Blue Team Level 1 Certification (Standard)

○ 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

○ Section Introduction, Logging
○ What is Logging?
○ Syslog
○ Windows Event Logs
Lab) Event Log Analysis
○ Sysmon
○ Other Logs
Activity) End of Section Review, Logging

○ SI3) Aggregation
● 2 Topics | 1 Quiz

○ SI4) Correlation
● 6 Topics | 1 Quiz

○ SI5) Using Splunk
● 5 Topics | 2 Quizzes

Lab) Event Log Analysis

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