

Threat Hunting with Python Training

Applied Technology Academy

This intermediate-level course 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.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	5 Days	2 years: Python	\$137,500	Yes

Course Overview

Successful completion of this course will enable students to:

- Test cyberthreat 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

Improve the speed and effectiveness of cyberthreat hunting activities through scripting and automation

Course Outline

The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Click to view Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Collection Operations
- Cyber Defense Analysis
- Cyber Operations
- Capstone Exercise

A programming assignment that includes the use of data structures, file and user I/O, condition/branching statements, functions, and exception handling.

Intended Audience

Basic knowledge of TCP/IP networking Successful completion of Python for Security Professionals course

Prerequisites

- Intermediate-level programming experience with Python
- Successful completion of Network Forensics and Investigation II or comparable experience

Follow-on Courses

- Python for Network Automation
- Python for Reverse Engineers

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.