Security Blue Team Level 2 (BTL2)

Course Duration: 6 Days
Exam Reference: BTL2

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.

Prerequisites

2+ Years Security experience

Course Objectives

Upon completion, you will be able to:

- Identify, analyze, prioritize, and remediate vulnerabilities to effectively reduce risk.
- Conduct static and dynamic malware analysis to gather indicators of compromise (IOCs) and document malware techniques.
- Conduct adversary emulation activities to identify gaps in SIEM detection rules and create effective operational dashboards.
- Perform threat hunts on individual systems and at scale to detect adversaries that have already breached the perimeter.

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 2 (BTL2)

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 Artefacts)
- 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