

ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Microsoft

Code: SC-200

Exam: Microsoft Security Operations Analyst

https://www.examsnest.com/exam/sc-200/

QUESTIONS & ANSWERS

DEMO VERSION

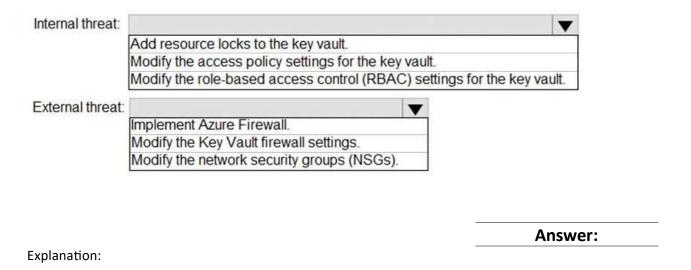
QUESTIONS & ANSWERS DEMO VERSION (LIMITED CONTENT)

Version: 26.0

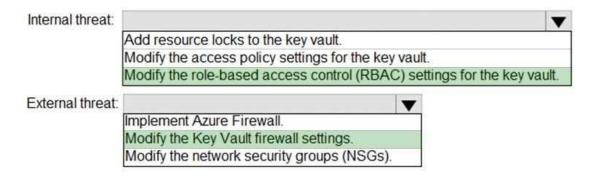
Question: 1
The issue for which team can be resolved by using Microsoft Defender for Endpoint?
A. executive
B. sales
C. marketing
Answer: C
Explanation:
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft- defender-atp-ios
Question: 2
The issue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

D. sales		
Explanation:		Answer: B
Reference: https://docs.microsoft.com/en-u teams? view=o365-worldwide	us/microsoft-365/security/office-365-secu	rity/atp-for-spo-odb-and-
Question: 3 HOTSPOT for the Azure virtual		
	ation actions for the Azure Defender alert	s for Fabrikam.
What should you recommend fo area.	r each threat? To answer, select the appro	opriate options in the answer
NOTE: Each correct selection is v	vorth one point.	

Answer Area



Answer Area



Reference:

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

Question: 4

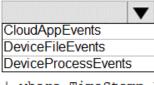
You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

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.			

Questions & Answers PDF

Page 5

Questions & Answers PDF Page 6

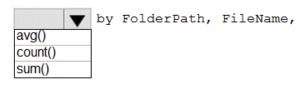


| where TimeStamp > ago(2d)

| summarize activityCount =

ActionType, AccountDisplayName

| where activityCount > 5



Answer:

Explanation:

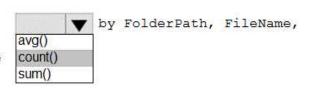


| where TimeStamp > ago(2d)

| summarize activityCount =

ActionType, AccountDisplayName

| where activityCount > 5





Thank You for trying the PDF Demo

Vendor: Microsoft

Code: SC-200

Exam: Microsoft Security Operations Analyst https://www.examsnest.com/exam/sc-200/

Use Coupon "SAVE15" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation