Blue Team Level 1 Certification (Standard)

● 10 Topics | 5 Quizzes

○ DF3) Digital Evidence Collection

● 8 Topics | 1 Quiz

○ 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

Section Introduction, Logging

Blue Team Level 1 Certification (Standard) > SI2) Logging > Section Introduction, Logging IN PROGRESS

This section of the SIEM domain will introduce you to logging, and how systems are able to report activity to the SIEM so that activity can be aggregated and normalized so that alerts can be generated when suspicious or abnormal activity is detected anywhere across the environment.

Managing logs effectively with your SIEM tool is essential for network visibility, compliance, and reliable incident detection and response. You as a security practitioner need the ability to ask questions of your data (usually using structured query language or SQL) to identify Indicators of Compromise (IoCs), find the users and systems affected, and share the final scope with remediation teams. Managing logs usually involves indexing data and correlating it with other data sets. The end goal is to give you an easy way to search for threats from one unified dashboard.

LEARNING OBJECTIVES

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

- Understand what logging is, and why it's used by security teams.
- Understand a range of log sources and log types.
- Understand the importance of syslog for security purposes.

< Previous Lesson

Mark Complete ✓

Next Topic >

Back to Lesson