BOSTON APPLICATION SECURITY CONFERENCE

The bearer of this certificate attended the following presentation on **Saturday, April 5, 2025, from 10:00 AM to 11:00 AM** at the Microsoft Technology Center, 5 Wayside Road, Burlington, MA 01803.

TALK - Don’t Make This Mistake: Painful Learnings of Applying AI in Security – Eitan Worcel
Agenda: Leveraging AI for AppSec presents promise and danger, as let’s face it, you cannot do everything with AI, especially when it comes to security. At our session, we’ll delve into the complexities of AI in the context of auto remediation. We’ll begin by examining our research, in which we used OpenAI to address code vulnerabilities. Despite ambitious goals, the results were underwhelming and revealed the risk of trusting AI with complex tasks. Our session features real-world examples and a live demo that exposes GenAI’s limitations in tackling code vulnerabilities. Our talk serves as a cautionary lesson against falling into the trap of using AI as a stand-alone solution to everything. We’ll explore the broader implications, communicating the risks of blind trust in AI without a nuanced understanding of its strengths and weaknesses. In the second part of our session, we’ll explore a more reliable approach to leveraging GenAI for security relying on the RAG Framework. RAG stands for Retrieval-Augmented Generation. It's a methodology that enhances the capabilities of generative models by combining them with a retrieval component. This approach allows the model to dynamically fetch and utilize external knowledge or data during the generation process. Attendees will leave with a clear understanding of how to responsibly and effectively deploy AI in their programs — and how to properly vet AI tools.

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.