Thursday, May 8, 2025
10:30 am – 10:50 am
Securing AI for National Defense: Mitigating Risks with the OWASP LLM Top Ten

Bill Church
Chief Technology Officer
F5

Abstract:

As the Department of Defense integrates AI into mission-critical operations, securing these workloads is no longer optional—it's imperative. This session explores the OWASP LLM Top Ten, the most pressing security risks facing AI-driven systems, and their implications for national security. Attendees will gain insights into real-world adversarial threats, supply chain vulnerabilities, and strategies for mitigating risks while maintaining operational effectiveness. Learn how to fortify AI deployments against manipulation, data poisoning, and prompt injection attacks to ensure AI remains a force multiplier rather than a liability.