

Blue Team Level 1 Certification
(Standard)☐ 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☒ 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,

Section Introduction, Detection & Analysis

Blue Team Level 1 Certification (Standard) > IR3) Detection and Analysis Phase > Section Introd...

IN PROGRESS



This section of the IR domain will cover how incidents are detected via different tools such as SIEM and IDPS, and how potential and confirmed incidents are analyzed via log and PCAP analysis to gather indicators of compromise which can be used in threat exposure checks and shared with other organizations.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Understand common events and incidents faced by organizations.
- Understand what baselines are, and how they can be used to detect unusual behavior from users, systems, and network traffic.
- Understand and perform log analysis and PCAP analysis.

[Previous Lesson](#)[Mark Complete](#) ✓[Back to Lesson](#)[Next Topic](#) >