

**Blue Team Level 1 Certification
(Standard)**☐ 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

6 Topics 1 Quiz

☐ SI5) Using Splunk

5 Topics 2 Quizzes

INCIDENT RESPONSE DOMAIN☐ IR1) Introduction to Incident Response

8 Topics 1 Quiz

Activity) End of Section Review, SIEM

Blue Team Level 1 Certification (Standard) > SI1) Introduction to SIEM > Activity) End of Section Review, SIEM



Congratulations on completing this section of the SIEM domain! This knowledge review is designed to test what you have learned about SIEM fundamentals. You will be able to re-take the quiz as many times as you like, but will need a score of 70% or above to pass. It is important that you feel confident answering these questions to ensure that you can complete tasks within the BTL1 exam and pass to become certified. If you get stuck, use the **Hint** feature!

Good luck!

KNOWLEDGE REVIEW

[Question 1/3] What does SIEM stand for?

Check

[Privacy & Cookies Policy](#)