

**Blue Team Level 1 Certification  
(Standard)****DIGITAL FORENSICS DOMAIN**☐ DF1) Introduction to Digital Forensics

5 Topics

☐ DF2) Forensics Fundamentals

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

☒ [Section Introduction, SIEM](#)☐ Security Information Management (SIM)☐ Security Event Management (SEM)☐ What is a SIEM?☐ SIEM Platforms☐ Further Reading Material, SIEM☐ SIEM Glossary☐ Activity) End of Section Review, SIEM☐ SI2) Logging

6 Topics 2 Quizzes

# Section Introduction, SIEM

Blue Team Level 1 Certification (Standard) &gt; SI1) Introduction to SIEM &gt; Section Introduction, SIEM

**IN PROGRESS**

In the first section of the SIEM domain, we're going to cover the history of SIEM, and how the two components, SIM and SEM, come together to provide a platform that allows central logging for an organizations assets so that security analysts can identify and respond to security events and suspicious behaviour on specific systems and across multiple networks in one panel.

## LEARNING OBJECTIVES

By the end of this section of the SIEM domain, you will be able to:

- Understand what Security Information Management (SIM) is, and how it features within SIEM.
- Understand what Security Event Management (SEM) is, and how it features within SIEM.
- Understand what SIEM is, and how it's used by security teams to aggregate, correlate, and normalise logs from a wide range of sources such as proxies, firewalls, IDPS, anti-virus, EDR, and various system logs.

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