CERTSinside

Free Questions for SC-200 by certsinside

Shared by Vargas on 29-01-2024

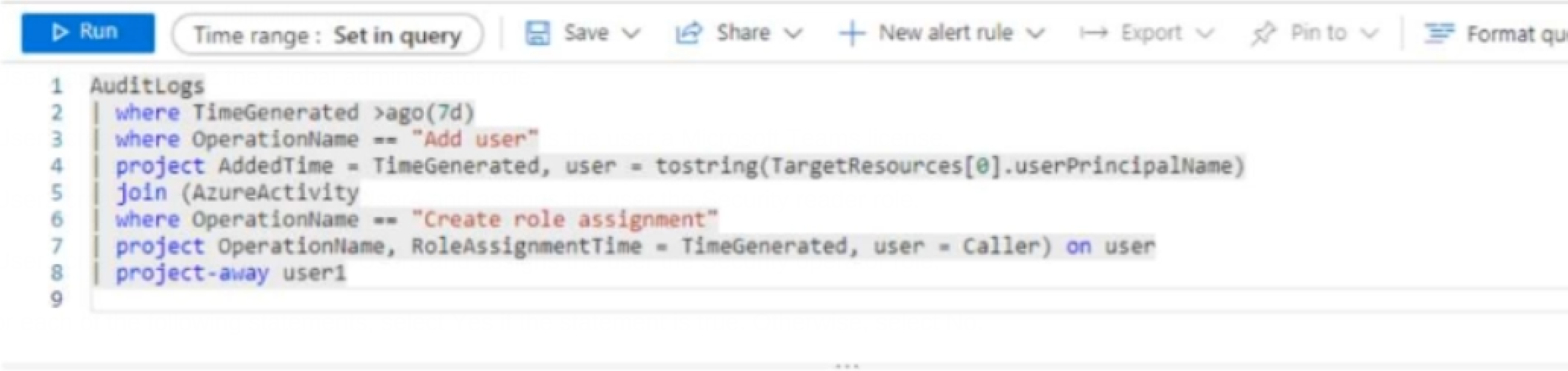
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: Hotspot

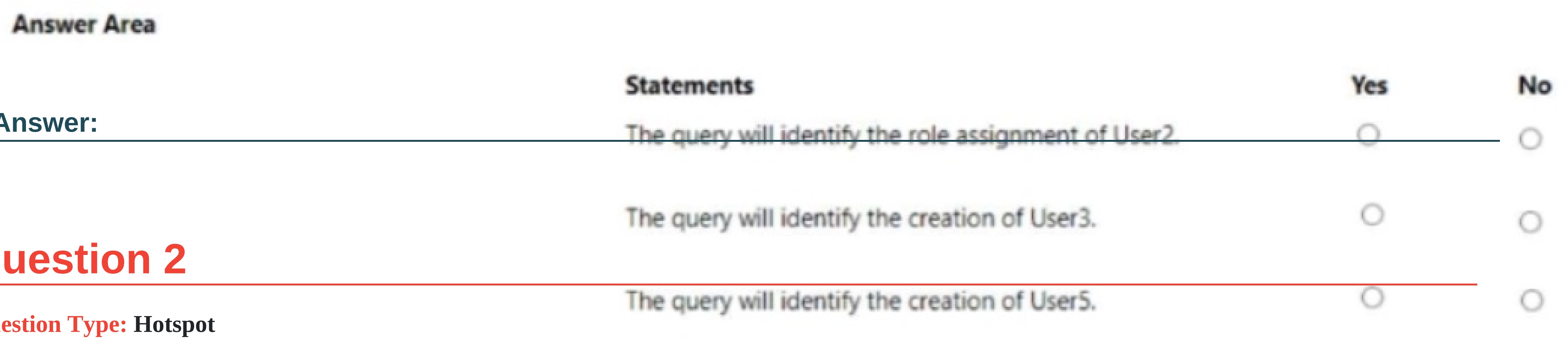
You have a Microsoft 365 E5 subscription that contains two users named User! and User2. You have the hunting query shown in the following exhibit.



```
AuditLogs
| where TimeGenerated >ago(7d)
| where OperationName == "Add user"
| project AddedTime = TimeGenerated, user = tostring(TargetResources[0].userPrincipalName)
| join (AzureActivity
| where OperationName == "Create role assignment"
| project OperationName, RoleAssignmentTime = TimeGenerated, user = Caller) on user
| project-away user1
```

NOTE: Each correct selection is worth one point.

Answer:



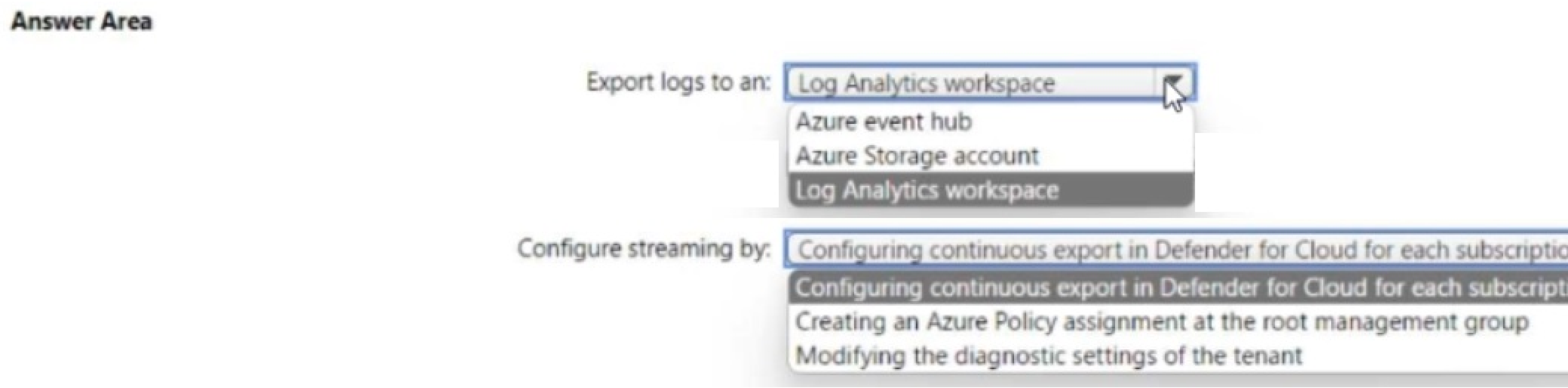
Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	○	○
The query will identify the creation of User3.	○	○
The query will identify the creation of User5.	○	○

Question 2

Question Type: Hotspot

You have 100 Azure subscriptions that have enhanced security features m Microsoft Defender for Cloud enabled. All the subscriptions are linked to a single Azure AD tenant. You need to stream the Defender for Cloud togs to a syslog server. The solution must minimize administrative effort What should you do? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point



Answer Area

Export logs to an: Log Analytics workspace

Azure event hub
Azure Storage account
Log Analytics workspace

Configure streaming by: Configuring continuous export in Defender for Cloud for each subscriptio

Configuring continuous export in Defender for Cloud for each subscript
Creating an Azure Policy assignment at the root management group
Modifying the diagnostic settings of the tenant

Answer:

Question 3

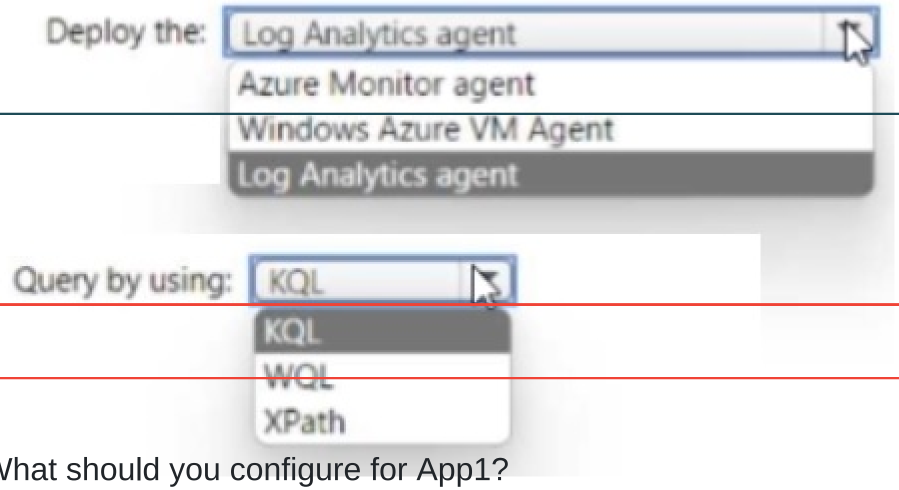
Question Type: Hotspot

You need to meet the Microsoft Sentinel requirements for collecting Windows Security event logs. What should you do? To answer, select the appropriate options in the answer are

a. NOTE Each correct selection is worth one point.

Answer Area

Answer:



Deploy the: Log Analytics agent

Query by using: KQL

Question 4

Question Type: MultipleChoice

You need to meet the Microsoft Sentinel requirements for App1. What should you configure for App1?

Options:

A- an API connection

B- a trigger

C- an connector

D- authorization

Answer:

B

Question 5

Question Type: MultipleChoice

You need to identify which mean time metrics to use to meet the Microsoft Sentinel requirements. Which workbook should you use?

Options:

A- Analytics Efficiency

B- Security Operations Efficiency

C- Event Analyzer

D- Investigation insights

Answer:

C

Question 6

Question Type: MultipleChoice

You need to correlate data from the SecurityEvent Log Anarytks table to meet the Microsoft Sentinel requirements for using UEB

Options:

A- Which Log Analytics table should you use?

A- SentwlAuoNt

B- AADRiskyUsers

C- IdentityOirectoryEvents

D- Identityinfo

Answer:

C