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