

Blue Team Level 1 Certification
(Standard)

<

IR1) Introduction to Incident Response

8 Topics1 Quiz

IR2) Preparation Phase

10 Topics2 Quizzes

IR3) Detection and Analysis Phase

7 Topics4 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 Topics1 Quiz

IR5) Lessons Learned and Reporting

7 Topics

IR6) MITRE ATT&CK

13 Topics2 Quizzes

BTL1 EXAM

Exam Preparation

Lab) CMD and PowerShell

Blue Team Level 1 Certification (Standard) > IR3) Detection and Analysis Phase > CMD and PowerShell For Incid...

Incident Response

CMD AND POWERSHELL

SBT

BLUE TEAM

LEVEL

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.

Access 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!

Once you have finished the lab, you can mark this lesson as complete.

Mark Lesson as Complete

Finish Quiz

Privacy & Cookies Policy