APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Security Blue Team Level 1 (BTL1) Training

Centri Authorized Training · Applied Technology Academy

Become a certified Blue Team defender. This hands-on course teaches essential SOC and Incident Response skills, covering forensics, SIEM analysis (Splunk), phishing defense, and MITRE ATT&CK concepts.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**4 Days**	**1-2 year: Security Operations**	**$110,000**	**Yes**

Course Overview

BTL1 is designed to train technical security defenders capable of defending networks and responding to cyber incidents. The comprehensive skills and tools learned are directly applicable to a range of operational security roles (SOC, Incident Response, Forensics) and are actively used by defenders around the world. The course emphasizes practical application across multiple security domains.

Course Outline

- **Module 1: Security Fundamentals**
  - Soft Skills for Security Professionals
  - Security Controls Overview
  - Networking 101 (TCP/IP, Common Protocols)
  - Security Management Principles
  - Active Directory Fundamentals
- **Module 2: Phishing Analysis**
  - Types of Phishing Emails (Spear, Whale, Vishing, etc.)
  - Tactics and Techniques Used by Threat Actors
  - Investigating a Phishing Email (Headers, URLs, Attachments)
  - Analyzing Phishing Artifacts
  - Taking Defensive Actions and Reporting
  - Phishing Response Challenge
- **Module 3: Threat Intelligence**
  - Threat Actors and Advanced Persistent Threats (APTs)
  - Operational Threat Intelligence (TTPs and Incident Validation)
  - Tactical Threat Intelligence (IOCs and Automated Blocking)
  - Strategic Threat Intelligence (Risk and Executive Reporting)
- **Module 4: Digital Forensics**
  - Forensics Fundamentals and Chain of Custody

  - Digital Evidence Collection Techniques
  - Windows Investigations (Registry, Event Logs, Pre-fetch)
  - Linux Investigations (Log Files, Users, Shell History)
  - Memory Analysis With Volatility
  - Disk Analysis With Autopsy (File System and Artefact Analysis)
- **Module 5: Security Information and Event Monitoring (SIEM)**
  - Logging and Log Aggregation Principles
  - Correlation and Alerting Concepts
  - Using Splunk SIEM for Investigation and Querying
- **Module 6: Incident Response**
  - Preparation Phase and Documentation
  - Detection and Analysis Phase (Triage)
  - Case Management and Documentation
  - Containment, Eradication, and Recovery Phase
  - Lessons Learned and Reporting
  - Introduction to the MITRE ATT&CK Framework

Intended Audience

- IT Personnel
- Security Analysts
- Incident Responders
- Threat Intelligence Analysts
- Forensics Analysts

Prerequisites

1–2 years security experience

Follow-On Courses

Security Blue Team Level 2

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.