BOSTON APPLICATION SECURITY CONFERENCE

The bearer of this certificate attended the following presentation on **Saturday, April 5, 2025, from 9:30 AM to 11:45 AM** at the Microsoft Technology Center, 5 Wayside Road, Burlington, MA 01803.

WORKSHOP - Riding the Snake With OpenDR: Detecting Living Off the Land Techniques in Python With a FOSS Tool – Craig Chamberlain and Anirudh Upadhyayula

Agenda: What do we call living off the land in Python? LOLmodules? There are numerous dual use modules such as the socket module which can import a shell. In Feb 2025, malicious code was found in a model published on HuggingFace and research was published on a novel method of embedding malware in an LLM model to be reconstituted by an execution payload using a serialization module. In both cases, the research trumpeted the claim that these were "undetectable" by AV or EDR tools. Why are these things undetected? How can we detect unexpected behavior in a Python IDE? Benign execution and network connection events are far too numerous to think about conventional alerting and the definition of what normal looks like, for any given codebase, is often in the head of the developer. In this workshop we introduce OpenDR, a lightweight FOSS EDR alternative for Windows and Linux implemented in Python. OpenDR generates logs of process, network and user events; running Windows services; installed software; and key information for threat hunting and detection including endpoint IP address, name and SIDs / GUIDs for positive identifications. It has two modes of operation; it can run in a stand-alone mode, for ad hoc monitoring or investigations, or it can ship logs to a database in a multi-agent deployment. . We will cover setup and deployment of both modes, local (and non-interrupting) alerting using toasters, and detection of an example reverse shell from a Python script. If you have additional examples of dual-use Python code you want to bring, we can include them in a threat hunting and detection engineering workshop using OpenDR data.

Attendees should come prepared with the following

1) A laptop with Anaconda, Postgresql and Beekeeper (a database client) installed, and a working Python instance, and VScode, or

2) a laptop with VMware Workstation or Fusion which can run a VM we provide. Such laptops should have at least 16 GB RAM and 100 GB free disk space.

3) Under Windows, having a D: drive is recommended to reduce the risk of filling up the C: drive in the event the EDR agents are left running for a long time and the C: drive is low on space.

4) You should have admin access on your laptop

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