

Blue Team Level 2 (BTL2)

Proposed instructor-led schedule: 5 days |

Course Overview

Blue Team Level 2 is an advanced defensive security course for practitioners seeking deeper technical capability. The published syllabus is organised around four principal domains: Malware Analysis, Threat Hunting, Advanced SIEM, and Vulnerability Management. This proposed five-day schedule allocates time to these domains and provides an integration and reporting session; the provider's official syllabus and course materials remain authoritative.

Day-wise Breakdown

Day 1: Malware Analysis — Environment and Static Analysis

- Malware analysis objectives, workflow, and safe laboratory setup
- Static analysis of file headers, strings, and functions
- Identifying file characteristics and suspicious artefacts
- Introduction to executable structure and assembly-language fundamentals
- Tools and techniques for initial malware triage
- Guided static-analysis practice scenario

Day 2: Malware Analysis — Dynamic Analysis and Reverse Engineering

- Dynamic analysis using sandboxing and debugging
- Observing process, file-system, registry, and network behaviour
- Reverse-engineering fundamentals and C code constructs
- Advanced analysis techniques and behaviour interpretation
- Analysis of ransomware, loaders, backdoors, and other malware types
- Malware analysis practice scenario and findings report

Day 3: Threat Hunting

- Threat-hunting objectives, hypotheses, and investigation workflow
- Setting up a threat-hunting environment
- Endpoint hunting: processes, registry, and file-system artefacts
- Network hunting: traffic analysis, protocols, and anomalies
- Hunting at scale using centralised platforms
- Reflecting on hunt results and producing a hunt report

Day 4: Advanced SIEM

- SIEM deployment architecture and data ingestion
- Data sources, normalization, and platform optimisation
- Proactive SIEM and advanced correlation logic
- Building detection rules to identify suspicious activity
- Adversary emulation to simulate tactics, techniques, and procedures
- Using emulation results to validate SIEM coverage and identify gaps

Day 5: Vulnerability Management and Integrated Review

- Host discovery and asset inventory
- Vulnerability discovery, scanning, and validation
- Analysis and prioritisation of vulnerabilities
- Integrating threat intelligence into prioritisation decisions
- Reporting findings and recommending remediation strategies
- Integrated review: relate malware, hunting, SIEM, and vulnerability findings
- Document technical evidence, limitations, and recommended next steps