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.pass2lead.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

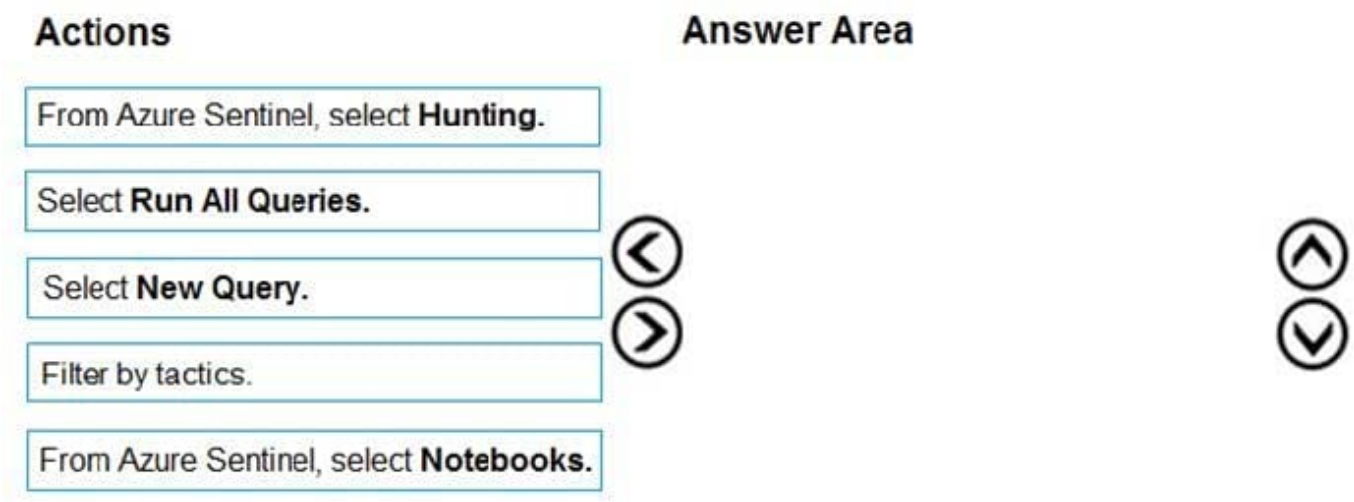
DRAG DROP

You have an Azure Sentinel deployment.

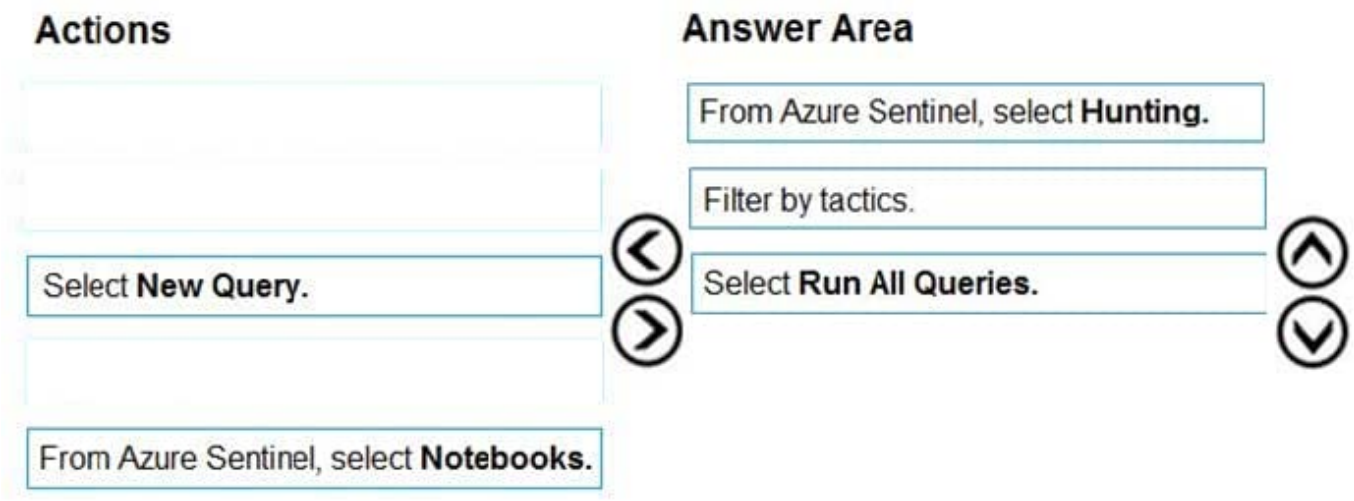
You need to query for all suspicious credential access activities.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Reference: https://davemccollough.com/2020/11/28/threat-hunting-with-azure-sentinel/

QUESTION 2

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a livestream

B. Add a data connector

C. Create an analytics rule

D. Create a hunting query.

E. Create a bookmark.

Correct Answer: BD

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

QUESTION 3

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

A. Modify the access control settings for the key vault.

B. Enable the Key Vault firewall.

C. Create an application security group.

D. Modify the access policy for the key vault.

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

QUESTION 4

You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. cp /bin/echo ./asc_alerttest_662jfi039n

B. ./alerttest testing eicar pipe

C. cp /bin/echo ./alerttest

D. ./asc_alerttest_662jfi039n testing eicar pipe

Correct Answer: AD

Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux-

QUESTION 5

You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

A. just-in-time (JIT) access

B. Azure Defender

C. Azure Firewall

D. Azure Application Gateway

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/security-center/azure-defender