Training: Centri
Blue Team Level 2 (BTL2)

CENTRI

TRAINING GOALS:

Advanced Security Operations training and certification covers Malware Analysis, Threat Hunting, Vulnerability Management, and Advanced SIEM and Emulation.

Why choose BTL2?

BTL2 is designed to strengthen technical defenders that already have experience and exposure to security operations. BTL2 will develop you in niche areas that make you stand out as an advanced defender. Below are some examples of the skills and experience you will gain.

- Identify, analyze, prioritize, and remediate vulnerabilities to effectively reduce risk.
- Conduct static and dynamic malware analysis to gather indicators of compromise and document details of the malware’s purpose and utilized techniques.
- Conducting adversary emulation activities with the purpose of identifying gaps in SIEM detection rules, creating operational dashboards to identify threats, and hunting on remote systems.
- Perform threat hunts on individual systems and at scale to detect adversaries that have already breached the perimeter.

Certified rewards

Once a student passes the practical exam and becomes BTL2 certified, they will receive a number of rewards for their hard work:

- Become Blue Team Level 2 certified for life
- BTL2 digital PDF certificate
- BTL2 Credly digital badge
- BTL2 printed certificate
- BTL2 silver challenge coin (gold if 90%+ is scored on first attempt)

Who is the course for?

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

BTL2 is aimed at security professionals with 2-4 years' experience in a practical role, but can be suitable for individuals with less experience provided they can commit to the intense training. Roles that we believe would benefit from this course include:

- Mid-Senior Security Analysts
- Mid-Senior Incident Responders
- Mid-Senior Security Consultants
- DFIR Specialists
- Threat Hunters
- Malware Analysts

CONSPECT:

- Malware Analysis
  - This section will develop your understanding of malware analysis, and will teach you how to use a range of tools to perform static and dynamic analysis on portable executables, portable documents, and Microsoft Office document filetypes.
    - Introduction to Malware Analysis
    - Setting up a Malware Analysis Home Lab
    - Static Malware Analysis
    - Dynamic Malware Analysis
    - Assembly Language
    - Reverse Engineering - C Code Constructs
    - Advanced Analysis
    - Different Malware Types
    - Malware Analysis Practice
- Threat Hunting
  - This section will develop your understanding of hunting, from generating a hypothesis and understand attacker techniques, to hunting on Windows and Linux systems, over the network, as well as at scale using frameworks such as GRR and Velociraptor.
    - Introduction to Threat Hunting
    - Endpoint Threat Hunting
    - Network Threat Hunting
    - Hunting at Scale
    - Hunt Reflection and Report Writing
- Advanced SIEM
  - The section will develop your understanding of SIEM, and will teach you how to build operational dashboards, conduct worthwhile emulation activities, and further your searching and analysis skills using Splunk.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Introduction to Advanced SIEM
- SIEM Deployment
- Proactive SIEM
- Adversary Emulation

- Vulnerability Management
  - The section will develop your understanding of vulnerabilities, and how to plan and execute vulnerability scans, triaging results using a risk-based approach, and having the most efficient impact on improving the security posture of the organization.
    - Introduction to Vulnerability Management
    - Host Discovery
    - Vulnerability Discovery
    - Analysis, Prioritization, & Threat Intelligence
    - Reporting and Remediation

- BTL2 Exam Preparation
  - This section provides you with all the information you need to feel comfortable starting your BTL2 certification exam.
    - Exam Details

REQUIREMENTS:

These are recommended, not required, prerequisites. It is advisable to complete BTL1 before enrolling in BTL2, but if you are confident in your abilities, you can jump straight in. BTL2 is designed for technical defenders with 2-4 years of experience in security operations. It aims to develop advanced skills in vulnerability management, malware analysis, adversary emulation, and threat hunting. While primarily targeted at experienced professionals, it can also be suitable for those with less experience who are willing to commit to intense training.

Difficulty level

CERTIFICATE:

Upon passing the BTL2 exam, you'll receive Blue Team Level 2 certification for four years, a BTL2 Acclaim digital badge, a printed certificate, a Blue Team Labs Online digital badge, and a silver challenge coin (gold if scoring 90%+ on the first attempt).

In the price you will get one BTL2 exam, which includes up to 72 hours to complete a practical assessment and submit a written report.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007