Course Outline

Threat Hunting with Python

Course Summary

Description

Threat Hunting with Python teaches students how to take threat hunting hypotheses generated from contextual data or threat intelligence feeds, and then write Python scripts that interact with various data sources and perform data analytics to determine the validity of those hypotheses. Techniques include the use of advanced data structures, active data gathering using Scapy and other tools, scripting database or SIEM queries, and more. Successful students will gain the ability to script or automate a variety of custom threat hunting tasks and speed up their threat hunting processes.

Objectives and Topics

At the end of this course, students will be able to:

- Test cyber threat hunting hypotheses by creating Python scripts that perform data gathering and analytics.
- Use advanced data structures to store, search, and manipulate data.
- Write Python code to interact with a variety of systems such as SIEM platforms and endpoints, as well as static data sources such as log files and traffic captures.
- Increase the speed and effectiveness of cyber threat hunting activities through scripting and automation.

Audience

This class is geared towards security professionals and incident responders who will be using security and logging products to assist with their network and endpoint hunting responsibilities.

Prerequisites

Learners should have prior experience coding in Python and familiarity with programming concepts including object types, branching and control statements, simple data structures, file and command-line I/O, error handling, functions, and libraries. Learners should also have 1-2 years' experience in incident handling or cyber threat analysis before taking this class.

Duration

Three days