# **Microsoft**

SC-200 Exam

## **Microsoft Security Operations Analyst**



Thank you for Downloading SC-200 exam PDF Demo

You can Buy Latest SC-200 Full Version Download

https://www.certkillers.net/Exam/SC-200

teams? view=o365-worldwide

# Version: 4.0

Question: 1	
The issue for which team can be resolved by using Microsoft Defe	nder for Endpoint?
A. executive	
B. sales	
C. marketing	
Explanation:	Answer: B
Reference:	
https://docs.microsoft.com/en-us/windows/security/threat-proteatp/microsoft- defender-atp-ios	ection/microsoft-defender-
Question: 2	
The issue for which team can be resolved by using Microsoft Defe	nder for Office 365?
A. executive	
B. marketing	
C. security	
D. sales	
	Answer: B
Explanation:	Allswer: B
Explanation.	
Reference:	

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-

### Question: 3

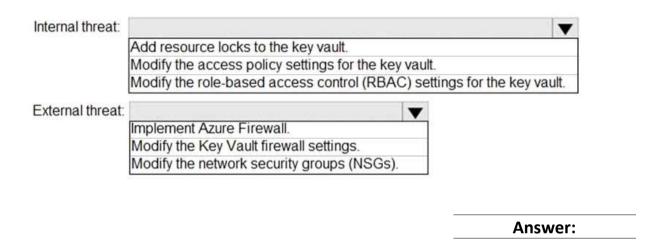
#### **HOTSPOT**

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

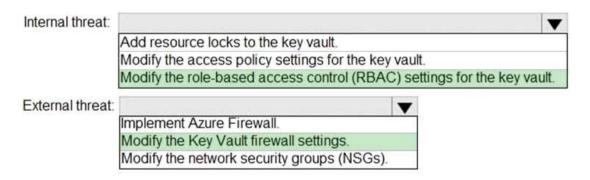
What should you recommend for each threat? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### **Answer Area**



#### **Answer Area**



#### Reference:

https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault

### Question: 4

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

**Answer: B** 

Explanation:

#### Reference:

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

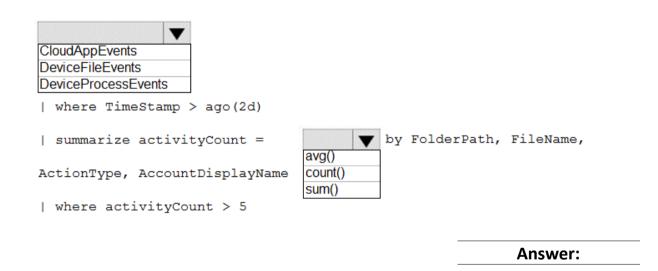
### Question: 5

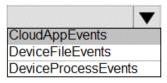
#### **HOTSPOT**

You need to create an advanced hunting query to investigate the executive team issue.

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

NOTE: Each correct selection is worth one point.



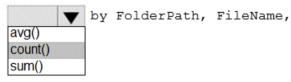


| where TimeStamp > ago(2d)

| summarize activityCount =

ActionType, AccountDisplayName

| where activityCount > 5



## Thank You for trying SC-200 PDF Demo

To Buy Latest SC-200 Full Version Download visit link below

https://www.certkillers.net/Exam/SC-200

# Start Your SC-200 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your SC-200 preparation with actual exam questions.