Security Blue Team Level 1 (BTL1)

Course Duration: 4 Days
Exam Reference: BTL1

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.

Prerequisites

0–2 Years Security experience

Course Objectives

Upon completion, you will be able to:

- Analyze and respond effectively to phishing attacks.
- Perform forensics investigations to collect and analyze digital evidence.
- Use a SIEM platform (Splunk) to investigate malicious activity.
- Conduct log and network traffic analysis to detect malware infections.
- Conduct threat actor research and apply threat intelligence operationally.

APPLIED TECHNOLOGY ACADEMY

Contact Us

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

Security Blue Team Level 1 (BTL1)

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