Training: Centri
Blue Team Level 1 (BTL1)

TRAINING GOALS:

BTL1 is our leading certification, designed to train technical defenders who can defend networks and respond to real-world cyber incidents. The skills and tools you learn apply directly to security roles and are used by defenders worldwide. In the past five years, more than 10000 students have earned BTL1, joining a global community of over 150000 learners, across 80+ countries, making it one of the most recognized and trusted blue team qualifications.

Why choose BTL1?

BTL1 goes beyond theory. Every lab, tool, and scenario is modelled on real incidents, so you learn to detect, investigate, and respond the way professionals do in live environments.

BTL1 develops practical capability across all core areas of cyber defense, giving you a wider skill base than courses focused only on SOC analysis. You'll gain experience in:

- Analyzing and responding to phishing attacks
- Performing forensics investigations to collect and analyze digital evidence
- Using a SIEM platform to investigate malicious activity
- Interpreting logs and network traffic to identify threats and malware
- Researching and profiling threat actors
- ... And much more

Certified rewards

Once a student passes the practical exam and becomes BTL1 certified, they will receive a number of rewards for their hard work:

- Become Blue Team Level 1 certified for life
- BTL1 digital PDF certificate
- BTL1 Credly digital badge
- BTL1 printed certificate
- BTL1 silver challenge coin (gold if 90%+ is scored on first attempt)

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

Who is the course for?

BTL1 is perfect for security enthusiasts or professionals that want to develop their practical defensive cyber skills. Roles that we believe would benefit from this course include:

- Students/IT Personnel
- Security Analysts
- Incident Responders
- Threat Intelligence Analysts
- Forensics Analysts

Whilst our content is aimed primarily at entry-level or junior roles, read our course syllabus to see if BTL1 is the right choice for you or your team!

CONSPECT:

- Security Fundamentals
  - This section covers the basics of information security, building a foundation for the rest of the course.
    - Introduction to Security Fundamentals
    - Soft Skills
    - Security Controls
    - Networking 101
    - Management Principles
    - Active Directory
- Phishing Analysis
  - This section will teach you how to combat phishing, from receiving a suspicious email through to taking defensive measures.
    - Introduction to Phishing and Emails
    - Types of Phishing Emails
    - Tactics and Techniques Used
    - Investigating a Phishing Email
    - Analyzing Artifacts
    - Taking Defensive Actions
    - Report Writing
    - Phishing Response Challenge

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Threat Intelligence
  - This section will cover everything from threat actors to attack motivations, the different threat intelligence disciplines, and global malware campaigns.
    - Introduction to Threat Intelligence
    - Threat Actors and APTs
    - Operational Threat Intelligence
    - Tactical Threat Intelligence
    - Strategic Threat Intelligence
- Digital Forensics
  - This section covers Windows, browser, and Linux-based artefacts that are useful for digital forensic investigations.
    - Introduction to Digital Forensics
    - Forensics Fundamentals
    - Digital Evidence Collection
    - Windows Investigations
    - Linux Investigations
    - Memory Analysis With Volatility
    - Disk Analysis With Autopsy
- Security Information and Event Monitoring
  - This section introduces you to the components of SIEM, and how to analyze logs during security investigations.
    - Introduction to SIEM
    - Logging and Aggregation
    - Correlation
    - Using Splunk SIEM
- Incident Response
  - This section prepares you to defend organizations and respond to cyber attacks effectively in a structured approach.
    - Introduction to Incident Response
    - Preparation Phase
    - Detection and Analysis Phase
    - Case Management
    - Containment, Eradication, and Recovery Phase
    - Lessons Learned and Reporting
    - MITRE ATT&CK Framework
- BTL1 Exam Preparation
  - This section provides you with all the information you need to feel comfortable starting your BTL1 certification exam.

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Exam Details
- Next Steps!

REQUIREMENTS:

BTL1 is suitable for security enthusiasts or professionals looking to develop practical defensive cyber skills. Ideal candidates include students, IT personnel, security analysts, incident responders, threat intelligence analysts, and forensics analysts. The course is primarily aimed at entry-level or junior roles and is designed to train technical defenders capable of protecting networks and responding to cyber incidents. The skills and tools taught are directly applicable to various security roles and are widely used by defenders globally.

Difficulty level



CERTIFICATE:

Upon passing the BTL1 exam, you'll receive lifetime BTL1 certification, digital and printed certificates, a Credly digital badge, and a silver challenge coin (or gold if scoring 90%+ on the first attempt).

In the price you will get one 24-hour practical incident response exam with immediate grading and feedback, and one free exam resit voucher.

ADDITIONAL INFORMATION:

What's included in the price?

The price includes 4 months of on-demand access to 330+ lessons, videos, activities, and quizzes, along with 23 browser labs providing 100 hours of access. You'll also get one 24-hour practical incident response exam with immediate grading and feedback, and one free exam resit voucher (additional resits can be purchased for each). Detailed feedback is provided for all exams to help you improve. Upon passing, you'll receive lifetime BTL1 certification, digital and printed certificates, a Credly digital badge, and a silver challenge coin (or gold if scoring 90%+ on the first attempt).

Lessons available in 9 languages with native text-to-speech (beta)

- English
- Polish
- German
- French
- Portuguese

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Italian
- Spanish
- Dutch
- Japanese

Note: the exams are available in English only.

How long is the access?

After gaining access to the course, you have 4 months on-demand access to the training material.

In summary, the BTL1 license includes:

- 4 months of access
- Approximately 40 to 50 hours to complete
- 330+ lessons, videos, activities, and quizzes, along with 23 browser labs
- 24-hour practical incident response exam with one free exam resit voucher (if needed)

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310