

**Blue Team Level 1 Certification
(Standard)****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

☐ Section Introduction, Splunk☐ Splunk Crash Course - Navigating Splunk☐ Splunk Crash Course - Search Queries☐ Splunk Crash Course - Creating Alerts☐ Splunk Crash Course - Creating
Dashboards☒ Lab) Splunk Investigation 1☐ Lab) Splunk Investigation 2**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

Lab) Splunk Investigation 1

Blue Team Level 1 Certification (Standard) > SI5) Using Splunk > Lab) Splunk Investigation 1



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.

[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!

If you have completed the lab on the elearning platform, then you can mark this lesson as complete by answering the question below.

☐ Mark lesson as complete[Finish Quiz](#)[Privacy & Cookies Policy](#)