BOSTON APPLICATION SECURITY CONFERENCE

The bearer of this certificate attended the following presentation on **Saturday, April 5, 2025, from 1:00 PM to 1:50 PM** at the Microsoft Technology Center, 5 Wayside Road, Burlington, MA 01803.

TALK - Analyzing Zero Trust Architecture in the Age of Agentic GenAI: A practical approach – Vineeth Sai Narajala
Agenda: The proliferation of generative artificial intelligence (GenAI) agents introduces unprecedented security challenges to modern organizations. As these autonomous systems increasingly generate content, make decisions, and execute actions with minimal human oversight, traditional perimeter-based security approaches prove inadequate. This paper examines the critical intersection of Zero Trust Architecture (ZTA) and GenAI agent deployment, proposing a framework for secure AI integration in enterprise environments. The rapid adoption of Generative AI (GenAI) presents unique security challenges that organizations must address while maintaining development velocity. This presentation provides practical strategies for building secure GenAI applications, with a focus on AWS services like Bedrock and Amazon Q. We introduce a comprehensive security framework that addresses three critical areas: threat modeling for GenAI systems, secure integration patterns, and robust output validation mechanisms. Through real-world case studies, we'll demonstrate how to identify and mitigate GenAI-specific vulnerabilities, including prompt injection attacks and data leakage risks. Attendees will learn concrete techniques for securing their entire GenAI pipeline, from input validation to output verification, with an emphasis on protecting sensitive information and preventing model hallucinations with an emphasis on speed and efficiency of the SDLC. The presentation includes hands-on examples of implementing security controls in GenAI applications, featuring code samples and architecture patterns that can be immediately applied.

Please retain this certificate as evidence of your attendance at this presentation and submit a claim for **ONE CPE CREDIT** in accordance with the guidelines of your certifying organization.