Blue Team Level 1 Certification (Standard)

○ 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

○ Section Introduction, Detection & Analysis
○ Common Events & Incidents
○ Using Baselines & Behavior Profiles
○ Introduction to Wireshark (GUI)
○ Introduction to Wireshark (Analysis)
Lab) Network Traffic Analysis
○ YARA Rules For Detection
Legacy Activity) Threat Hunting With YARA
○ CMD and PowerShell For Incident Response
Lab) CMD and PowerShell
Activity) End of Section Review, Detection & Analysis

○ IR4) Containment, Eradication, and Recovery Phase
● 5 Topics | 1 Quiz

○ IR5) Lessons Learned and Reporting

Lab) Network Traffic Analysis

Blue Team Level 1 Certification (Standard) > IR3) Detection and Analysis Phase > Introduction to Wireshark (Ana...

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

Privacy - Terms