SC-900 Dumps

Microsoft Security. Compliance and Identity Fundamentals

https://www.certleader.com/SC-900-dumps.html

NEW QUESTION 1
Microsoft 365 Endpoint data loss prevention (Endpoint DLP) can be used on which operating systems?

A. Windows 10 and iOS only
B. Windows 10 and Android only
C. Windows 10, Android, and iOS
D. Windows 10 only

Answer: A

NEW QUESTION 2
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 use information barriers with Microsoft Exchange.	○	○
You can use information barriers with Microsoft SharePoint.	○	○
You can use information barriers with Microsoft Teams.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
You can use information barriers with Microsoft Exchange.	○	☐○☐
You can use information barriers with Microsoft SharePoint.	☐○☐	○
You can use information barriers with Microsoft Teams.	☐○☐	○

NEW QUESTION 3
What can you use to ensure that all the users in a specific group must use multi-factor authentication (MFA) to sign in to Azure AD?

A. Azure Policy
B. a communication compliance policy
C. a Conditional Access policy
D. a user risk policy

Answer: C

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
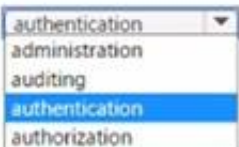D. where to store files

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

When users attempt to access an application or a service, | authentication ▼ | controls their level of access.
administration
auditing
authentication
authorization

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

When users attempt to access an application or a service, | authentication ▼ | controls their level of access.
administration
auditing
authentication
authorization

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
You can create custom roles in Azure Active Directory (Azure AD).	○	○
Global administrator is a role in Azure Active Directory (Azure AD).	○	○
An Azure Active Directory (Azure AD) user can be assigned only one role.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
Azure AD supports custom roles.
Box 2: Yes
Global Administrator has access to all administrative features in Azure Active Directory. Box 3: No

NEW QUESTION 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 Area

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.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 9
Microsoft 365 Endpoint data loss prevention (Endpoint DLP) can be used on which operating systems?

A. Windows 10 and newer only
B. Windows 10 and newer and Android only
C. Windows 10 and newer and macOS only
D. Windows 10 and newer, Android, and macOS

Answer: C

NEW QUESTION 10
Which Azure Active Directory (Azure AD) feature can you use to restrict Microsoft Intune- managed devices from accessing corporate resources?

A. network security groups (NSGs)
B. Azure AD Privileged Identity Management (PIM)
C. conditional access policies
D. resource locks

Answer: B

NEW QUESTION 10
What is an example of encryption at rest?

A. encrypting communications by using a site-to-site VPN
B. encrypting a virtual machine disk
C. accessing a website by using an encrypted HTTPS connection
D. sending an encrypted email

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest

NEW QUESTION 14
DRAG DROP
You are evaluating the compliance score in Microsoft Purview Compliance Manager. Match the compliance score action subcategories to the appropriate actions.
To answer, drag the appropriate action subcategory from the column on the left to its action on the right. Each action subcategory may be used once, more than once, or not at all.
NOTE: Each correct match is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Action Subcategories	Answer Area	
Corrective	Preventative	Encrypt data at rest.
Detective	Detective	Perform a system access audit.
Preventative	Corrective	Make configuration changes in response to a security incident.

NEW QUESTION 18
You have an Azure subscription that contains multiple resources.
You need to assess compliance and enforce standards for the existing resources. What should you use?

A. the Anomaly Detector service
B. Microsoft Sentinel
C. Azure Blueprints
D. Azure Policy

Answer: D

NEW QUESTION 22
What are two reasons to deploy multiple virtual networks instead of using just one virtual network? Each correct answer presents a complete solution.
NOTE; Each correct selection is worth one point.

A. to separate the resources for budgeting
B. to meet Governance policies
C. to isolate the resources
D. to connect multiple types of resources

Answer: BC

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.

Statements	Yes	No
You can use Advanced Audit in Microsoft 365 to view billing details.	○	○
You can use Advanced Audit in Microsoft 365 to view the contents of an email message.	○	○
You can use Advanced Audit in Microsoft 365 to identify when a user uses the search bar in Outlook on the web to search for items in a mailbox.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
Advanced Audit helps organizations to conduct forensic and compliance investigations by increasing audit log retention.
Box 2: No
Box 3: Yes

NEW QUESTION 28
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
Sensitivity labels can be used to encrypt documents.	○	○
Sensitivity labels can add headers and footers to documents.	○	○
Sensitivity labels can apply watermarks to emails.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
You can use sensitivity labels to provide protection settings that include encryption of emails and documents to prevent unauthorized people from accessing this data.
Box 2: Yes
You can use sensitivity labels to mark the content when you use Office apps, by adding watermarks, headers, or footers to documents that have the label applied.
Box 3: NO
https://docs.microsoft.com/en-us/information-protection/deploy-use/configure-policy-markings

NEW QUESTION 30
HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

When users sign in, [authentication ▼] verifies their credentials to prove their identity.
- administration
- auditing
- **authentication**
- authorization

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

When users sign in, [authentication ▼] verifies their credentials to prove their identity.
- administration
- auditing
- authentication
- authorization

NEW QUESTION 33
HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

Microsoft Sentinel provides quick insights into data by using [Azure Logic Apps. ▼]
- Azure Logic Apps.
- Azure Monitor workbook templates.
- Azure Resource Graph Explorer.
- playbooks.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Microsoft Sentinel provides quick insights into data by using | Azure Logic Apps. ▼

Azure Logic Apps.
Azure Monitor workbook templates.
Azure Resource Graph Explorer.
playbooks.

NEW QUESTION 37
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 42
DRAG DROP
Match the Microsoft 365 insider risk management workflow step to the appropriate task.
To answer, drag the appropriate step from the column on the left to its task on the right. Each step may be used once, more than once, or not at all.
NOTE: Each correct match is worth one point.

Steps

| Action |
| Investigate |
| Triage |

Answer Area

	Review and filter alerts
	Create cases in the Case dashboard
	Send a reminder of corporate policies to users

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Steps

| Action |
| Investigate |
| Triage |

Answer Area

Triage	Review and filter alerts
Investigate	Create cases in the Case dashboard
Action	Send a reminder of corporate policies to users

NEW QUESTION 43
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) Identity Protection can add users to groups based on the users' risk level.	○	○
Azure Active Directory (Azure AD) Identity Protection can detect whether user credentials were leaked to the public.	○	○
Azure Active Directory (Azure AD) Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
Box 2: Yes
Leaked Credentials indicates that the user's valid credentials have been leaked.
Box 3: Yes
Multi-Factor Authentication can be required based on conditions, one of which is user risk.

NEW QUESTION 48
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 DDoS Protection Standard protects against man-in-the-middle (MITM) attacks.	○	○
Azure DDoS Protection Standard is enabled by default in an Azure subscription.	○	○
Azure DDoS Protection Standard protects against protocol attacks.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Azure DDoS Protection Standard protects against man-in-the-middle (MITM) attacks.	○	○
Azure DDoS Protection Standard is enabled by default in an Azure subscription.	○	○
Azure DDoS Protection Standard protects against protocol attacks.	○	○

NEW QUESTION 52
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 53
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 58
HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

	a file makes the data in the file readable and usable to viewers that have the appropriate key.
Archiving	
Compressing	
Deduplicating	
Encrypting	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

	a file makes the data in the file readable and usable to viewers that have the appropriate key.
Archiving	
Compressing	
Deduplicating	
Encrypting	

NEW QUESTION 59
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 61
What can you use to deploy Azure resources across multiple subscriptions in a consistent manner?

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

Answer: D

NEW QUESTION 66
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 70
Which Microsoft 365 compliance center feature can you use to identify all the documents on a Microsoft SharePoint Online site that contain a specific key word?

A. Audit
B. Compliance Manager
C. Content Search
D. Alerts

Answer: C

Explanation:
The Content Search tool in the Security & Compliance Center can be used to quickly find email in Exchange mailboxes, documents in SharePoint sites and OneDrive locations, and instant messaging conversations in Skype for Business.
The first step is to starting using the Content Search tool to choose content locations to search and configure a keyword query to search for specific items.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-content?view=o365- worldwide

NEW QUESTION 72
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.

A. Mastered
B. Not Mastered
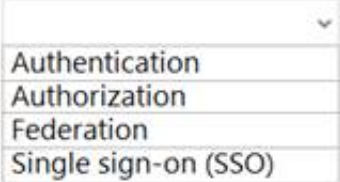
Answer: A

Explanation:

NEW QUESTION 76
HOTSPOT
Select the answer that correctly completes the sentence.

_____ is the process of identifying whether a signed-in user can access a specific resource.

Authentication
Authorization
Federation
Single sign-on (SSO)

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text
Description automatically generated

NEW QUESTION 77
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 80
HOTSPOT
Select the answer that correctly completes the sentence.

You can use dynamic groups in Azure Active Directory (Azure AD) to automate the [access / object / **privileged access**] lifecycle process.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

You can use dynamic groups in Azure Active Directory (Azure AD) to automate the [access / object / **privileged access**] lifecycle process.

NEW QUESTION 85
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 86
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 89
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.	○	○
Azure Bastion provides secure user connections by using RDP.	○	○
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
You can create one Azure Bastion per virtual network.	○	○
Azure Bastion provides secure user connections by using RDP.	○	○
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	○	○

NEW QUESTION 94
HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

In Microsoft Sentinel, you can automate common tasks by using [playbooks. ▼]
- deep investigation tools.
- hunting search-and-query tools.
- **playbooks.**
- workbooks.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

In Microsoft Sentinel, you can automate common tasks by using [playbooks. ▼]
- deep investigation tools.
- hunting search-and-query tools.
- **playbooks.**
- workbooks.

NEW QUESTION 96
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 99
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 100
HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 101
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 103
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 105
HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

Microsoft Purview Compliance Manager assesses compliance data [continually ▼] for an organization.
continually
monthly
on-demand
quarterly

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Microsoft Purview Compliance Manager assesses compliance data [continually ▼] for an organization.
continually
monthly
on-demand
quarterly

NEW QUESTION 107
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)
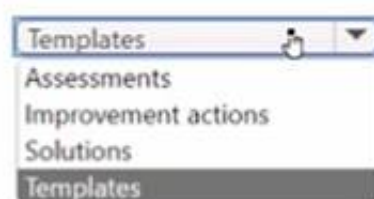multi-factor authentication (MFA)

will be enabled for all Azure AD users.

NEW QUESTION 108
HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

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

Assessments
Improvement actions
Solutions
Templates

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

Assessments
Improvement actions
Solutions
Templates
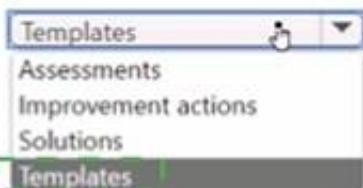
NEW QUESTION 109
Which two tasks can you implement by using data loss prevention (DLP) policies in Microsoft 365? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Display policy tips to users who are about to violate your organization's policies.
B. Enable disk encryption on endpoints.
C. Protect documents in Microsoft OneDrive that contain sensitive information.
D. Apply security baselines to devices.

Answer: AC

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

NEW QUESTION 114
HOTSPOT
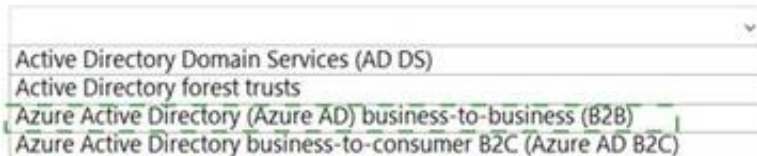Select the answer that correctly completes the sentence.

▾	enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.
Active Directory Domain Services (AD DS)	
Active Directory forest trusts	
Azure Active Directory (Azure AD) business-to-business (B2B)	
Azure Active Directory business-to-consumer B2C (Azure AD B2C)	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

▾	enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.
Active Directory Domain Services (AD DS)	
Active Directory forest trusts	
Azure Active Directory (Azure AD) business-to-business (B2B)	
Azure Active Directory business-to-consumer B2C (Azure AD B2C)	

NEW QUESTION 116
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 117
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 120
What can you use to provision Azure resources across multiple subscriptions in a consistent manner?

A. Azure Defender
B. Azure Blueprints
C. Azure Sentinel
D. Azure Policy

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

NEW QUESTION 123
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.	○	○
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	○	○
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	○	○

A. Mastered
B. Not Mastered

Answer: A

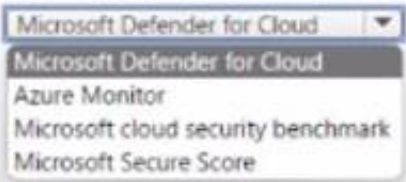**Explanation:**

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

NEW QUESTION 126
HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

Microsoft Defender for Cloud ▼ provides cloud workload protection for Azure and hybrid cloud resources.
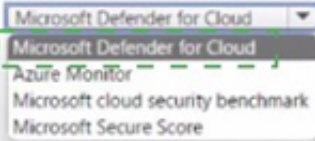
| Microsoft Defender for Cloud |
| Azure Monitor |
| Microsoft cloud security benchmark |
| Microsoft Secure Score |

Answer Area

Microsoft Defender for Cloud ▼ provides cloud workload protection for Azure and hybrid cloud resources.

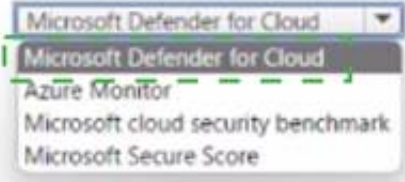| Microsoft Defender for Cloud |
| Azure Monitor |
| Microsoft cloud security benchmark |
| Microsoft Secure Score |

Answer Area

Microsoft Defender for Cloud ▼ provides cloud workload protection for Azure and hybrid cloud resources.

Answer:

Answer Area

Microsoft Defender for Cloud ▼ provides cloud workload protection for Azure and hybrid cloud resources.

| Microsoft Defender for Cloud |
| Azure Monitor |
| Microsoft cloud security benchmark |
| Microsoft Secure Score |

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 131
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 136
What can you use to provide threat detection for Azure SQL Managed Instance?

A. Microsoft Secure Score
B. application security groups
C. Microsoft Defender for Cloud
D. Azure Bastion

Answer: C

NEW QUESTION 138
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 139
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 141
HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

You can manage Microsoft Intune by using the [ ]

Azure Active Directory admin center.
Microsoft 365 compliance center.
Microsoft 365 security center.
Microsoft Endpoint Manager admin center.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

You can manage Microsoft Intune by using the [ ]

Azure Active Directory admin center.
Microsoft 365 compliance center.
Microsoft 365 security center.
Microsoft Endpoint Manager admin center.

NEW QUESTION 146
You need to connect to an Azure virtual machine by using Azure Bastion. What should you use?

A. an SSH client
B. PowerShell remoting
C. the Azure portal
D. the Remote Desktop Connection client

Answer: D

NEW QUESTION 149
HOTSPOT
Select the answer that correctly completes the sentence.
Answer Area

With Windows Hello for Business, a user's biometric data used for authentication [ ]

is stored on an external device.
is stored on a local device only.
is stored in Azure Active Directory (Azure AD).
is replicated to all the devices designated by the user.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text, letter
Description automatically generated
Biometrics templates are stored locally on a device. Reference: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for- business/hello-overview

NEW QUESTION 153
HOTSPOT
Select the answer that correctly completes the sentence.

[ ] 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:

Customer Lockbox	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.
Information barriers	
Privileged Access Management (PAM)	
Sensitivity labels	

NEW QUESTION 156
What is an assessment in Compliance Manager?

A. A grouping of controls from a specific regulation, standard or policy.
B. Recommended guidance to help organizations align with their corporate standards.
C. A dictionary of words that are not allowed in company documents.
D. A policy initiative that includes multiple policies.

Answer: A

Explanation:
Microsoft Purview Compliance Manager is a feature in the Microsoft Purview compliance portal that helps you manage your organization's compliance requirements with greater ease and convenience. Compliance Manager can help you throughout your compliance journey, from taking inventory of your data protection risks to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.
Watch the video below to learn how Compliance Manager can help simplify how your organization manages compliance:
Compliance Manager helps simplify compliance and reduce risk by providing:
? Pre-built assessments for common industry and regional standards and regulations, or custom assessments to meet your unique compliance needs (available assessments depend on your licensing agreement; learn more).
? Workflow capabilities to help you efficiently complete your risk assessments through a single tool.
? Detailed step-by-step guidance on suggested improvement actions to help you
comply with the standards and regulations that are most relevant for your organization. For actions that are managed by Microsoft, you'll see implementation details and audit results.
? A risk-based compliance score to help you understand your compliance posture by
measuring your progress in completing improvement actions.

NEW QUESTION 161
When you enable Azure AD Multi-Factor Authentication (MFA), how many factors are required for authentication?

A. 1
B. 2
C. 3
D. 4

Answer: B

NEW QUESTION 164
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
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	○	○
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	○	○
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	○	○
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	○	○
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	○	○

NEW QUESTION 167
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.	○	○
A single system-assigned managed identity can be used by multiple Azure resources.	○	○
If you delete an Azure resource that has a user-assigned managed identity, the managed identity is deleted automatically.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Device identity can be stored in Azure AD.	⊡	○
A single system-assigned managed identity can be used by multiple Azure resources.	⊡	○
If you delete an Azure resource that has a user-assigned managed identity, the managed identity is deleted automatically.	○	⊡

NEW QUESTION 172
Which pillar of identity relates to tracking the resources accessed by a user?

A. auditing
B. authorization
C. authentication
D. administration

Answer: A

NEW QUESTION 177
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 178
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. phone call
B. text message (SMS)
C. email verification
D. Microsoft Authenticator app
E. security question

Answer: ABD

NEW QUESTION 181
HOTSPOT
Select the answer that correctly completes the sentence.

An Azure resource can use a system-assigned [___ Azure Active Directory (Azure AD) joined device / managed identity / service principal / user identity ___] to access Azure services.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

An Azure resource can use a system-assigned [___ Azure Active Directory (Azure AD) joined device / managed identity / service principal / user identity ___] to access Azure services.

NEW QUESTION 184
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 185
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.	O	O
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	O	O
The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	O	O

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Microsoft Sentinel uses logic apps to identify anomalies across resources.	O	[O]
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	O	[O]
The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	[O]	O

NEW QUESTION 188
What do you use to provide real-time integration between Azure Sentinel and another
security source?

A. Azure AD Connect
B. a Log Analytics workspace
C. Azure Information Protection
D. a data connector

Answer: D

Explanation:
To on-board Azure Sentinel, you first need to connect to your security sources. Azure Sentinel comes with a number of connectors for Microsoft solutions,
including Microsoft 365 Defender solutions, and Microsoft 365 sources, including Office 365, Azure AD, Microsoft Defender for Identity, and Microsoft Cloud App

Security, etc.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/overview

NEW QUESTION 190
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.	○	○
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	○	○
Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
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.

NEW QUESTION 192
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.	○	○
Conditional access policies are evaluated before a user is authenticated.	○	○
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	○	○

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 193
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	○	○
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	○	○
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Global administrators are exempt from conditional access policies	O	Ⓞ
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	O	Ⓞ
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	Ⓞ	O

NEW QUESTION 197
HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

You can use [_____ ▾] in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.
- Reports
- Hunting
- Attack simulator
- Incidents

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

You can use [_____ ▾] in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.
- Reports
- Hunting
- Attack simulator
- Incidents

NEW QUESTION 200
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
Verify explicitly is one of the guiding principles of Zero Trust.	O	O
Assume breach is one of the guiding principles of Zero Trust.	O	O
The Zero Trust security model assumes that a firewall secures the internal network from external threats.	O	O

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
Box 2: Yes
Box 3: No
The Zero Trust model does not assume that everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network.

NEW QUESTION 201
HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

Compliance Manager assesses compliance data [▼] for an organization.

| continually |
| monthly |
| on-demand |
| quarterly |

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Compliance Manager assesses compliance data [▼] for an organization.

| continually |
| monthly |
| on-demand |
| quarterly |

NEW QUESTION 204
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
Software tokens are an example of passwordless authentication.	○	○
Windows Hello is an example of passwordless authentication.	○	○
FIDO2 security keys are an example of passwordless authentication.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Software tokens are an example of passwordless authentication.	○	○
Windows Hello is an example of passwordless authentication.	○	○
FIDO2 security keys are an example of passwordless authentication.	○	○

NEW QUESTION 207
......

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SC-900 Exam with Our Prep Materials Via below:

https://www.certleader.com/SC-900-dumps.html