BOSTON APPLICATION SECURITY CONFERENCE

The bearer of this certificate attended the following presentation on **Saturday, April 5, 2025, from 11:00 AM to 11:25 AM** at the Microsoft Technology Center, 5 Wayside Road, Burlington, MA 01803.

TALK - Day in the Life of a Supply Chain Security Researcher – Derian Stenglein and Diptendu Kar
Agenda: We will walk through the steps that a Security Researcher takes to understand a vulnerability and write a Semgrep rule to provide the best possible coverage. We evaluate vulnerabilities affecting open source software packages and maintain and build tooling to enable our research. This session will present an overview of how we go from an advisory to a rule that will help catch actionable vulnerabilities in your code and the strategy behind that process.
1. Get in line, you pesky vulnerabilities - CVSS Scores, EPSS Scores, KEV Scores - How we prioritize vulns - What vulns we look at - Ingestion sources (GHSAs, OSV, etc) - Types of vulnerabilities (reachable, upgrade only, malicious)

2. Reviewing Advisories - Example of an advisory - What makes a good advisory - Example of an advisory with very little detail - What we pay attention to in an advisory

3. Let’s a write a rule together - Pick a vuln. Example: https://github.com/advisories/GHSA-qqv2-35q8-p2g2 - Analysis - Referenced patch links, source code, release notes, commit history, security advisories, function analysis, private vs public functions - Rule construction - Balancing general vs adding more specificity in the rule - Helper functions and automation for common patterns - Rule testing - Each rule has test code - How we prevent false positives, false negatives - How we get feedback for our rules - Rule metrics - Metabase dashboards

4. What’s next - BRAT - Rule automation Key Takeaways: - Methods for evaluating security vulnerabilities affecting open-source software packages - How a Security Researcher can write rules to enable users to prioritize fixing issues that matter - Strategies for prioritizing vulnerabilities

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.