

Exam Questions SC-900

Microsoft Security. Compliance and Identity Fundamentals

<https://www.2passeasy.com/dumps/SC-900/>



NEW QUESTION 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Azure Active Directory (Azure AD) is
 used for authentication and authorization.

an extended detection and response (XDR) system
an identity provider
a management group
a security information and event management (SIEM) system

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service. Reference:
<https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide>

NEW QUESTION 2

What can you protect by using the information protection solution in the Microsoft 365 compliance center?

- A. computers from zero-day exploits
- B. users from phishing attempts
- C. files from malware and viruses
- D. sensitive data from being exposed to unauthorized users

Answer: D

Explanation:

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide>

NEW QUESTION 3

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Azure Blueprints
Azure Policy
The Microsoft Cloud Adoption Framework for Azure
A resource lock

provides best practices from Microsoft employees, partners, and customers, including tools and guidance to assist in an Azure deployment.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure Blueprints
Azure Policy
The Microsoft Cloud Adoption Framework for Azure
A resource lock

provides best practices from Microsoft employees, partners, and customers, including tools and guidance to assist in an Azure deployment.

NEW QUESTION 4

What is the purpose of Azure Active Directory (Azure AD) Password Protection?

- A. to control how often users must change their passwords
- B. to identify devices to which users can sign in without using multi-factor authentication (MFA)
- C. to encrypt a password by using globally recognized encryption standards
- D. to prevent users from using specific words in their passwords

Answer: D

Explanation:

Azure AD Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization.

With Azure AD Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. To support your own business and security needs, you can define entries in a custom banned password list.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises>

NEW QUESTION 5

What can you specify in Microsoft 365 sensitivity labels?

- A. how long files must be preserved
- B. when to archive an email message
- C. which watermark to add to files
- D. where to store files

Answer: C

Explanation:

Reference:<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

NEW QUESTION 6

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Azure DDoS Protection Standard can be used to protect

Azure Active Directory (Azure AD) applications.
Azure Active Directory (Azure AD) users.
resource groups.
virtual networks.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure DDoS Protection Standard can be used to protect

Azure Active Directory (Azure AD) applications.
Azure Active Directory (Azure AD) users.
resource groups.
virtual networks.

NEW QUESTION 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.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Azure AD Identity Protection can add users to groups based on the users' risk level.	<input type="radio"/>	<input checked="" type="radio"/>
Azure AD Identity Protection can detect whether user credentials were leaked to the public.	<input checked="" type="radio"/>	<input type="radio"/>
Azure AD Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 8

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

▼	is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution used to provide a single solution for alert detection, threat visibility, proactive hunting, and threat response.
Azure Advisor	
Azure Bastion	
Azure Monitor	
Azure Sentinel	

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

NEW QUESTION 9

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Microsoft Defender for Identity can identify advanced threats from

▼	signals.
Azure Active Directory (Azure AD)	
Azure AD Connect	
on-premises Active Directory Domain Services (AD DS)	

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Microsoft Defender for Identity is a cloud-based security solution that leverages your on- premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

NEW QUESTION 10

What are two capabilities of Microsoft Defender for Endpoint? Each correct selection presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. automated investigation and remediation
 B. transport encryption
 C. shadow IT detection
 D. attack surface reduction

Answer: AD

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide>

NEW QUESTION 10

HOTSPOT

Select the answer that correctly completes the sentence.

Microsoft Defender for Cloud Apps	is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.
Microsoft Defender for Endpoint	
Microsoft Defender for Identity	
Microsoft Defender for Office 365	

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

NEW QUESTION 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.

Answer Area

Statements	Yes	No
You can create a hybrid identity in an on-premises Active Directory that syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
User accounts created in Azure AD sync automatically to an on-premises Active Directory.	<input type="radio"/>	<input type="radio"/>
When using a hybrid model, authentication can either be done by Azure AD or by another identity provider.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
You can create a hybrid identity in an on-premises Active Directory that syncs to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User accounts created in Azure AD sync automatically to an on-premises Active Directory.	<input type="radio"/>	<input checked="" type="radio"/>
When using a hybrid model, authentication can either be done by Azure AD or by another identity provider.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 12

You plan to implement a security strategy and place multiple layers of defense throughout a network infrastructure. Which security methodology does this represent?

- A. threat modeling
- B. identity as the security perimeter
- C. defense in depth
- D. the shared responsibility model

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/2-what-is-defense-in-depth>

NEW QUESTION 15

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

Explanation:

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>

NEW QUESTION 16

What are customers responsible for when evaluating security in a software as a service (SaaS) cloud services model?

- A. applications
- B. network controls
- C. operating systems
- D. accounts and identities

Answer: A

NEW QUESTION 18

DRAG DROP

Match the Microsoft Defender for Office 365 feature to the correct description.

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

NOTE: Each correct match is worth one point.

Features	Answer Area
Threat Explorer	Feature Provides intelligence on prevailing cybersecurity issues
Threat Trackers	Feature Provides real-time reports to identify and analyze recent threats
Anti-phishing protection	Feature Detects impersonation attempts

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Features	Answer Area
Threat Explorer	Anti-phishing protection Provides intelligence on prevailing cybersecurity issues
Threat Trackers	Threat Explorer Provides real-time reports to identify and analyze recent threats
Anti-phishing protection	Threat Trackers Detects impersonation attempts

NEW QUESTION 22

In a hybrid identity model, what can you use to sync identities between Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD)?

- A. Active Directory Federation Services (AD FS)
B. Azure Sentinel
C. Azure AD Connect
D. Azure Ad Privileged Identity Management (PIM)

Answer: C

Explanation:

Explanation

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect>

NEW QUESTION 25

HOTSPOT

Select the answer that correctly completes the sentence.

When users sign in to the Azure portal, they are first

assigned permissions.

authenticated.

authorized.

resolved.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

When users sign in to the Azure portal, they are first

assigned permissions.

authenticated.

authorized.

resolved.

NEW QUESTION 26

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
Communication compliance is configured by using the Microsoft 365 admin center.	<input type="radio"/>	<input type="radio"/>
Microsoft SharePoint Online supports communication compliance.	<input type="radio"/>	<input type="radio"/>
Communication compliance can remediate compliance issues.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Communication compliance is configured by using the Microsoft 365 admin center.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft SharePoint Online supports communication compliance.	<input checked="" type="radio"/>	<input type="radio"/>
Communication compliance can remediate compliance issues.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 31

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Multi-factor authentication (MFA)
Pass-through authentication
Password writeback
Single sign-on (SSO)

requires additional verification, such as a verification code sent to a mobile phone.

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan.

NEW QUESTION 35

What can you use to view the Microsoft Secure Score for Devices?

- A. Microsoft Defender for Cloud Apps
 B. Microsoft Defender for Endpoint
 C. Microsoft Defender for Identity
 D. Microsoft Defender for Office 365

Answer: B

Explanation:

Microsoft Secure Score for Devices

? Artikel

? 12.05.2022

? 3 Minuten Lesedauer Applies to:

? Microsoft Defender for Endpoint Plan 2

? Microsoft Defender Vulnerability Management

? Microsoft 365 Defender

Some information relates to pre-released product which may be substantially modified before it's commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here.

To sign up for the Defender Vulnerability Management public preview or if you have any questions, contact us (mdvmtrial@microsoft.com).

Already have Microsoft Defender for Endpoint P2? Sign up for a free trial of the Defender Vulnerability Management Add-on.

Configuration score is now part of vulnerability management as Microsoft Secure Score for Devices.

Your score for devices is visible in the Defender Vulnerability Management dashboard of the Microsoft 365 Defender portal. A higher Microsoft Secure Score for

Devices means your endpoints are more resilient from cybersecurity threat attacks. It reflects the collective security configuration state of your devices across the following categories:

- ? Application
- ? Operating system
- ? Network
- ? Accounts
- ? Security controls

Select a category to go to the Security recommendations page and view the relevant recommendations.

Turn on the Microsoft Secure Score connector

Forward Microsoft Defender for Endpoint signals, giving Microsoft Secure Score visibility into the device security posture. Forwarded data is stored and processed in the same location as your Microsoft Secure Score data.

Changes might take up to a few hours to reflect in the dashboard.

? In the navigation pane, go to Settings > Endpoints > General > Advanced features

? Scroll down to Microsoft Secure Score and toggle the setting to On.

? Select Save preferences. How it works

Microsoft Secure Score for Devices currently supports configurations set via Group Policy. Due to the current partial Intune support, configurations which might have been set through Intune might show up as misconfigured. Contact your IT Administrator to verify the actual configuration status in case your organization is using Intune for secure configuration management.

The data in the Microsoft Secure Score for Devices card is the product of meticulous and ongoing vulnerability discovery process. It is aggregated with configuration discovery assessments that continuously:

- ? Compare collected configurations to the collected benchmarks to discover misconfigured assets
- ? Map configurations to vulnerabilities that can be remediated or partially remediated (risk reduction)
- ? Collect and maintain best practice configuration benchmarks (vendors, security feeds, internal research teams)
- ? Collect and monitor changes of security control configuration state from all assets

NEW QUESTION 36

What feature in Microsoft Defender for Endpoint provides the first line of defense against cyberthreats by reducing the attack surface?

- A. automated remediation
- B. automated investigation
- C. advanced hunting
- D. network protection

Answer: D

Explanation:

Network protection helps protect devices from Internet-based events. Network protection is an attack surface reduction capability.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?view=o365-worldwide>

NEW QUESTION 37

HOTSPOT

Select the answer that correctly completes the sentence.

In an environment that has on-premises resources and cloud resources,

the cloud

a firewall

identity

Microsoft Defender for Cloud

should be the primary security perimeter.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

In an environment that has on-premises resources and cloud resources,

the cloud

a firewall

identity

Microsoft Defender for Cloud

should be the primary security perimeter.

NEW QUESTION 41

HOTSPOT

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

NOTE: Each connect selection a worth one point.

er Area

Statements	Yes	No
An external email address can be used to authenticate self-service password reset (SSPR).	<input type="radio"/>	<input type="radio"/>
A notification to the Microsoft Authenticator app can be used to authenticate self-service password reset (SSPR).	<input type="radio"/>	<input type="radio"/>
To perform self-service password reset (SSPR), a user must already be signed in and authenticated to Azure AD.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

er Area

Statements	Yes	No
An external email address can be used to authenticate self-service password reset (SSPR).	<input type="radio"/>	<input checked="" type="radio"/>
A notification to the Microsoft Authenticator app can be used to authenticate self-service password reset (SSPR).	<input checked="" type="radio"/>	<input type="radio"/>
To perform self-service password reset (SSPR), a user must already be signed in and authenticated to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 44

HOTSPOT

Select the answer that correctly completes the sentence.

<div>▼</div>	provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.
Azure Defender	
The Microsoft 365 compliance center	
The Microsoft 365 security center	
Microsoft Endpoint Manager	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Text

Description automatically generated

NEW QUESTION 45

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

Explanation:

Reference:

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

NEW QUESTION 47

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
Azure Policy supports automatic remediation.	<input type="radio"/>	<input type="radio"/>
Azure Policy can be used to ensure that new resources adhere to corporate standards.	<input type="radio"/>	<input type="radio"/>
Compliance evaluation in Azure Policy occurs only when a target resource is created or modified.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Azure Policy supports automatic remediation.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Policy can be used to ensure that new resources adhere to corporate standards.	<input checked="" type="radio"/>	<input type="radio"/>
Compliance evaluation in Azure Policy occurs only when a target resource is created or modified.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 50

Which two cards are available in the Microsoft 365 Defender portal? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Users at risk
- B. Compliance Score
- C. Devices at risk
- D. Service Health
- E. User Management

Answer: BC

NEW QUESTION 55

Which three authentication methods does Windows Hello for Business support? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. fingerprint
- B. facial recognition
- C. PIN
- D. email verification
- E. security question

Answer: ABC

Explanation:

Reference:
<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works-authentication>

NEW QUESTION 57

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
You can create one Azure Bastion per virtual network.	<input type="radio"/>	<input type="radio"/>
Azure Bastion provides secure user connections by using RDP.	<input type="radio"/>	<input type="radio"/>
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
You can create one Azure Bastion per virtual network.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Bastion provides secure user connections by using RDP.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 62

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
Users can apply sensitivity labels manually.	<input type="radio"/>	<input type="radio"/>
Multiple sensitivity labels can be applied to the same file.	<input type="radio"/>	<input type="radio"/>
A sensitivity label can apply a watermark to a Microsoft Word document.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Users can apply sensitivity labels manually.	<input checked="" type="radio"/>	<input type="radio"/>
Multiple sensitivity labels can be applied to the same file.	<input type="radio"/>	<input checked="" type="radio"/>
A sensitivity label can apply a watermark to a Microsoft Word document.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 64

Which Azure Active Directory (Azure AD) feature can you use to evaluate group membership and automatically remove users that no longer require membership in a group?

- A. access reviews

- B. managed identities
- C. conditional access policies
- D. Azure AD Identity Protection

Answer: A

Explanation:

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

NEW QUESTION 65

In the Microsoft Cloud Adoption Framework for Azure, which two phases are addressed before the Ready phase? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Plan
- B. Manage
- C. Adopt
- D. Govern
- E. Define Strategy

Answer: AE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview>

NEW QUESTION 70

Which Microsoft 365 feature can you use to restrict communication and the sharing of information between members of two departments at your organization?

- A. sensitivity label policies
- B. Customer Lockbox
- C. information Barriers
- D. Privileged Access Management (PAM)

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers>

NEW QUESTION 75

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

<div><div></div><div>Customer Lockbox</div><div>Data loss prevention (DLP)</div><div>eDiscovery</div><div>A resource lock</div></div>	is used to identify, hold, and export electronic information that might be used in an investigation.
---	--

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

eDiscovery

<https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide>

NEW QUESTION 76

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>

NEW QUESTION 80

Which three authentication methods can be used by Azure Multi-Factor Authentication (MFA)? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. text message (SMS)
- B. Microsoft Authenticator app
- C. email verification
- D. phone call
- E. security question

Answer: ABD

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

NEW QUESTION 83

HOTSPOT

Select the answer that correctly completes the sentence.

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Microsoft Defender for Cloud
Microsoft Sentinel
Microsoft Defender for Cloud Apps

can use conditional access policies

to control sessions in real time.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Microsoft Defender for Cloud
Microsoft Sentinel
Microsoft Defender for Cloud Apps

can use conditional access policies

to control sessions in real time.

NEW QUESTION 88

HOTSPOT

Select the answer that correctly completes the sentence.

Applications registered in Azure Active Directory (Azure AD) are associated automatically to a

guest account.
managed identity.
service principal.
user account.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.

NEW QUESTION 89

HOTSPOT

Select the answer that correctly completes the sentence.

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

▼

Azure AD Identity Protection

Azure AD Privileged Identity Management (PIM)

multi-factor authentication (MFA)

will be enabled for all Azure AD users.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

▼

Azure AD Identity Protection

Azure AD Privileged Identity Management (PIM)

multi-factor authentication (MFA)

will be enabled for all Azure AD users.

NEW QUESTION 94

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Templates

Assessments

Improvement actions

Solutions

Templates

track compliance with groupings of controls from a specific regulation or requirement.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Templates

Assessments

Improvement actions

Solutions

Templates

track compliance with groupings of controls from a specific regulation or requirement.

NEW QUESTION 95

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
You can add a resource lock to an Azure subscription.	<input type="radio"/>	<input type="radio"/>
You can add only one resource lock to an Azure resource.	<input type="radio"/>	<input type="radio"/>
You can delete a resource group containing resources that have resource locks.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

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>

NEW QUESTION 96

What are three uses of Microsoft Cloud App Security? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. to discover and control the use of shadow IT
- B. to provide secure connections to Azure virtual machines
- C. to protect sensitive information hosted anywhere in the cloud
- D. to provide pass-through authentication to on-premises applications
- E. to prevent data leaks to noncompliant apps and limit access to regulated data

Answer: ACE

Explanation:

Reference:
<https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps>

NEW QUESTION 99

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: AD

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.

NEW QUESTION 101

What is a use case for implementing information barrier policies in Microsoft 365?

- A. to restrict unauthenticated access to Microsoft 365
- B. to restrict Microsoft Teams chats between certain groups within an organization
- C. to restrict Microsoft Exchange Online email between certain groups within an organization
- D. to restrict data sharing to external email recipients

Answer: B

Explanation:

Information barriers are supported in Microsoft Teams, SharePoint Online, and OneDrive for Business. A compliance administrator or information barriers administrator can define policies to allow or prevent communications between groups of users in Microsoft Teams. Information barrier policies can be used for situations like these:

NEW QUESTION 105

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

You can use

classifications
incidents
policies
Secure score

 in the Microsoft 365 security center to identify devices that are affected by an alert.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

You can use

classifications

incidents

policies

Secure score

 in the Microsoft 365 security center to identify devices that are affected by an alert.

NEW QUESTION 106

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
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	<input type="radio"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input type="radio"/>	<input type="radio"/>
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	<input checked="" type="radio"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 107

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

NEW QUESTION 110

Which statement represents a Microsoft privacy principle?

- A. Microsoft does not collect any customer data.
- B. Microsoft uses hosted customer email and chat data for targeted advertising.
- C. Microsoft manages privacy settings for its customers.
- D. Microsoft respects the local privacy laws that are applicable to its customers.

Answer: C

NEW QUESTION 113

Which type of identity is created when you register an application with Active Directory (Azure AD)?

- A. a user account
- B. a user-assigned managed identity
- C. a system-assigned managed identity
- D. a service principal

Answer: D

Explanation:

When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

NEW QUESTION 116

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
With Advanced Audit in Microsoft 365, you can identify when email items were accessed.	<input type="radio"/>	<input type="radio"/>
Advanced Audit in Microsoft 365 supports the same retention period of audit logs as core auditing.	<input type="radio"/>	<input type="radio"/>
Advanced Audit in Microsoft 365 allocates customer-dedicated bandwidth for accessing audit data.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

The MailItemsAccessed event is a mailbox auditing action and is triggered when mail data is accessed by mail protocols and mail clients.

Box 2: No

Basic Audit retains audit records for 90 days.

Advanced Audit retains all Exchange, SharePoint, and Azure Active Directory audit records for one year. This is accomplished by a default audit log retention policy that retains any audit record that contains the value of Exchange, SharePoint, or AzureActiveDirectory for the Workload property (which indicates the service in which the activity occurred) for one year.

Box 3: yes

Advanced Audit in Microsoft 365 provides high-bandwidth access to the Office 365 Management Activity API.

NEW QUESTION 120

HOTSPOT

Select the answer that correctly completes the sentence.

<div><div></div><div></div></div>	can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.
Customer Lockbox	
Information barriers	
Privileged Access Management (PAM)	
Sensitivity labels	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<div><div></div><div></div></div>	can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.
Customer Lockbox	
Information barriers	
Privileged Access Management (PAM)	
Sensitivity labels	

NEW QUESTION 125

What is a characteristic of a sensitivity label in Microsoft 365?

- A. persistent
- B. encrypted
- C. restricted to predefined categories

Answer: B

NEW QUESTION 128

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
Azure Active Directory (Azure AD) is deployed to an on-premises environment.	<input type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	<input type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) is an identity and access management service.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Box 1: No
Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.
Box 2: Yes
Microsoft 365 uses Azure Active Directory (Azure AD). Azure Active Directory (Azure AD) is included with your Microsoft 365 subscription.
Box 3: Yes
Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.

NEW QUESTION 131

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
Device identity can be stored in Azure AD.	<input type="radio"/>	<input type="radio"/>
A single system-assigned managed identity can be used by multiple Azure resources.	<input type="radio"/>	<input type="radio"/>
If you delete an Azure resource that has a user-assigned managed identity, the managed identity is deleted automatically.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Device identity can be stored in Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
A single system-assigned managed identity can be used by multiple Azure resources.	<input checked="" type="radio"/>	<input type="radio"/>
If you delete an Azure resource that has a user-assigned managed identity, the managed identity is deleted automatically.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 136

Which three tasks can be performed by using Azure Active Directory (Azure AD) Identity Protection? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. Configure external access for partner organizations.
- B. Export risk detection to third-party utilities.
- C. Automate the detection and remediation of identity based-risks.
- D. Investigate risks that relate to user authentication.
- E. Create and automatically assign sensitivity labels to data.

Answer: BCD

NEW QUESTION 140

When security defaults are enabled for an Azure Active Directory (Azure AD) tenant, which two requirements are enforced? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. All users must authenticate from a registered device.
- B. Administrators must always use Azure Multi-Factor Authentication (MFA).
- C. Azure Multi-Factor Authentication (MFA) registration is required for all users.
- D. All users must authenticate by using passwordless sign-in.
- E. All users must authenticate by using Windows Hello.

Answer: BC

Explanation:

Security defaults make it easy to protect your organization with the following preconfigured security settings:

? Requiring all users to register for Azure AD Multi-Factor Authentication.

? Requiring administrators to do multi-factor authentication.

? Blocking legacy authentication protocols.

? Requiring users to do multi-factor authentication when necessary.

? Protecting privileged activities like access to the Azure portal.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

NEW QUESTION 144

You need to keep a copy of all files in a Microsoft SharePoint site for one year, even if users delete the files from the site. What should you apply to the site?

- A. a data loss prevention (DLP) policy
- B. a retention policy
- C. an insider risk policy
- D. a sensitivity label policy

Answer: B

NEW QUESTION 146

Which Microsoft 365 compliance feature can you use to encrypt content automatically based on specific conditions?

- A. Content Search
- B. sensitivity labels
- C. retention policies
- D. eDiscovery

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide>

NEW QUESTION 148

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
Azure AD Connect can be used to implement hybrid identity.	<input type="radio"/>	<input type="radio"/>
Hybrid identity requires the implementation of two Microsoft 365 tenants.	<input type="radio"/>	<input type="radio"/>
Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	<input checked="" type="radio"/>	<input type="radio"/>
Hybrid identity requires the implementation of two Microsoft 365 tenants.	<input type="radio"/>	<input checked="" type="radio"/>
Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 153

What can you use to scan email attachments and forward the attachments to recipients only if the attachments are free from malware?

- A. Microsoft Defender for Office 365
- B. Microsoft Defender Antivirus
- C. Microsoft Defender for Identity
- D. Microsoft Defender for Endpoint

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description>

NEW QUESTION 155

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
Microsoft Sentinel uses logic apps to identify anomalies across resources.	<input type="radio"/>	<input type="radio"/>
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	<input type="radio"/>	<input type="radio"/>
The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Microsoft Sentinel uses logic apps to identify anomalies across resources.	<input type="radio"/>	<input checked="" type="radio"/>
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	<input type="radio"/>	<input checked="" type="radio"/>
The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 156

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 can be applied to global administrators.	<input type="radio"/>	<input type="radio"/>
Conditional access policies are evaluated before a user is authenticated.	<input type="radio"/>	<input type="radio"/>
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, email Description automatically generated
Box 1: Yes
Conditional access policies can be applied to all users
Box 2: No
Conditional access policies are applied after first-factor authentication is completed.
Box 3: Yes
Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

NEW QUESTION 160

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
Global administrators are exempt from conditional access policies	<input type="radio"/>	<input type="radio"/>
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	<input type="radio"/>	<input type="radio"/>
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Global administrators are exempt from conditional access policies	<input type="radio"/>	<input checked="" type="radio"/>
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 163

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

You can use

Reports

Hunting

Attack simulator

Incidents

 in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

You can use

Reports

Hunting

Attack simulator

Incidents

 in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

NEW QUESTION 165

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Compliance Manager assesses compliance data

continually

monthly

on-demand

quarterly

 for an organization.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Compliance Manager assesses compliance data  for an organization.

continually ¹
monthly
on-demand
quarterly

NEW QUESTION 170

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-900 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-900 Product From:

<https://www.2passeasy.com/dumps/SC-900/>

Money Back Guarantee

SC-900 Practice Exam Features:

- * SC-900 Questions and Answers Updated Frequently
- * SC-900 Practice Questions Verified by Expert Senior Certified Staff
- * SC-900 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SC-900 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year