Blue Team Level 1 Certification (Standard)

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

○ 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

○ Section Introduction, Correlation

○ Normalization and Processing

○ SIEM Rules

○ Sigma Rules

○ Regex

○ Activity) Writing Sigma Rules

Activity) End of Section Review, Correlation

○ 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

○ IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz

○ IR5) Lessons Learned and Reporting

Activity) End of Section Review, Correlation

Blue Team Level 1 Certification (Standard) > SI4) Correlation > Activity) End of Section Review, Correlation

Congratulations on completing this section of the SIEM domain! This knowledge review is designed to test what you have learned about SIEM normalization and correlation. 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] Using Amazon Web Services (AWS) S3 Buckets can be utilised for log storage in the cloud, true or false?

○ True

○ False

Check