolving APIs in AI workflows, highlighting strategies to overcome these challenges.