APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Security Blue Team Level 2 (BTL2) Training

Centri Authorized Training · Applied Technology Academy

Master static and dynamic malware analysis, complex threat hunting, adversary emulation, and vulnerability management for mid-senior defenders and DFIR specialists.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Advanced	**6 Days**	**2+ years: Security Operations**	**$115,000**	**Yes**

Course Overview

This course provides Advanced Security Operations training, equipping experienced defenders with specialized skills across multiple disciplines. The certification focuses on techniques actively used by threat hunters and incident response teams, covering Malware Analysis, Threat Hunting, Vulnerability Management, and Advanced SIEM. Students will learn to conduct static and dynamic analysis, perform adversary emulation, and build proactive SIEM detections to reduce organizational risk effectively.

Course Outline

- **Module 1: Malware Analysis**
  - Setting up a Malware Analysis Home Lab
  - Static Malware Analysis (Header, Strings, Functions)
  - Dynamic Malware Analysis (Sandboxing, Debugging)
  - Assembly Language Fundamentals
  - Reverse Engineering - C Code Constructs
  - Advanced Analysis Techniques
  - Different Malware Types (Ransomware, Loaders, Backdoors)
  - Malware Analysis Practice Scenarios
- **Module 2: Threat Hunting**
  - Setting up a Threat Hunting Home Lab
  - Endpoint Threat Hunting (Processes, Registry, File System Artifacts)
  - Network Threat Hunting (Traffic Analysis, Protocols, Anomalies)
  - Hunting at Scale (Using centralized platforms)
  - Hunt Reflection and Report Writing
- **Module 3: Advanced SIEM**
  - SIEM Deployment (Architecture, Data Ingestion, Optimization)
  - Proactive SIEM (Building advanced correlation and detection rules)
  - Adversary Emulation (Simulating TTPs to validate SIEM coverage)

- **Module 4: Vulnerability Management**
  - Host Discovery and Asset Inventory
  - Vulnerability Discovery and Scanning
  - Analysis, Prioritization, & Threat Intelligence Integration
  - Reporting and Remediation Strategies

Intended Audience

- Mid-Senior Security Analysts
- Mid-Senior Incident Responders
- DFIR Specialists
- Threat Hunters, and Malware Analysts

Prerequisites

2+ years security experience

Follow-On Courses

PEN-200 (OSCP)

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.