APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Security Onion Fundamentals for Analysts & Threat Hunters Training

Security Onion Authorized Training · Applied Technology Academy

Students should attend the free 2-hour Security Onion Essentials course before the first day of class. One topic covered by the Essentials course is building a Security Onion VM. Note that students do not need to build a Security Onion VM for this class. We will be using a pre-installed lab.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**4 Days**	**2 years: Agile**	**$150,000**	**Yes**

Course Overview

This hands-on course is geared for security analysts and threat hunters using the Security Onion 2 platform, with very light coverage of administration. Students will learn core analyst techniques and how to apply them using real-world case studies covering major analyst workflows.

- Agile Overview
- Agile Manifesto
- Agile Principles
- Agile Methods
- Scrum Overview
- Scrum Advantages

Course Outline

- Security Onion Console Overview
- Security Onion 2 Grid Architecture
- Basic Administrative Tasks Manage User Accounts
- Validate Grid Health
- Crucial Network Protocols and Host-Based Datasets
- (HTTP, SSL, DNS, Windows, Sysmon, etc.)
- Correlate Network and Host Data with Security
- Onion Console
- Discuss SOC Analyst Methodologies Key Elements of the Security Event Management
- Process Incident Escalation and Resolution
- Understanding the Analysis & Investigation Process
- Leveraging the MITRE ATT&CK Framework to
- Improve Threat Hunting

- Security Onion Analyst Workflows
- Alert Triage & Case Creation with Alerts and Cases
- Threat Hunting with Hunt and Dashboards
- Detection Engineering with Playbook
- Searching for Data in Security Onion
- Lucene
- Onion Query Language (OQL)
- Analyst Techniques Analyzing and Reconstructing Obfuscated
- Executables from Packets Finding Malicious Activity in Encrypted Traffic
- Detecting Hostile DNS Traffic (DNS tunneling, C2 over DNS, etc.)
- Tracking Adversary Activity Using Process
- Command Lines Identifying Anomalies Utilizing Network and Host
- Baselines
- Examining Data with CyberChef
- Visualizing Enterprise Data in Kibana
- Capstone Capture the Flag Event
- Multiple Labs and Case Studies

Intended Audience

Students should have a basic understanding of networks, TCP/IP, and standard protocols such as DNS, HTTP, etc. Some Linux knowledge/experience is recommended, but not required.

Prerequisites

- Security Onion Essentials at https://securityonionsolutions.com/training (2 hours; free)
- Should have a basic understanding of networks, TCP/IP, and standard protocols such as DNS, HTTP, SSL, etc.
- Knowledge/experience with Linux is recommended, but not required.

Follow-On Courses

Threat Hunting with Python

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.