SC-200 Q&As

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/sc-200.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You need to visualize Microsoft Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC). What should you use?

A. notebooks in Microsoft Sentinel

B. Microsoft Defender for Cloud Apps

C. Azure Monitor

Correct Answer: A

To visualize Azure Sentinel data and enrich it by using third-party data sources to identify indicators of compromise (IoC), you can use notebooks in Azure Sentinel.

Notebooks in Azure Sentinel are interactive documents that allow you to run queries, create visualizations, and perform data analysis on your Azure Sentinel data. They also allow you to connect to other data sources, such as third-party

threat intelligence feeds, to enrich the data and identify indicators of compromise (IoCs).

Once you have connected to the third-party data source, you can use Azure Sentinel notebook to blend the data, and create visualizations, and perform data analysis to identify the potential attack.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/notebooks

QUESTION 2

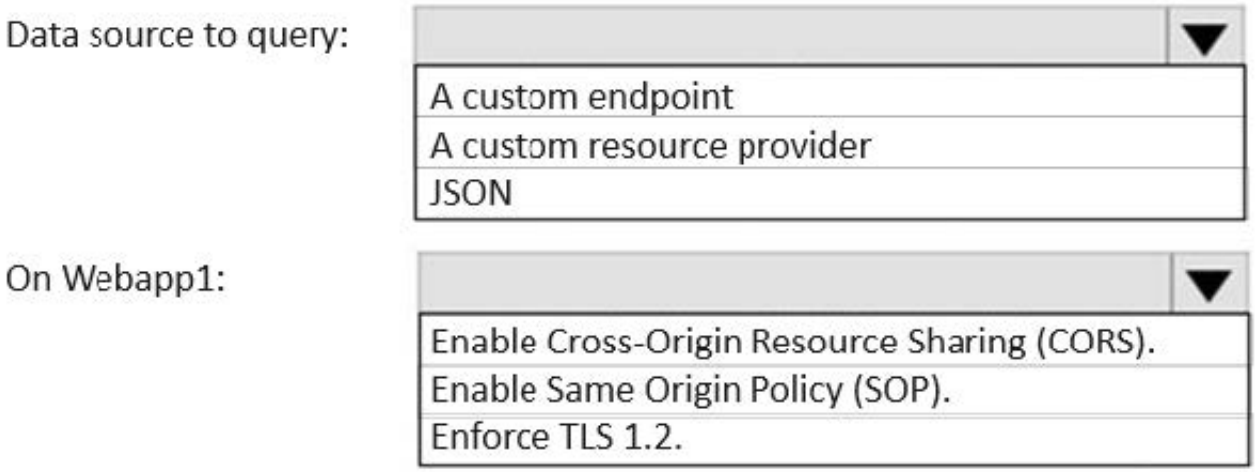
HOTSPOT

You need to implement the query for Workbook1 and Webapp1.

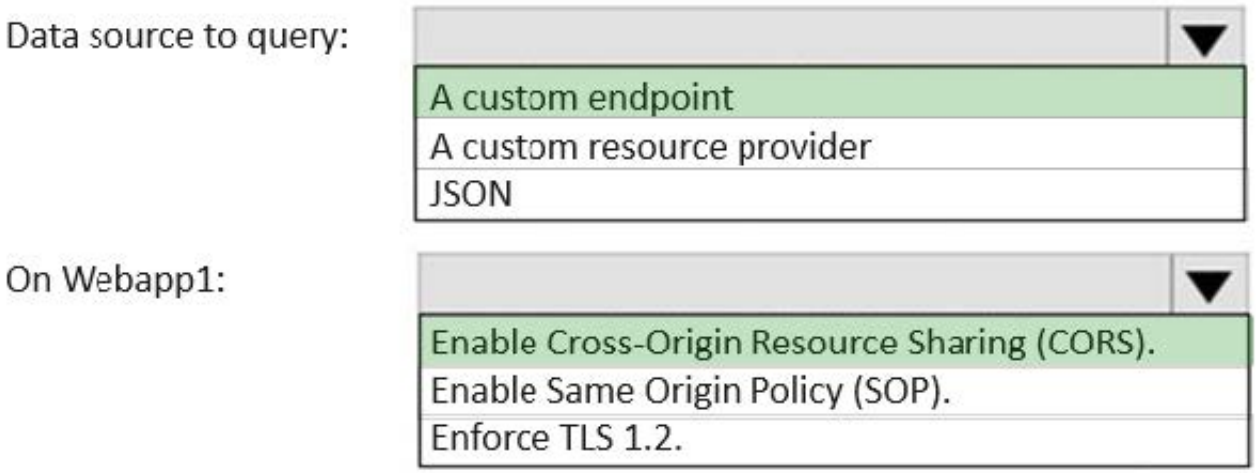
The solution must meet the Microsoft Sentinel requirements.

How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



QUESTION 3

You have an on-premises network.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Identity.

From the Microsoft Defender portal, you investigate an incident on a device named Device1 of a user named User1. The incident contains the following Defender for Identity alert.

Suspected identity theft (pass-the-ticket) (external ID 2018)

You need to contain the incident without affecting users and devices. The solution must minimize administrative effort.

What should you do?

A. Disable User1 only.

B. Quarantine Device1 only.

C. Reset the password for all the accounts that previously signed in to Device1.

D. Disable User1 and quarantine Device1.

E. Disable User1, quarantine Device1, and reset the password for all the accounts that previously signed in to Device1.

Correct Answer: E

QUESTION 4

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 5

You create a hunting query in Azure Sentinel.

You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.

What should you use?

A. a playbook

B. a notebook

C. a livestream

D. a bookmark

Correct Answer: C

Use livestream to run a specific query constantly, presenting results as they come in.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/hunting