+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on September 10, 2026

Sign Up

Blue Team Level 2 Certification Training

5 days (35 hours)

Overview

Blue Team Level 2 (BTL2) is an advanced certification in defensive cybersecurity designed for professionals seeking to deepen their skills in investigation, threat detection, and incident response.

Our Blue Team Level 2 training will enable you to develop an advanced approach to operational defense by working on scenarios that closely mirror the situations faced by SOC and Blue Team teams.

You will learn to conduct in-depth investigations, implement threat hunting techniques, and analyze data from systems, networks, and security tools to identify signs of a compromise.

The training will also allow you to deepen your understanding of malware analysis, advanced use of SIEMs, and vulnerability management. You will learn to correlate the information collected to understand an attacker's actions and improve your organization's detection capabilities.

Our hands-on workshop will guide you step-by-step through a comprehensive investigation by combining event analysis, threat hunting, forensic investigation, and threat analysis.

This training prepares you to earn the Blue Team Level 2 (BTL2) certification by developing the technical and methodological skills necessary to conduct advanced investigations.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Conduct advanced investigations on compromised systems and environments
- Implement threat hunting techniques to actively search for threats
- Analyze behaviors and artifacts associated with malware
- Use a SIEM to correlate events and identify suspicious activity
- Assess vulnerabilities and understand how they are exploited in an attack scenario
- Prepare to take the Blue Team Level 2 (BTL2) certification exam

Target Audience

- Experienced SOC analysts
- Cybersecurity analysts
- Incident Responders
- Threat Hunters
- DFIR/forensic analysts
- Cybersecurity Consultants

Requirements

- Have some experience in security analysis, SOC operations, or incident response
- Familiarity with the fundamentals of Windows environments and their main system logs
- Proficiency in the basics of TCP/IP networks and common protocols
- Have some experience with log analysis and using a SIEM

Technical Prerequisites

- Access to an isolated lab environment dedicated to training
- Access to the Windows machines and analysis environments required for investigations
- Access to the SIEM and log sources used during the exercises
- Access to the malware analysis, threat hunting, and vulnerability management tools provided for the workshops
- A recent web browser and a stable Internet connection to access the labs

Blue Team Level 2 Training Curriculum

[Day 1 - Morning]

Certification framework and SOC methodology

- Overview of the Blue Team Level 2 (BTL2) certification and the skills assessed.
- Organization of the four domains: malware analysis, threat hunting, advanced SIEM, and vulnerability management.
- The investigation process, from initial qualification to reporting results.
- Prioritizing alerts, managing evidence, and constructing an incident timeline.

- Review of a compromise scenario and identification of expected deliverables for the exam.

[Day 1 - Afternoon]

Fundamentals of Advanced Investigation

- Collection and classification of indicators of compromise: hashes, domains, IP addresses, and host artifacts.
- Analysis of Windows events, processes, services, and persistence mechanisms.
- Analysis of network logs and DNS, HTTP, and authentication traces.
- Formulating investigative hypotheses and validating them by cross-referencing telemetry sources.
- Hands-on workshop: Analyzing a set of host and network logs to establish an initial timeline of the compromise.

[Day 2 - Morning]

Static malware analysis

- Security framework for handling a suspicious file in an isolated environment.
- Identifying the file type, its fingerprint, structure, and metadata.
- Search for strings, imports, resources, and artifacts useful for classification.
- Extraction of indicators and detection of obfuscation or evasion techniques.
- Creation and validation of YARA rules to characterize a malware family.

[Day 2 - Afternoon]

Dynamic Analysis and Malicious Behavior

- Setting up a detonation virtual machine and understanding containment principles.
- Monitoring processes, files, registry keys, scheduled tasks, and network connections.
- Analysis of command-and-control communications and identification of abnormal behavior.
- Correlating observed actions with MITRE ATT&CK tactics and techniques.
- Hands-on workshop: Perform static and dynamic analysis of a controlled sample, then document the indicators and observed behaviors.

[Day 3 - Morning]

Hypothesis-Driven Threat Hunting

- Principles of threat hunting and the difference between reactive detection and proactive hunting.

- Formulating hypotheses based on threat intelligence and adversary techniques.
- Selecting data sources: endpoints, identity, network, email, and cloud.
- Searching for weak signals, behavioral anomalies, and connections between events.
- Qualifying results, reducing false positives, and preparing response actions.

[Day 3 - Afternoon]

Investigation and Detection in SIEM

- Advanced search in a SIEM: filters, aggregations, joins, and correlations.
- Analysis of authentications, privilege escalations, lateral movement, and data exfiltration.
- Designing detection queries aligned with a compromise hypothesis.
- Documenting results and enriching alerts with context useful to analysts.
- Hands-on workshop: conducting a threat hunt in a SIEM based on a hypothesis related to lateral movement.

[Day 4 - Morning]

Advanced Detection and Continuous Improvement

- The lifecycle of a detection rule: requirements, data, logic, testing, and deployment.
- Writing and adapting Sigma rules to standardize detections.
- Evaluating detection coverage against MITRE ATT&CK.
- Reducing noise, adjusting thresholds, and setting alert prioritization criteria.
- Measuring operational effectiveness: data quality, coverage, and processing times.

[Day 4 - Afternoon]

Risk-Based Vulnerability Management

- Vulnerability management lifecycle: discovery, assessment, prioritization, remediation, and monitoring.
- Interpreting scan results and contextualizing CVSS scores.
- Taking into account exposure, exploitability, critical assets, and active threats.
- Developing a remediation plan and tracking security exceptions.
- Hands-on workshop: Prioritizing a set of vulnerabilities based on business risks and drafting a remediation plan.

[Day 5 - Morning]

Incident Report and Findings

- Structure of an investigation report tailored to certification requirements.
- Defining the scope, sources examined, timeline, and evidence collected.
- Presentation of indicators, attacker techniques, potential impacts, and confidence levels.

- Formulation of recommendations for containment, eradication, remediation, and detection.
- Critical review: technical accuracy, traceability of findings, and clarity for decision-makers.

[Day 5 – Afternoon]

Exam preparation simulation

- Summary of key areas and competencies for Blue Team Level 2 (BTL2).
- Time-management strategy for an extensive practical investigation.
- Selection of tools, logging of actions, and preservation of evidence.
- Self-assessment of knowledge gaps and individual preparation plan prior to taking the exam.
- Hands-on workshop: handling an end-to-end compromise scenario, analyzing evidence, and producing a summary report in the style of an exam.

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific professional knowledge or modern methods.

Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth operation of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.