



# Activity) End of Section Review, Aggregation

Blue Team Level 1 Certification (Standard) > SI3) Aggregation > Activity) End of Section Review, Aggregation



Congratulations on completing this section of the SIEM domain! This knowledge review is designed to test what you have learned about log aggregation. 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 1/2]** Logs can be sent from log sources to a Syslog server where they are stored. SIEM log aggregators can read and process Syslog data, true or false?

☐ True

☐ False

Check

Privacy & Cookies Policy



### Blue Team Level 1 Certification (Standard)

0 Topics 0 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

☒ SI3) Aggregation

2 Topics 1 Quiz

☐ Section Introduction, Aggregation

☐ Log Aggregation Explained

☒ Activity) End of Section Review, Aggregation

☐ 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

☐ IR2) Preparation Phase

10 Topics 2 Quizzes

☐ IR3) Detection and Analysis Phase

7 Topics 4 Quizzes

☐ IR4) Containment, Eradication, and Recovery Phase