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 | 2 Quizzes
- TI5) Strategic Threat Intelligence — 5 Topics | 1 Quiz
- TI6) Malware and Global Campaigns — 6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

Lab and Forum Access

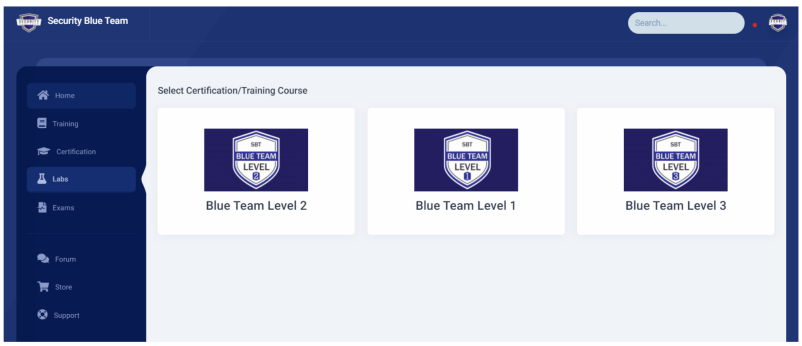
BTL1 is split into four main elements:

- **The Training Course** *(you're here!)*
- **The Student Forum**
- **Our Cloud Labs**
- **And the BTL1 Exam Lab**

While the training course is hosted here at securityblue.team, the labs are hosted at our new site at elearning.blueteamlabs.online! We have plans to migrate our training courses to the new site, but for now, students must access both resources. Our new and improved student forum allows students to ask questions, help each other, and get support from SBT Student Advisors. We will cover how to access this new platform below.

GAINING ACCESS

We have whitelisted the email address you're currently using for your SBT account, so you just need to register at https://elearning.blueteamlabs.online/register and you'll immediately see BTL1 when selecting the 'Labs' tab. If have an issue with registering, please reach out to us via email at contact@securityblue.team.

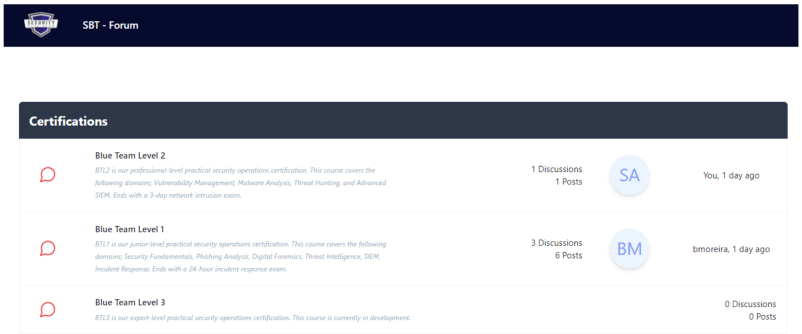


BTL1 STUDENT FORUM

We have an improved student forum also running on the same platform, allowing students and SBT staff to communicate. If you are experiencing an issue, this should be one of the first places you look to get an answer quickly. We believe having an open place for discussion about BTL1 lessons and labs is a great opportunity for students to network (pun intended), and help each other out.

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
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 | 3 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 5 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

On the new platform simply go to the 'Forums' page and you'll be able to read and write posts.



BTL1 BROWSER LABS

During the course, some lessons are used as placeholders for labs on our new platform. They will include the name of the lab and a link to access it – you may be required to log in if you do not already have an active session.

Blue Team Level 1 Certification (Standard) < DF6) Volatility < Volatility Walkthrough < Lab) Memory Analysis In...

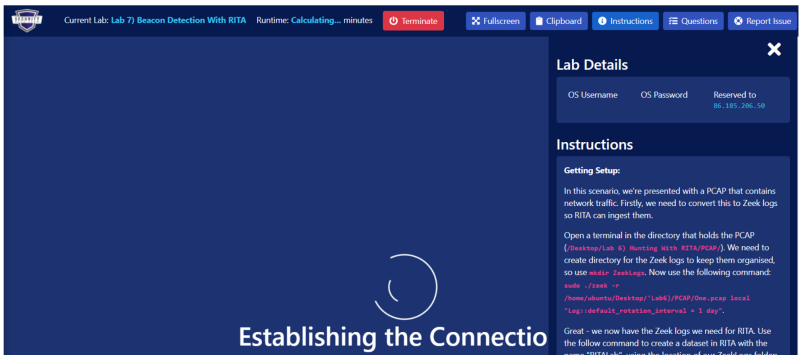
This lesson corresponds with a lab on the SBT eLearning platform. You can click the button below to open the lab platform in a new browser tab.

(Coming 26th) **Launch Lab Platform**

All the information you need will be available to you in the lab, including instructions and questions that you must answer to complete the activity.

Once you have completed the lab you can mark this lesson as complete below!

Instructions on what steps to take and questions to answer will all be included in the lab client, on the "Instructions" and "Questions" tabs as shown below:



All BTL1 students have 100 hours of lab time available to them for free. Based on our testing, this is more than enough time to complete the exercises however, we understand that some students may need or want to spend more time in our labs. To accommodate this, we offer the ability to purchase additional lab time via the platform store for a small fee.

Previous Lesson

Back to Course

Next Lesson

Privacy & Cookies Policy

Privacy - Terms