Blue Team Level 1 Certification (Standard) ‹

○ 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
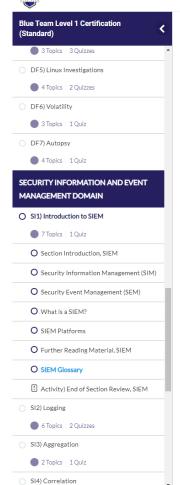
○ SI3) Aggregation

○ 2 Topics | 1 Quiz

○ SI4) Correlation

SIEM Glossary

Blue Team Level 1 Certification (Standard) > SI1) Introduction to SIEM > SIEM Glossary   **IN PROGRESS**

We have created a PDF that contains all of the terms and phrases used in this domain of Blue Team Level 1. While we work to ensure we declare full names of acronyms before they're used in a lesson, this document may help you remember them better and make studying easier. This PDF can either be viewed digitally or printed.

[Download BTL1_SIEM_Glossary.pdf]

‹ **Previous Topic**   **Mark Complete** ✓

Back to Lesson