Free Questions for SC-200 by certsdeals

Shared by Strickland on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: Hotspot

You have on-premises servers that run Windows Server.

You have a Microsoft Sentinel workspace named SW1. SW1 is configured to collect Windows Security log entries from the servers by using the Azure Monitor Agent data connector.

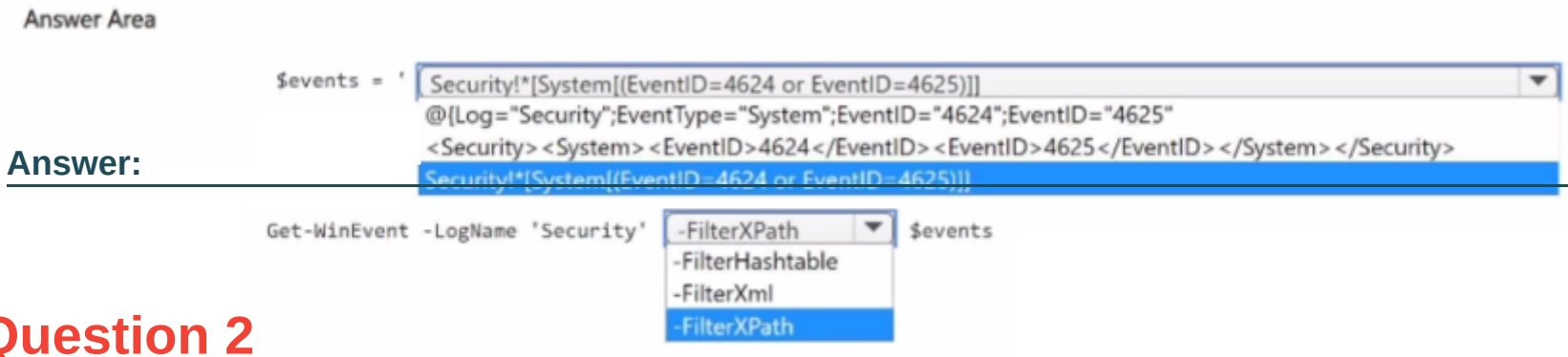
You plan to limit the scope of collected events to events 4624 and 462S only.

You need to use a PowerShell script to validate the syntax of the filter applied to the connector.

How should you complete the script? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Question 2

Question Type: MultipleChoice

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR and contains a user named User1.

You need to ensure that User1 can manage Microsoft Defender XDR custom detection rules and Endpoint security policies. The solution must follow the principle of least privilege.

Which role should you assign to User1?

Options:

A- Desktop Analytics Administrator

B- Security Operator

C- Security Administrator

D- Cloud Device Administrator

Answer:

C

Question 3

Question Type: **DragDrop**

You have a Microsoft Sentinel workspace that contains the following Advanced Security Information Model (ASIM) parsers:

* _Im_ProcessCreate

* InProceessCreate

You create a new source-specific parser named vimProcessCreate.

You need to modify the parsers to meet the following requirements:

* Call all the ProcessCreate parsers.

* Standardize fields to the Process schema.

Which parser should you modify to meet each requirement? To answer, drag the appropriate parsers to the correct requirements. tach parser may be used once, more than once, or not at all You may need to drag the split bar between panes or scroll to view content.

NOTE Each correct selection is worth one point.

Answer:

Question 4

Question Type: **Hotspot**

You have a Microsoft 365 subscription

You need to identify all the security principals that submitted requests to change or delete groups. How should you complete the KQL query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
MicrosoftGraphActivityLogs
| where [RequestUri ▾] contains '/group'
| where RequestMethod != ["GET" ▾]
| project AppId, UserId, ServicePrincipalId
```

RequestUri (selected)
Scopes
Type

"GET" (selected)
"POST"
"PUT"

Answer:

Question 5

Question Type: MultipleChoice

You have a Microsoft 365 subscription that uses Microsoft Defender XDR.

You are investigating an attacker that is known to use the Microsoft Graph API as an attack vector. The attacker performs the tactics shown the following table.

Name	Tactic
Tactic1	Conditional Access policy reconnaissance
Tactic2	Mailbox reconnaissance
Tactic3	Invites guest users to the tenant

You need to search for malicious activities in your organization.

Which tactics can you analyze by using the MicrosoftGraphActivityLogs table?

Options:

A- Tactic? only

B- Tactic1 and Tactic2 only

C- Tac1ic2 and Tactic3 only

D- Taclic1. Tac1ic2. andTactic3

Answer:

B

Question 6

Question Type: **MultipleChoice**

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan Z and contains 1,000 Windows devices.

You have a PowerShell script named Script Vps1 that is signed digitally.

You need to ensure that you can run Script1.psl in a live response session on one of the devices.

What should you do first from the live response session?

Options:

A- Run the library command.

B- Run the putfile command

C- Modify the PowerShell execution policy of the device.

D- Upload Script1.ps 1 to the library.

Answer:

D