Practice Exam Questions



SC-900

Microsoft Security, Compliance and Identity Fundamentals



Microsoft

Exam SC-900

Microsoft Security Compliance and Identity Fundamentals

Version: 8.0

[Total Questions: 138]

Question No: 1 HOTSPOT

Select the answer that correctly completes the sentence.



Answer:

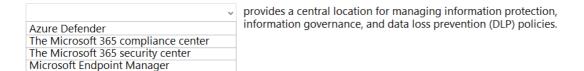


Text

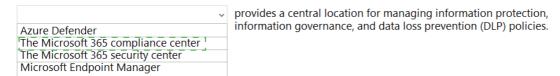
Description automatically generated

Question No: 2 HOTSPOT

Select the answer that correctly completes the sentence.



Answer:





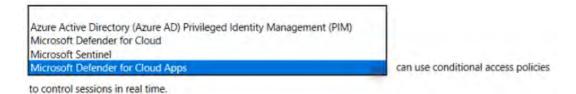
provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.

Text

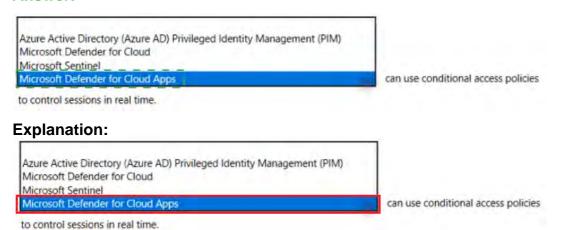
Description automatically generated

Question No: 3 HOTSPOT

Select the answer that correctly completes the sentence.



Answer:



Question No: 4

Which Azure Active Directory (Azure AD) feature can you use to provide just-in-time (JIT) access to manage Azure resources?

- A. conditional access policies
- B. Azure AD Identity Protection
- C. Azure AD Privileged Identity Management (PIM)
- D. authentication method policies

Answer: C

Explanation:

Azure AD Privileged Identity Management (PIM) provides just-in-time privileged access to Azure AD and Azure resources

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Question No: 5 HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area			
	Statements	Yes	No
	Applying system updates increases an organization's secure score in Azure Security Center.	0	0
	The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	0	O
	Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	0	0

Answer:

Answer Area			
	Statements	Yes	No
	Applying system updates increases an organization's secure score in Azure Security Center.	0	0
	The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	[0]	0
	Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	101	0

Explanation:

Answer Area			
	Statements	Yes	No
	Applying system updates increases an organization's secure score in Azure Security Center.	0	0
	The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	0	Ö
	Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	0	[©] Graphical user

interface, text, application, email

Description automatically generated

Box 1: Yes

System updates reduces security vulnerabilities, and provide a more stable environment for end users. Not applying updates leaves unpatched vulnerabilities and results in environments that are susceptible to attacks.

Box 2: Yes

Box 3: Yes

If you only use a password to authenticate a user, it leaves an attack vector open. With MFA enabled, your accounts are more secure.

Question No: 6

Which two Azure resources can a network security group (NSG) be associated with? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. a network interface
- B. an Azure App Service web app
- C. a virtual network
- **D.** a virtual network subnet
- E. a resource group

Answer: C,E

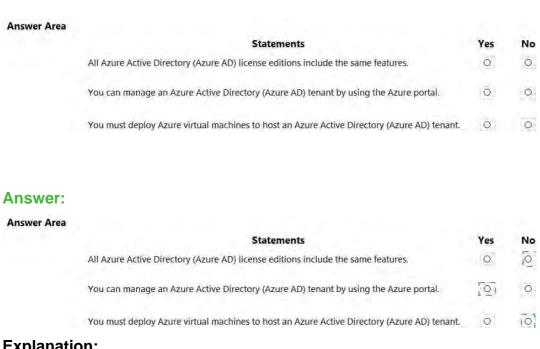
Explanation:

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.

Question No: 7 HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Explanation:



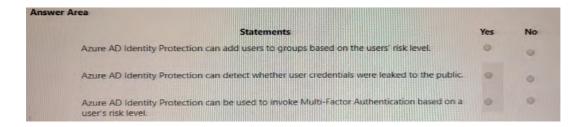
interface, text, application

Description automatically generated

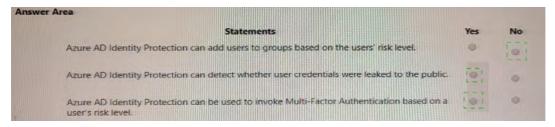
Question No: 8 HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Answer:



Statements Statements Yes No Azure AD Identity Protection can add users to groups based on the users' risk level. Azure AD Identity Protection can detect whether user credentials were leaked to the public. Azure AD Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.

Question No: 9 HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

	Microsoft SC-900 : Practice Test		
Answer Area			
	Statements	Yes	No
	Azure Defender can detect vulnerabilities and threats for Azure Storage.	0	0
	Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	0	0
	Azure Security Center can evaluate the security of workloads deployed to Azure or on- premises.	0	0
Answer:			
Answer Area			
	Statements	Yes	No
	Azure Defender can detect vulnerabilities and threats for Azure Storage.	0	0
	Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	10)	O
	Azure Security Center can evaluate the security of workloads deployed to Azure or on- premises.	0	0
Explanati Answer Area	on:		
	Statements	Yes	No
	Azure Defender can detect vulnerabilities and threats for Azure Storage.	Ø	Ö
	Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	0	O

Azure Security Center can evaluate the security of workloads deployed to Azure or on-

interface, text, application, email

Description automatically generated

Box 1: Yes

Azure Defender provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, your storage, and more

Box 2: Yes

Cloud security posture management (CSPM) is available for free to all Azure users.

Box 3: Yes

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as

© Graphical user

well as on premises.

Question No: 10 DRAG DROP

Match the types Of compliance score actions to the appropriate tasks.

To answer. drag the appropriate action type from the column on the left to its task on the right. Each type may be used once. more than once, or not at all.

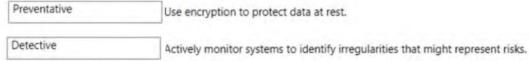
NOTE: Each correct match is worth one point.



Answer:



Explanation:



Question No: 11 HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	0	0
Conditional access policies can be used to block access to an application based on the location of the user.	0	0
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	0	0

Answer:

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	0	0
Conditional access policies can be used to block access to an application based on the location of the user.	[0]	0
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	0	0
Explanation:		

Explanation.		
Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	0	0
Conditional access policies can be used to block access to an application based on the location of the user.	0	0
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	0	Graphical user

interface, text, application, email

Description automatically generated

Question No: 12

Which two types of resources can be protected by using Azure Firewall? Each correct answer presents a complete solution.

- A. Azure virtual machines
- B. Azure Active Directory (Azure AD) users
- C. Microsoft Exchange Online inboxes
- D. Azure virtual networks
- E. Microsoft SharePoint Online sites

Answer: A,D

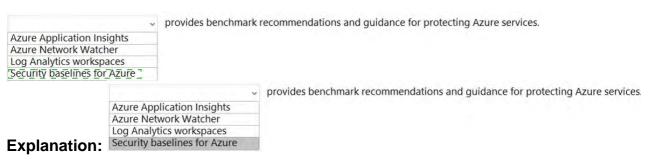
Explanation: Firewall is really not directly protecting the Virtual Networks though DDOS would have been ideal for VNETS

Question No: 13 HOTSPOT

Select the answer that correctly completes the sentence.



Answer:



Text

Description automatically generated with medium confidence

Question No: 14 HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area Statements Yes No Control is a key privacy principle of Microsoft. 0 0 Transparency is a key privacy principle of Microsoft. 0 0 Shared responsibility is a key privacy principle of Microsoft. **Answer: Answer Area Statements** Yes No 0 Control is a key privacy principle of Microsoft. 0 Transparency is a key privacy principle of Microsoft. 101 0 Shared responsibility is a key privacy principle of Microsoft. 101 **Explanation: Answer Area Statements** Yes No Control is a key privacy principle of Microsoft. 0 0 Transparency is a key privacy principle of Microsoft. 0 0 Graphical user Shared responsibility is a key privacy principle of Microsoft. 0 interface, text, application, email

Description automatically generated

Question No: 15 HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements	Yes	No
You can add a resource lock to an Azure subscription.	0	0
You can add only one resource lock to an Azure resource.	0	0
You can delete a resource group containing resources that have resource locks.	0	0

Answer:

Statements	Yes	No
You can add a resource lock to an Azure subscription.	0	0
You can add only one resource lock to an Azure resource.	O	0
You can delete a resource group containing resources that have resource locks.	0	0

Explanation: Yes

NO

NO

YES - As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

NO - The most restrictive lock in the inheritance takes precedence.

NO - If you delete a resource group with a locked resource, the portal UI will give you an error and no resources are deleted.

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json

Question No: 16 HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements Yes No Conditional access policies can use the device state as a signal. Conditional access policies apply before first-factor authentication is complete. Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.

Answer:

Answer Area		
Statements	Yes	No
Conditional access policies can use the device state as a signal.	0	0
Conditional access policies apply before first-factor authentication is complete.	0	0
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	0	0

Explanation:

Answer Area		
Statements	Yes	No
Conditional access policies can use the device state as a sign	nal.	0
Conditional access policies apply before first-factor authentical complete.	ation is O	0
Conditional access policies can trigger multi-factor authentica (MFA) if a user attempts to access a specific application.	tion	Graphical user

interface, text, application, email

Description automatically generated

Box 1: Yes

Box 2: No

Conditional Access policies are enforced after first-factor authentication is completed. Box

3: Yes

Question No: 17

What can you use to provision Azure resources across multiple subscriptions in a consistent manner?

- A. Microsoft Defender for Cloud
- **B.** Azure Blueprints
- C. Microsoft Sentinel
- D. Azure Policy

Answer: B

Question No: 18

What should you use in the Microsoft 365 security center to view security trends and track the protection status of identities?

- A. Attack simulator
- B. Reports
- **C.** Hunting
- **D.** Incidents

Answer: B

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-and-insights-in-security- and-compliance?view=o365-worldwide

Question No: 19 HOTSPOT

Select the answer that correctly completes the sentence.

When you enable security defaults in Azure Active Directory (Azure AD),



will be enabled for all Azure AD users.

Answer:

When you enable security defaults in Azure Active Directory (Azure AD),



will be enabled for all Azure AD users.

When you enable security defaults in Azure Active Directory (Azure AD),



will be enabled for all Azure AD users.

Explanation:

Graphical user interface, text, application

Description automatically generated

Question No: 20

Which score measures an organization's progress in completing actions that help reduce risks associated to data protection and regulatory standards?

- A. Microsoft Secure Score
- B. Productivity Score
- C. Secure score in Azure Security Center
- D. Compliance score

Answer: D Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365- worldwide

Question No: 21

Which Microsoft 365 feature can you use to restrict users from sending email messages that contain lists of customers and their associated credit card numbers?

- A. retention policies
- B. data loss prevention (DLP) policies
- C. conditional access policies
- D. information barriers

Answer: B

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

Question No: 22 HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	0	0
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	0	0
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	0	0

Answer:

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	101	0
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	191	0
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	101	0

Explanation:

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	•	0
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	•	0
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	•	0

Question No: 23

Which Microsoft portal provides information about how Microsoft cloud services comply with regulatory standard, such as International Organization for Standardization (ISO)?

- A. the Microsoft Endpoint Manager admin center
- B. Azure Cost Management + Billing
- C. Microsoft Service Trust Portal
- **D.** the Azure Active Directory admin center

Answer: C

Explanation:

The Microsoft Service Trust Portal contains details about Microsoft's implementation of controls and processes that protect our cloud services and the customer data therein.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365- worldwide

Question No: 24 HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point

Statements	Yes	No
Security defaults require an Azure Active Directory (Azure AD) Premium license.	0	0
Security defaults can be enabled for a single Azure Active Directory (Azure AD) user.	0	0
When Security defaults are enabled, all administrators must use multi-factor authentication (MFA).	0	0

Answer:

Statements	Yes	No
Security defaults require an Azure Active Directory (Azure AD) Premium license.	101	0
Security defaults can be enabled for a single Azure Active Directory (Azure AD) user.	0	101
When Security defaults are enabled, all administrators must use multi-factor authentication (MFA).	101	0

Explanation: