

Blue Team Level 1 Certification
(Standard)

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

How to Start Your Exam

Blue Team Level 1 Certification (Standard) > How to Start Your Exam

IN PROGRESS

Blue Team Level 1 Exam
START YOUR EXAM

The new and improved BTL1 exam is LIVE on our new platform!

If you have already taken this current exam, you must re-sit the old version to ensure that your feedback is still related to the scenario. Please contact us at contact@securityblue.team to take your re-sit exam and become certified.

If you have not yet taken any BTL1 exams, you can take the new exam available on <https://elearning.securityblue.team>. The new exam is ONLY accessible by students that have used 0 exam attempts.

Find more details about moving to the new website here:
<https://securityblue.team/migration/>

< Previous Lesson

Mark Complete ✓

Back to Course

