Blue Team Level 1 (BTL1) Certification Study Guide

Incident Response

Understand the IR lifecycle: Preparation, Detection, Containment, Eradication, Recovery, and Lessons Learned. Practice responding to simulated attacks using tools like TheHive and Cortex.

Digital Forensics

Learn to analyze browser history, file metadata, and deleted files. Use tools such as FTK Imager, Autopsy, Scalpel, and JumpList Explorer.

Threat Intelligence

Research threat actors and indicators of compromise (IOCs). Utilize platforms like MISP, OpenCTI, VirusTotal, and DomainTools.

Phishing Analysis

Identify phishing emails and malicious attachments. Practice using tools like PhishTool and URL2PNG to analyze suspicious content.

SIEM & Log Analysis

Investigate logs using Splunk and Sigma rules. Analyze Windows Event Logs and Sysmon data to detect anomalies and threats.

MITRE ATT&CK Framework

Map attacker behavior to MITRE ATT&CK tactics and techniques. Understand how attacks progress through different stages of the kill chain.

Case Management

Document findings and manage investigations using platforms like TheHive5. Learn structured case tracking and reporting.

Blue Team Level 1 (BTL1) Certification Study Guide

Tools & Techniques

Familiarize yourself with PowerShell, ProcDump, Wireshark, KAPE, PECmd, and CyberChef for decoding and data manipulation.

Suggested 4-Week Study Plan

Week 1: Incident Response + SIEM Basics

Tools: Splunk, Sigma

Week 2: Digital Forensics + Phishing

Tools: Autopsy, PhishTool

Week 3: Threat Intelligence + ATT&CK Framework

Tools: MISP, VirusTotal

Week 4: Case Management + Final Review

Tools: TheHive, CyberChef