Blue Team Level 1 Certification (Standard)

Introduction to BTL1

✓ ~~Welcome to Blue Team Level 1!~~
4 Topics

✓ ~~Lab and Forum Access~~

SECURITY FUNDAMENTALS DOMAIN

✓ ~~Introduction to Security Fundamentals~~
1 Topic

✓ ~~Soft Skills~~
7 Topics

✓ ~~Security Controls~~
5 Topics | 1 Quiz

✓ ~~Networking 101~~
6 Topics | 1 Quiz

✓ ~~Management Principles~~
4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

✓ ~~PA1) Introduction to Emails and Phishing~~
7 Topics | 1 Quiz

✓ ~~PA2) Types of Phishing Emails~~
10 Topics | 2 Quizzes

✓ ~~PA3) Tactics and Techniques Used~~
12 Topics | 2 Quizzes

✓ ~~PA4) Investigating a Phishing Email~~
8 Topics | 2 Quizzes

✓ ~~PA5) Analysing URLs, Attachments, and Artifacts~~
8 Topics | 1 Quiz

PA6) Taking Defensive Actions
12 Topics | 1 Quiz

○ PA7) Report Writing
7 Topics | 1 Quiz

○ PA8) Phishing Response Challenge
3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

○ TI1) Introduction to Threat Intelligence
7 Topics

○ TI2) Threat Actors & APTs
6 Topics | 2 Quizzes

○ TI3) Operational Threat Intelligence
7 Topics | 1 Quiz

○ TI4) Tactical Threat Intelligence
7 Topics | 1 Quiz

○ TI5) Strategic Threat Intelligence
5 Topics | 1 Quiz

○ TI6) Malware and Global Campaigns
6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

○ DF1) Introduction to Digital Forensics
5 Topics

○ DF2) Forensics Fundamentals
10 Topics | 5 Quizzes

○ DF3) Digital Evidence Collection
8 Topics | 1 Quiz

○ DF4) Windows Investigations
3 Topics | 3 Quizzes

○ DF5) Linux Investigations
4 Topics | 2 Quizzes

○ DF6) Volatility
3 Topics | 1 Quiz

Exam Preparation

Blue Team Level 1 Certification (Standard) > Exam Preparation IN PROGRESS

BTL1 Certification Exam
EXAM PREPARATION

SBT BLUE TEAM LEVEL 1

This lesson will introduce you to the format of the BTL1 assessment exam, so you understand what you'll be doing during the 24 hours from when you start. We will have a Frequently Asked Questions (FAQ) section at the bottom of the lesson, so please check there before contacting us in case your question has already been answered.

This lesson is also designed to give you some useful tips and advice to prepare for the BTL1 exam so you can pass and become certified. Let's start with the basics, all students should have completed the entirety of the BTL1 training course, including reading the lessons, watching the videos, passing the knowledge tests, and participating in the practical activities. The whole purpose of the course is to prepare you for the exam, so make sure you're familiar with the content and the tools we have covered.

EXAM FORMAT

The BTL1 practical exam is 24 hours long, with up to 12 hours spent in our virtual lab environment performing security investigations, then up to 12 hours writing your report which must be submitted within 24 hours of starting the exam. Don't worry you won't be sat at your PC for 24 hours straight, that's just the maximum time you'll have access to the lab and submit your PDF report.

After 12 hours have passed you will no longer be able to connect to the lab and you will need to focus on completing the report template that we provide. This is the piece that will be hand-marked and graded, determining whether you have scored enough points to pass the exam and become BTL1 certified.

STARTING YOUR EXAM

You will be able to start your exam whenever you feel ready. Clicking on the 'Start Exam' button will open a new tab in your browser which includes your unique lab environment. Here's what happens next:

- **Step One –** Agree to the BTL1 Exam NDA and start your exam attempt.
- **Step Two –** Read the Instructions page within your exam environment, it will provide you with all of the information you need!
- **Step Three –** Perform security investigations. Your lab will automatically expire after 12 hours, but you can end it earlier if you believe you have done everything (you won't be able to reopen it!)
- **Step Four –** You will email your PDF report to exams@securityblue.team within 24 hours of starting your exam, and it will be hand-marked. If the report is even a second late you will automatically fail. Watch the clock!
- **Step Five –** You will receive feedback within 30 days, including whether you have passed or failed and your score percentage. You can resit after 14 days using your free resit voucher.

EXAM FEEDBACK

Within 30 days you will receive feedback on your exam report submission, and you will be notified if you have passed or failed via email. We will provide you with your exact score, and human-written feedback on your strong areas and weak areas so you can improve. We believe this is extremely important to train strong defenders.

IF YOU PASS THE EXAM

If you pass we'll contact you via email to verify your full name which will be printed on your physical certificate. If you have scored over 90% on the exam, and are eligible for the rare BTL1 gold challenge coin. We will also verify

○ DF7) Autopsy

● 4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

○ SI1) Introduction to SIEM

● 7 Topics | 1 Quiz

○ SI2) Logging

● 6 Topics | 2 Quizzes

○ SI3) Aggregation

● 2 Topics | 1 Quiz

○ SI4) Correlation

● 6 Topics | 1 Quiz

○ SI5) Using Splunk

● 5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

○ IR1) Introduction to Incident Response

● 8 Topics | 1 Quiz

○ IR2) Preparation Phase

● 10 Topics | 2 Quizzes

○ IR3) Detection and Analysis Phase

● 7 Topics | 4 Quizzes

○ IR4) Containment, Eradication, and Recovery Phase

● 5 Topics | 1 Quiz

○ IR5) Lessons Learned and Reporting

● 7 Topics

○ IR6) MITRE ATT&CK

● 13 Topics | 2 Quizzes

BTL1 EXAM

○ **Exam Preparation**

○ Using RDP and SSH

○ How to Start Your Exam

your home address so we can post your physical rewards including; certificate, challenge coin, and stickers!

IF YOU FAIL THE EXAM

Don't worry – the exam is challenging and not everyone will pass the first time. As mentioned above we will give you personal feedback so that you're aware of areas needing improvement, allowing you to go away and study again to prepare for round 2. When you're ready to go again (but not within 14 days of failing), you can start the exam again. All students have 1 free resit voucher, if you fail a second time you will need to purchase a resit voucher for £150.

EXAM TIPS

Below are a number of tips that you should follow, giving you the best chance of scoring highly in the exam and becoming certified.

- **Don't Rush –** Seriously, slow down and think things over. It's easy to rush into things, but this means you may miss obvious information which is crucial to the exam scenario.
- **… But Don't Go Slow Either –** Remember you have 12 hours of access to the exam lab, so make sure you aren't going to be busy and that distractions will be to a minimum. This is more that enough time to complete your investigations, but keep an eye on the clock.
- **Make Sure you Have Good Notes –** If you don't already, go back and take notes from the course, this will make it a lot easier than having to find specific information while you are running through the exam. It's a good idea to note down how to use tools and any related commands, but remember that cheatsheets exist online!
- **Read the Exam Brief. No, Seriously, Read it –** The whole point of this information, which you'll be able to view on the sidebar in your lab environment, is to gently guide you through the scenario and tell you what information you need to collect. It will introduce you to the entire scenario so that you understand what's happened, and what needs to be done.
- **Also Read the Report Template –** This is what you'll be submitting to us for marking, make sure you understand what information you're being asked to collect, and take lots of notes while going through the exam so that you don't forget any important information.
- **SCREENSHOTS, ALL OF THE SCREENSHOTS! –** Screenshots are a great way of recording information. When you're going through the exam, take screenshots of important information so that you can look at it even after your lab access expires. Screenshots are also very useful in your report template! Make sure they are cropped to only highlight the important information, and explain what you are showing after or before using a screenshot.
- **Five Domains –** The exam is designed to test your knowledge and practical ability across all five of the BTL1 domains. We aren't going to ask you to complete tasks involving knowledge or tools that we haven't covered, so again, make sure you're familiar with the course content and you'll be fine.

‹ Previous Lesson | Mark Complete ✓ | Next Lesson ›

Back to Course