Question 1

You have a Microsoft 365 subscription

You need to recommend a security solution to monitor the following activities:

* User accounts that were potentially compromised

* Users performing bulk file downloads from Microsoft SharePoint Online

What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each Correct selection is worth one Point.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exfiltration

https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users

Answer:

Question 2

Question Type: **MultipleChoice**

You need to recommend a solution to resolve the virtual machine issue. What should you include in the recommendation?

Options:

A) Onboard the virtual machines to Microsoft Defender for Endpoint.

B) Onboard the virtual machines to Azure Arc.

C) Create a device compliance policy in Microsoft Endpoint Manager.

D) Enable the Qualys scanner in Defender for Cloud.

Answer:

A

Question 3

Question Type: **MultipleChoice**

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You need to enforce ISO 2700V2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatical

What should you use?

Options:

A) the regulatory compliance dashboard in Defender for Cloud

B) Azure Policy

C) Azure Blueprints

D) Azure role-based access control (Azure RBAC)

Answer:

D

Question 4

You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases. All resources are backed up multiple times a day by using Azure Backup. You are developing a strategy to protect against ransomware attacks.

You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successtu\ ransonvwaTe

attack.

Which two controls should you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

Options:

A) Use Azure Monitor notifications when backup configurations change.

B) Require PINs for critical operations.

C) Perform offline backups to Azure Data Box.

D) Encrypt backups by using customer-managed keys (CMKs).

E) Enable soft delete for backups.

Answer:

B, C

Question 5

Question Type: **MultipleChoice**

A customer has a Microsoft 365 E5 subscription and an Azure subscription.

The customer wants to centrally manage security incidents, analyze log, audit activity, and hunt for potential threats across all deployed services.

You need to recommend a solution for the customer. The solution must minimize costs.

What should you include in the recommendation?

Options:

A) Microsoft 365 Defender

B) Microsoft Defender for Cloud

C) Microsoft Defender for Cloud Apps

D) Microsoft Sentinel

Answer:

D

Question 6

Question Type: MultipleChoice

Your company has a hybrid cloud infrastructure.

Data and applications are moved regularly between cloud environments.

The company's on-premises network is managed as shown in the following exhibit.

NOTE Each correct selection is worth one point.

Options:

A) Azure VPN Gateway

B) guest configuration in Azure Policy

C) on-premises data gateway

D) Azure Bastion

E) Azure Arc

Answer:

C, E

Question 7

Question Type: **MultipleChoice**

Your company has a hybrid cloud infrastructure.

Data and applications are moved regularly between cloud environments.

The company's on-premises network is managed as shown in the following exhibit.

NOTE Each correct selection is worth one point.

Options:

A) Azure VPN Gateway

B) guest configuration in Azure Policy

C) on-premises data gateway

D) Azure Bastion

E) Azure Arc

Answer:

C, E

Question 8

A customer has a Microsoft 365 E5 subscription and an Azure subscription.

The customer wants to centrally manage security incidents, analyze log, audit activity, and hunt for potential threats across all deployed services.

You need to recommend a solution for the customer. The solution must minimize costs.

What should you include in the recommendation?

Options:
A) Microsoft 365 Defender

B) Microsoft Defender for Cloud

C) Microsoft Defender for Cloud Apps

D) Microsoft Sentinel

Answer:
D

Question 9

You need to recommend a solution to resolve the virtual machine issue. What should you include in the recommendation?

Options:

A) Onboard the virtual machines to Microsoft Defender for Endpoint.

B) Onboard the virtual machines to Azure Arc.

C) Create a device compliance policy in Microsoft Endpoint Manager.

D) Enable the Qualys scanner in Defender for Cloud.

Answer:

A

Question 10

Question Type: **MultipleChoice**

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You need to enforce ISO 2700V2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatical

What should you use?

Options:

A) the regulatory compliance dashboard in Defender for Cloud

B) Azure Policy

C) Azure Blueprints

D) Azure role-based access control (Azure RBAC)

Answer:

D

Question 11

Question Type: **MultipleChoice**

You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases. All resources are backed up multiple times a day by using Azure Backup. You are developing a strategy to protect against ransomware attacks.

You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successtu\ ransonvwaTe

attack.

Which two controls should you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

Options:

A) Use Azure Monitor notifications when backup configurations change.

B) Require PINs for critical operations.

C) Perform offline backups to Azure Data Box.

D) Encrypt backups by using customer-managed keys (CMKs).

E) Enable soft delete for backups.

Answer:

B, C

Question 12

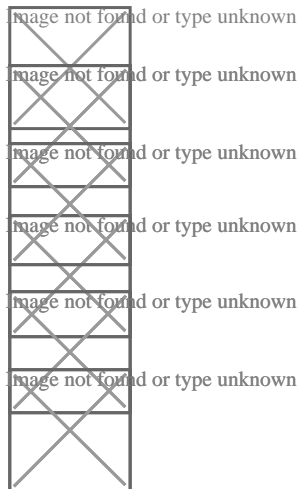You have a Microsoft 365 subscription

You need to recommend a security solution to monitor the following activities:

* User accounts that were potentially compromised

* Users performing bulk file downloads from Microsoft SharePoint Online

What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each Correct selection is worth one Point.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exfiltration

https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users

Answer: