SC-200$^{Q\&As}$

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add each account as a Sensitive account.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

QUESTION 2

You have a custom analytics rule to detect threats in Azure Sentinel.

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

A. There are connectivity issues between the data sources and Log Analytics.

B. The number of alerts exceeded 10,000 within two minutes.

C. The rule query takes too long to run and times out.

D. Permissions to one of the data sources of the rule query were modified.

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

QUESTION 3

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed.

You need to simulate an attack on the virtual machine that will generate an alert.

What should you do first?

A. Run the Log Analytics Troubleshooting Tool.

B. Copy and executable and rename the file as ASC_AlertTest_662jfi039N.exe.

C. Modify the settings of the Microsoft Monitoring Agent.

D. Run the MMASetup executable and specify the -foo argument.

Correct Answer: B

Simulate alerts on your Azure VMs (Windows)

After the Log Analytics agent is installed on your machine, follow these steps from the computer where you want to be the attacked resource of the alert:

1.

Copy an executable (for example calc.exe) to the computer\\'s desktop, or other directory of your convenience, and rename it as ASC_AlertTest_662jfi039N.exe.

2.

Open the command prompt and execute this file with an argument (just a fake argument name), such as: ASC_AlertTest_662jfi039N.exe -foo

3.

Wait 5 to 10 minutes and open Defender for Cloud Alerts. An alert should appear.

Reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/alert-validation

QUESTION 4

You have an Azure subscription that uses Microsoft Sentinel.

You detect a new threat by using a hunting query.

You need to ensure that Microsoft Sentinel automatically detects the threat. The solution must minimize administrative effort.

What should you do?

A. Create a playbook.

B. Create a watchlist.

C. Create an analytics rule.

D. Add the query to a workbook.

Correct Answer: C

By creating an analytics rule, you can set up a query that will automatically run and alert you when the threat is detected, without having to manually run the query. This will help minimize administrative effort, as you can set up the rule once and it will run on a schedule, alerting you when the threat is detected.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-rule

QUESTION 5

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You need to configure the continuous export of high-severity alerts to enable their retrieval from a third- party security information and event management (SIEM) solution.

To which service should you export the alerts?

A. Azure Cosmos DB

B. Azure Event Grid

C. Azure Event Hubs

D. Azure Data Lake

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal