Blue Team Level 1 (BTL1)

Proposed instructor-led schedule: 5 days |

Course Overview

Blue Team Level 1 develops practical defensive cybersecurity skills for aspiring and junior security professionals. The published syllabus is organised around six domains: Security Fundamentals, Phishing Analysis, Threat Intelligence, Digital Forensics, Security Information and Event Management (SIEM), and Incident Response. This proposed five-day instructor-led schedule groups those domains for classroom delivery; it is a suggested timetable rather than a provider-prescribed daily schedule.

Day-wise Breakdown

Day 1: Security Fundamentals

- Introduction to defensive cybersecurity and blue-team roles
- Professional skills for security operations: communication, teamwork, problem solving, and time management
- Security controls: physical, network, endpoint, and email
- Networking fundamentals, OSI model, network devices, tools, ports, and services
- Port scanning concepts and review of network fundamentals
- Risk, policies and procedures, compliance, and security frameworks

Day 2: Phishing Analysis

- Phishing concepts, common techniques, and investigation workflow
- Email structure and analysis of email headers and message artefacts
- Analysis of suspicious links, URLs, attachments, and files
- Identifying indicators and assessing suspicious messages
- Documenting findings and determining appropriate escalation
- Scenario-based phishing investigation and review

Day 3: Threat Intelligence

- Threat intelligence concepts, purpose, and operational value
- Threat actors, campaigns, and common threat behaviours
- Indicators of compromise and threat intelligence sources
- Collecting, reviewing, and enriching threat information
- Applying intelligence to security investigations and defensive decisions
- Threat intelligence analysis exercise and findings summary

Day 4: Digital Forensics

- Digital forensics principles and investigative workflow
- Evidence identification, preservation, integrity, and documentation
- Windows artefacts and event evidence relevant to investigations
- File-system and user-activity artefacts
- Analysing forensic evidence to establish an event timeline
- Reporting findings and maintaining evidence traceability

Day 5: SIEM and Incident Response

- SIEM concepts, platforms, logging, and event collection
- Log aggregation, normalization, correlation, regular expressions, and SIEM rules
- Searching and analysing events, baselines, and behaviour profiles
- Network traffic and packet-capture analysis
- Incident response preparation, prevention, containment, eradication, and recovery
- Identifying malicious artefacts, root cause, and recovery considerations
- Lessons learned, documentation, metrics, and reporting