

Microsoft Security Operations Analyst

Questions & Answers Demo

Version: 8.0

Question: 1

The issue for which team can be resolved by using Microsoft Defender for Endpoint?

A. executive

B. sales

C. marketing

Explanation:

Answer: B

Reference: <u>https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios</u>

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

Answer: B

Explanation:

Reference:

<u>https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams</u>? view=o365-worldwide

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

| | Add resource locks to the key vault. | |
|------------------|-------------------------------------------------------------------------|--|
| | Modify the access policy settings for the key vault. | |
| | Modify the role-based access control (RBAC) settings for the key vault. | |
| | | |
| External threat: | | |
| External threat: | Implement Azure Firewall. | |
| External threat: | Implement Azure Firewall. Modify the Key Vault firewall settings. | |

Answer:

Explanation:

Answer Area

| Internal threat: | | |
|------------------|--------------------------------------------------------------|--------------|
| | Add resource locks to the key vault. | |
| | Modify the access policy settings for the key vault. | |
| | Modify the role-based access control (RBAC) settings for the | e key vault. |
| External threat: | | |
| | Implement Azure Firewall. | |
| | Modify the Key Vault firewall settings. | |
| | Modify the network security groups (NSGs). | |

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

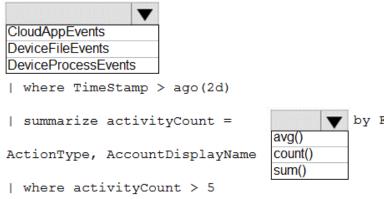
Question: 5

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.

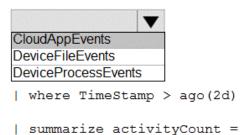
NOTE: Each correct selection is worth one point.



by FolderPath, FileName,

Answer:

Explanation:





by FolderPath, FileName,

ActionType, AccountDisplayName

| where activityCount > 5