ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

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
All Azure Active Directory (Azure AD) license editions include the same features.	O'	O
You can manage an Azure Active Directory (Azure AD) tenant by using toe Azure portal.	O	O
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant. 0		O

Answer:

Explanation:

Answer Area

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	O	O
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	O	O
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant. O ' O		

Question: 2

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

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

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

Answer:

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

Reference:
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/

Question: 3

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

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

Answer:

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

Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview

Question: 4
HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

You can manage Microsoft tntune by using the

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

Answer:

Explanation:

Answer Area

You can manage Microsoft tntune by using the

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

Question: 5
HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Federation is used to establish ▼ between organizations, multi-factor authentication (MFA) a trust relationship

Answer:

Explanation:

Answer Area

Federation is used to establish

_____ ▼	between organizations,
multi-factor authentication (MFA)	a trust relationship
user account synchronization	a VPN connection

Federation is a collection of domains that have established trust. Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

Question: 6

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.	O'	O
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	Q	Q
Enabling multi-factor authentication (MFA) increasesan organization's secure score in Azure Security Center.	O	.0

Answer:

Explanation:

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

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.

Reference:
https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls

Question: 7

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

Question: 8

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

Question: 9

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

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

Answer: C

Explanation:

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

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

Question: 10

In the shared responsibility model for an Azure deployment, what is Microsoft solely responsible for managing?

A. the management of mobile devices
B. the permissions for the user data stored in Azure
C. the creation and management of user accounts
D. the management of the physical hardware

Answer: D

Explanation:

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
Verify explicitly is one of the guiding principles of Zero Trust.	0	0
Assume breach is one ofthe guiding principles of Zero Trust.	0	E
The Zero Trust security model assumes that a firewall secures the internal network from Q external threats.		El

Answer:

Explanation:

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.	0	0
The Zero Trust security model assumes that a firewall secures the internal network from external threats.	Q	Q

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.

Reference:

https://docs.microsoft.com/en-us/security/zero-trust/

Question: 12

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

Control is a key privacy principle of Microsoft.	0	O
Transparency is a key privacy principle of Microsoft.	O	O
Shared responsibility is a key privacy principle of Microsoft. O		O

Answer:

Explanation:

Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	o	o
Transparency is a key privacy principle of Microsoft.	o	o
Shared responsibility is a key privacy principle of Microsoft. O		O

Reference: https://privacy.microsoft.com/en-US/

Question: 13

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

Answer:

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

Question: 14

What can you use to provide a user with a two-hour window to complete an administrative task in Azure?

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. Azure Multi-Factor Authentication (MFA)
C. Azure Active Directory (Azure AD) Identity Protection
D. conditional access policies

Answer: D

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim- configure
Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management: Provide just-in-time privileged access to Azure AD and Azure resources Assign time-bound access to resources using start and end dates Require approval to activate privileged roles Enforce multi-factor authentication to activate any role Use justification to understand why users activate Get notifications when privileged roles are activated Conduct access reviews to ensure users still need roles Download audit history for internal or external audit Prevents removal of the last active Global Administrator role assignment

Question: 15

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:

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

Question: 16

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).	O	O
Global administrator is a role in Azure Active Directory (Azure AD).	O	O
An Azure Active Directory (Azure AD) user can be assigned only one role.	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
You can create custom roles in Azure Active Directory (Azure AD).	0	0
Global administrator is a role in Azure Active Directory (Azure AD).	0	E
An Azure Active Directory (Azure AD) user can be assigned only one role.	0	0

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

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/concept-understand-roles
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Question: 17

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 onpremises environment.	®	0
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	O	0
Azure Active Directory (Azure AD) is an identity and access management service.	0	0

Answer:

Explanation:

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) is deployed to an onpremises environment.		
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.		O
Azure Active Directory (Azure AD) is an identity and access management service.	O	

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.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide

Question: 18

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

With Windows Hello for Business, a users 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.

Answer:

Explanation:

Answer Area

With Windows Hello for Business, a users biometric data used for authentication rs 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.

Biometrics templates are stored locally on a device. Reference:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

Question: 19

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:

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

Question: 20

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:

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

Question: 21

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Multi-factor authentication (MFA)	requires additional verification, such as a verification code sent to a mobile phone.
Pass-through authentication	
Password writeback	
Single sign-on (SSO)	

Answer:

Explanation:

Answer Area

Multi-factor authentication (MFA)	requires additional verification, such as a verification code sent to a mobile phone.
Pass-through authentication	
Password writeback	
Single sign-on (SSO)	

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.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Question: 22

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
Conditional access policies can use the device state as a signal.	o	o
Conditional access policies apply before first-factor authentication is complete.	O	O
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	Q	O

Answer:

Explanation:

Answer Area

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

Box 1: Yes

Box 2: No

Conditional Access policies are enforced after first-factor authentication is completed. Box 3: Yes

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Question: 23

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Microsoft Cloud App Security
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Defender for Office 365

- is a cloud-based solution that leverages on-premises Active Directory signals ' to identify, detect, and investigate advanced threats,

Answer:

Explanation:

Answer Area

Microsoft Cloud App Security
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Defender for Office 365

■■ is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats,

Reference:
https://docs.microsoft.com/en-us/defender-for-identity/what-is

Question: 24

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)
| Aztire AD Coffnect
on-premises Active Directory Domain Services (AD DS)

Answer:

Explanation:

Answer Area

Microsoft Defender for Identity can identify advanced threats from _____ - signals.

Azure Active Directory (Azure AD)
A/ljrt'All Ccillliyr.r on-premises Active Directory Domain Services (AD DS)

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.

Reference:
https://docs.microsoft.com/en-us/defender-for-identity/what-is

Question: 25

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

Answer:

Explanation:

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

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

Question: 26

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

manage Azure resources?

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

Answer: C

Explanation:

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

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

Question: 27

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Azure Defender
Azure Sentinel
Microsoft Cloud App Security

can use conditional access policies to control sessions in realtime

Answer:

Explanation:

Answer Area

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Ah#fe Defender
Azure Sentinel
Microsoft Cloud App Security

can use conditional access policies to control sessions in real time.

Reference:
https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

Question: 28

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.

Answer:

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.

Reference:
https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

Question: 29

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

Question: 30

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

You can use ^ in the Microsoft 365 security center to identify devices that are affected by an aiert.
classifications incidents policies Secure score

Answer:

Explanation:

Answer Area

You can use -in the Microsoft 365 security center to identify devices that are affected by an aiert.
classifications incidents policies Secure score

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide

Question: 31

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

Question: 32

DRAG DROP

Match the Azure networking service to the appropriate description.

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

NOTE: Each correct match is worth one point.

Services	Answer Area
Azure Bastion	Provides Network Address Translation (NAT) services
Azure Firewall	Provides secure and seamless Remote Desktop connectivity to Azure virtual machines
Network security group (NSG)	Provides traffic filtering that can be applied to specific network interfaces on a virtual network

Answer:

Explanation:

Services	Answer Area
Azure Bastion	Azure Firewall provides Network Address Translation (NAT) services
Azure Firewall	Azure Bastion Provides secure and seamless Remote Desktop connectivity to Azure virtual machines
Network security group (NSG)	Network security group (NSG) Provides traffic filtering that can be applied to specific network interfaces on a virtual network

Box 1: Azure Firewall

Azure Firewall provide Source Network Address Translation and Destination Network Address Translation.

Box 2: Azure Bastion

Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.

Box 3: Network security group (NSG)

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network.

Reference:

https://docs.microsoft.com/en-us/azure/networking/fundamentals/networking-overview https://docs.microsoft.com/en-us/azure/bastion/bastion-overview https://docs.microsoft.com/en-us/azure/firewall/features

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Question: 33
HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

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

Answer:

Explanation:

Answer Area

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

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

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

Question: 34
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 Defender can detect vulnerabilities and threats far Azure Storage.	O'	O
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	O	0
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	Q	Q

Answer:

Explanation:

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

Box 1: Yes
Azure Defender provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, your storage, and more

Box 2: Yes
Cloud security posture management (CSPM) is available for free to all Azure users.

Box 3: Yes
Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

Reference:
https://docs.microsoft.com/en-us/azure/security-center/azure-defender

https://docs.microsoft.com/en-us/azure/security-center/defender-for-storage-introduction
https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction

Question: 35
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.

Answer:

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.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/threat-analytics?view=o365- worldwide

Question: 36

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.	o	Q
Advanced Audit in Microsoft 365 supports the same retention period of audit logs as core auditing.	O	O
Advanced Audit in Microsoft 365 allocates customer-dedicated bandwidth for accessing audit data.	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
With Advanced Audit in Microsoft 365, you can identify when email items were accessed.	O	
Advanced Audit in Microsoft 365 supports the same retention period of audit logs as core auditing.	O	
Advanced Audit in Microsoft 365 allocates customer-dedicated bandwidth for accessing audit data.	O	

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.

Reference:

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

https://docs.microsoft.com/en-us/microsoft-365/compliance/auditing-solutions- overview?view=o365-worldwide#licensing-requirements

https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service- descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security- compliance-licensing-guidance#advanced- audit

Question: 37

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 o O groups based on the users' risk level.		
Azure Active Directory (Azure AD) Identity Protection can detect whether o user credentials were leaked to the public.	0	
Azure Active Directory (Azure AD) Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	O	O

Answer:

Explanation:

Answer Area

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

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.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity- protection
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept- identity-protection-risks
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

Question: 38

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

Question: 39

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

Question: 40

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Compliance Manager assesses compliance data for an organization.

continually monthly on-demand quarterly

Answer:

Explanation:

Answer Area

Compliance Manager assesses compliance data for an organization.

continually monthly on-demand quarterly

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365- worldwide#how-compliance-manager-continuously-assesses-controls

Question: 41

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.	O	0
Sensitivity labels can add headers and footers to documents.	0	O
Sensitivity labels can apply watermarks to emails.	0	o

Answer:

Answer Area

Statements	Yes	No
Sensitivity labels can be used to apply encryption to documents.	•	
Sensitivity labels can be used to add headers and footers to documents.	•	0
Sensitivity labels can be used to apply watermarks to emails.	0	9

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

Question: 42

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

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
Compliance Manager tracks only customer-managed controls.	O	O
Compliance Manager provides predefined templates for creating assessments.	O	O
Compliance Manager can help you asses whether data adheres to specific data protection standards.	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
Compliance Manager tracks only customer-managed controls, o	O	
Compliance Manager provides predefined templates for O creating assessments.	O	
Compliance Manager can help you asses whether data adheres to specific data protection standards.	O	

Box 1: No

Compliance Manager tracks Microsoft managed controls, customer-managed controls, and shared controls.

Box 2: Yes

Box 3: Yes

Reference:

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

Question: 44

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.	o	H
Azure Policy can be used to ensure that new resources adhere o to corporate standards.		o
Compliance evaluation in Azure Policy occurs only when a O target resource is created or modified.		o

Answer:

Explanation:

Answer Area

Statements	Yes	No
Azure Policy supports automatic remediation.	○	○
Azure Policy can be used to ensure that new resources adhere to corporate standards.	○	○
Compliance evaluation in Azure Policy occurs only when a target resource is created or modified.	○	○

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

Question: 45

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:

Question: 46

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

Question: 47

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

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
Network security groups (NSGs) can deny inbound traffic from the internet	O	O

Network security groups (NSGs) can deny outbound traffic to the internet	O	O
Network security groups (NSGs) can filter traffic based on IP address. protocol, and port	O	O

Answer:

Explanation:

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	O	O
Network security groups (NSGs) can deny outbound traffic to the internet	O	O
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port	O	O

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. For each rule, you can specify source and destination, port, and protocol.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Question: 49

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 Intune can be used to manage Android devices.	O	O
Microsoft Intune can be used to provision Azure subscriptions	O	O
Microsoft Intune can be used to manage organization-owned devices and personal devices	O	O

Answer:

Explanation:

Statements	Yes	No
Microsoft Intune can be used to manage Android devices	O	O
Microsoft Intune can be used to provision Azure subscriptions	O	O
Microsoft Intune can be used to manage organization-owned devices and personal devices	O	O

Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune
https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management

Question: 50

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	O	O
Azure Bastion provides secure user connections by using RDP	O	O
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal	O	O

Explanation:

Answer:

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

Reference:

https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

https://docs.microsoft.com/en-us/azure/bastion/tutorial-create-host-portal

Question: 51

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
Digitally signing a document requires a private key.	0	0
Verifying the authenticity of a digitally signed document requires the public key of the signer.	o	0
Verifying the authenticity of a digitally signed document requires the private key of the singer.	i^i	0

Answer:

Explanation:

Box 1: Yes
A certificate is required that provides a private and a public key.

Box 2: Yes
The public key is used to validate the private key that is associated with a digital signature.

Box 3: Yes

Reference:
https://support.microsoft.com/en-us/office/obtain-a-digital-certificate-and-create-a-digital- signature-e3d9d813-3305-4164-a820-2e063d86e512

https://docs.microsoft.com/en-us/dynamics365/fin-ops-core/fin-ops/organization-administration/electronic-signature-overview

Question: 52

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.

Answer:

When users sign in to the Azure portal, they are first assigned permissions, authenticated. _____ authorized resolved.

Question: 53

HOTSPOT

Select the answer that correctly completes the sentence.

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

Authentication Authorization Federation
Single sign-on (SSO)

Answer:

Explanation:

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

Authentication

Authorization Federation
Single sign-on (SSO)

Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization

Question: 54

HOTSPOT

Select the answer that correctly completes the sentence.

Active Director DornainServices (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)

enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.

Answer:

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)

enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

Question: 55

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

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

Question: 56

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
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	0	0
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	0	0
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	0	0

Answer:

Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	0	o
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	O	El
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	0	0

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
Azure AD Connect can be used to implement hybrid identity.	0	0
Hybrid identity requires the implementation of two Microsoft 365 tenants.	0	0
Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	0	0

Answer:

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	O	O
Hybrid identity requires the implementation of two Microsoft 365 tenants.	O	O

Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD). o o

Question: 58

HOTSPOT

Select the answer that correctly completes the sentence.

v provides benchmark recommendations and guidance for protecting Azure services.

Azure Application Insights
Azure Network Watcher
Log Analytics workspaces
Security baselines for Azure

Answer:

provides benchmark recommendations and guidance for protecting Azure services.

Azure Application Insights
Azure Network Watcher
Log Analytics workspaces
Security baselines for Azure

Reference:
https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/cloud-services-security-baseline

Question: 59

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

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

Question: 60

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

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

Question: 61

HOTSPOT

Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

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

Answer:

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

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

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
Conditional access policies can be applied to global administrators.	0	0
Conditional access policies are evaluated before a user is authenticated.	0	0
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	0	0

Answer:

Statements	Yes	No
Conditional access policies can be applied to global administrators.	O	0
Conditional access policies are evaluated before a user is authenticated.	0	1°
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	0	0

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.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Question: 63

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.

Answer:

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

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

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

Question: 64

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

Reference:

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

Question: 65

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.

Answer:

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.

Reference:

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

Question: 66

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

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

Question: 67

HOTSPOT

Select the answer that correctly completes the sentence.

In Azure Sentinel, you can automate common tasks by using

deep investigation tools.
hunting search-and-query tools.
playbooks.
workbooks.

Answer:

In Azure Sentinel, you can automate common tasks by using

deep investigation tools.
hunting search-and-query tools playbooks.
workbooks.

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

Question: 68

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

NOTE: Each correct selection is worth one point.

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

Answer: D, E

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

Question: 69

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

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

Question: 70

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 Endpoint can protect Android devices.	O	O
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	O	O
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	O	O

Answer:

Statements	Yes	No
Microsoft Defender for Endpoint can protect Android devices	O	O
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	Q	Q
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses		

Question: 71

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

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

Question: 72

Which feature provides the extended detection and response (XDR) capability of Azure Sentinel?

A. integration with the Microsoft 365 compliance center
B. support for threat hunting
C. integration with Microsoft 365 Defender
D. support for Azure Monitor Workbooks

Answer: C

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365- worldwide

Question: 73

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

Question: 74

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 Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	O	O
From the Microsoft 365 security center, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	O	O
Microsoft Secure Score in the Microsoft 365 security center gives you points if you address the improvement action by using a third-party application or software.	O	O

Answer:

Statements	Yes	No
Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	O	O
From the Microsoft 365 security center, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	O	O
Microsoft Secure Score in the Microsoft 365 security center gives you points if you address the improvement action by using a third-party application or software.	O	O

Question: 75

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

Question: 76

HOTSPOT

Select the answer that correctly completes the sentence.

Azure Defender
The Microsoft 365 compliance center
The Microsoft 365 security center
Microsoft Endpoint Manager

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

Answer:

Azure Defender
The Microsoft 365 compliance center
The Microsoft 365 security center
Microsoft Endpoint Manager

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

Reference:

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

MIP capabilities are included with Microsoft 365 Compliance and give you the tools to know your data, protect your data, and prevent data loss.

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

Question: 77

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

A. retention policies
B. data loss prevention (DLP) policies
C. conditional access policies

D. information barriers

Answer: B

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

Question: 78

HOTSPOT

Select the answer that correctly completes the sentence.

lockbox v can be used to provide Microsoft Support Engineers with access to an organization's data Customer stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.

Information barriers
Privileged Access Management (PAM)
Sensitivitylabels

Answer:

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

Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview

Question: 79

In a Core eDiscovery workflow, what should you do before you can search for content?

A. Create an eDiscovery hold.
B. Run Express Analysis.
C. Configure attorney-client privilege detection.

D. Export and download results.

Answer: A

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwide

Question: 80

Which Microsoft portal provides information about how Microsoft manages privacy, compliance, and security?

A. Microsoft Service Trust Portal
B. Compliance Manager
C. Microsoft 365 compliance center
D. Microsoft Support

Answer: A

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

Question: 81

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

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

Question: 82

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

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

Question: 83

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.	O	O
You can use Advanced Audit in Microsoft 365 to view the contents of an email message.	0	O
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.	C}	n

Answer:

Statements	Yes	No
You can use Advanced Audit in Microsoft 365 to view billing details.	0	O
You can use Advanced Audit in Microsoft 365 to view the contents of an email message.	0	0
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.	0	0

Box 1: No

Advanced Audit helps organizations to conduct forensic and compliance investigations by increasing audit log retention.

Box 2: No

Box 3: Yes

Reference:

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

Question: 84

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.	0	o
You can add only one resource lock to an Azure resource.	0	0
You can delete a resource group containing resources that have resource locks.	0	0

Answer:

Yes
NO
NO
YES - As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.
NO - The most restrictive lock in the inheritance takes precedence.
NO - If you delete a resource group with a locked resource, the portal UI will give you an error and no resources are deleted.

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

Question: 85

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.	0	0
Multiple sensitivity labels can be applied to the same file.	O	0
A sensitivity label can apply a watermark to a Microsoft Word document.	0	0

Answer:

Statements	Yes	No
Users can apply sensitivity labels manually.	O	O
Multiple sensitivity labels can be applied to the same file.	O	O
A sensitivity label can apply a watermark to a Microsoft Word document.	O	O

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity- labels?view=o365-

worldwide

Question: 86

Which three statements accurately describe the guiding principles of Zero Trust? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Define the perimeter by physical locations.
B. Use identity as the primary security boundary.
C. Always verity the permissions of a user explicitly.
D. Always assume that the user system can be breached.
E. Use the network as the primary security boundary.

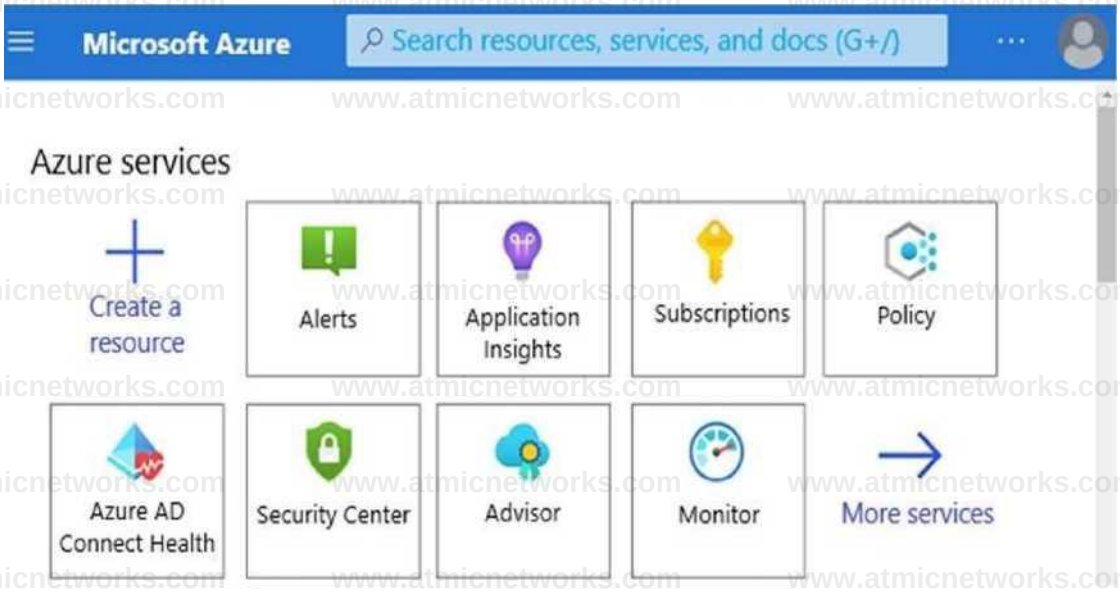
Answer: BCD

Reference:
https://docs.microsoft.com/en-us/security/zero-trust/

Question: 87

HOTSPOT

Which service should you use to view your Azure secure score? To answer, select the appropriate service in the answer area.



Answer:

Security Center

Reference:

https://docs.microsoft.com/en-us/azure/security-center/secure-score-access-and-track

Question: 88

You have an Azure subscription.You need to implement approval-based, tiProme-bound role activation.

What should you use?

A. Windows Hello for Business
B. Azure Active Directory (Azure AD) Identity Protection
C. access reviews in Azure Active Directory (Azure AD)
D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Answer: D

Reference:

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

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
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		

Answer:

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		

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional- access-policy-admin-mfa

Question: 90

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

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

Question: 91

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

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

Question: 92

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: B, C, D

Question: 93

You have a Microsoft 365 E3 subscription.

You plan to audit user activity by using the unified audit log and Basic Audit.

For how long will the audit records be retained?

A. 15 days
B. 30 days
C. 90 days
D. 180 days

Answer: C

Question: 94

To which type of resource can Azure Bastion provide secure access?

A. Azure Files
B. Azure SQL Managed Instances
C. Azure virtual machines
D. Azure App Service

Answer: C

Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.

Reference:
https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

Question: 95

What are three uses of Microsoft Cloud App Security? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.to discover and control the use of shadow IT

A. to provide secure connections to Azure virtual machines
B. to protect sensitive information hosted anywhere in the cloud
C. to provide pass-through authentication to on-premises applications

D. to prevent data leaks to noncompliant apps and limit access to regulated data

Answer: ACE

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

Question: 96

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 the insider risk management solution to detect phishing scams.	○	○
You can access the insider risk management solution from the Microsoft 365 compliance center.	○	○
You can use the insider risk management solution to detect data leaks by unhappy employees.	○	○

Answer:

Box 1: No
Phishing scams are external threats.

Box 2: Yes
Insider risk management is a compliance solution in Microsoft 365.

Box 3: Yes

Insider risk management helps minimize internal risks from users. These include:

Leaks of sensitive data and data spillage

Confidentiality violations

Intellectual property (IP) theft

Fraud

Insider trading

Regulatory compliance violations

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide

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

Question: 97

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

Answer:

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

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide

Question: 98

HOTSPOT

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

NOTE: Each correct selection is worth one point

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

Answer:

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

Question: 99

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

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

Question: 100

HOTSPOT

Select the answer that correctly completes the sentence.

Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Defender for Office 365

is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.

Answer

Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Defender for Office 365

is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.

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.

Question: 101

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: A, D

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

Question: 102

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 i Provides real-time reports to identify and analyze recent threats
Anti-phishing protection	Feature . Detects impersonation attempts

Answer:

Explanation:

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

Question: 103

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

Explanation:

Question: 104

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: A

Explanation:

Question: 105

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.

Question: 106

You need to create a data loss prevention (DLP) policy. What should you use?

A. the Microsoft 365 admin center
B. the Microsoft Endpoint Manager admin center
C. the Microsoft 365 Defender portal
D. the Microsoft 365 Compliance center

Answer: A

Explanation:

Question: 107

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
You can use information barriers with Microsoft Exchange.	
You can use information barriers with Microsoft SharePoint.	
You can use information barriers with Microsoft Teams.	

Answer

Explanation:

Statements
You can use information barriers with Microsoft Exchange.
You can use information barriers with Microsoft SharePoint
You can use information barriers with Microsoft Teams.

Question: 108

HOTSPOT

Select the answer that correctly completes the sentence.

A domain controller Active Directory Domain Services (AD DS) Azure Active Directory (Azure AD) Privilege Identity Management (PIM)	Federation provides single sign-on (SSO) capabilities across multiple identity providers.

Answer

Explanation:

A domain controller Active Directory Domain Services (AD DS) Azure Active Directory (Azure AD) Privilege Identity Management (PIM) Federation	provides single sign-on (SSO) capabilities across multiple identity providers.

Question: 109

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

Explanation:

Question: 110

HOTSPOT

Select the answer that correctly completes the sentence.

In an environment that has on-premises resources and cloud resources, should be the primary security perimeter.

the cloud a firewall identity Microsoft Defender for Cloud

Answer:

Explanation:

In an environment that has on-premises resources and cloud resources, should be the primary security perimeter, the cloud

a firewall

identity

Microsoft Defender for Cloud

Question: 111

HOTSPOT

Select the answer that correctly completes the sentence.

Azure Active Directory (Azure AD) joined device managed identity service principal user identity

An Azure resource can use a system-assigned to access Azure services.

managed identity
service principal user identity

Answer:

Explanation:

An Azure resource can use a system-assigned to access Azure services.

Azure Active Directory (Azure AD) joined device

Question: 112

Which compliance feature should you use to identify documents that are employee resumes?

A. pre-trained classifiers
B. Content explorer
C. Activity explorer
D. eDiscovery

Answer: A

Explanation:

Question: 113

HOTSPOT

Select the answer that correctly completes the sentence.

Compliance Manager can be directly accessed from the

Microsoft 365 admin center.
Microsoft 365 Defender portal.
Microsoft 365 Compliance Center
Microsoft Support portal.

Answer:

Explanation:

Compliance Manager can be directly accessed from the

[Microsoft 365 admin center.
Microsoft 365 Defender portal.
Microsoft 365 Compliance Center
Microsoft Support portal.

Question: 114

HOTSPOT

Select the answer that correctly completes the sentence.

Microsoft Sentinel

analytic rules
hunting queries
playbooks
workbooks

use Azure Logic Apps to automate and orchestrate responses to alerts.

Answer:

Explanation:

playbooks

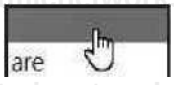
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Question: 115

HOTSPOT

Select the answer that correctly completes the sentence.

When using multi-factor authentication (MFA), a password is considered something you



Answer:

Explanation:

When using multi-factor authentication (MFA), a password is considered something you

Multifactor authentication combines two or more independent credentials: what the user knows, such as a password; what the user has, such as a security token; and what the user is, by using biometric verification methods.

Question: 116

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: A, B, D

Explanation:

Question: 117

What should you use to ensure that the members of an Azure Active Directory group use multi-factor authentication (MFA) when they sign in?

A. Azure Active Directory (Azure AD) Identity Protection
B. a conditional access policy
C. Azure role-based access control (Azure RBAC)

D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Answer: B

Explanation:

The recommended way to enable and use Azure AD Multi-Factor Authentication is with Conditional Access policies. Conditional Access lets you create and define policies that react to sign-in events and that request additional actions before a user is granted access to an application or service.

Question: 118

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

Explanation:

Question: 119

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 Sentinel data connectors support only Microsoft services.		
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.		
Hunting provides you with the ability to identify security threats before an alert is triggered.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	○	®
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel. •		
Hunting provides you with the ability to identify security threats before an aleri is $ triggered		

Question: 120

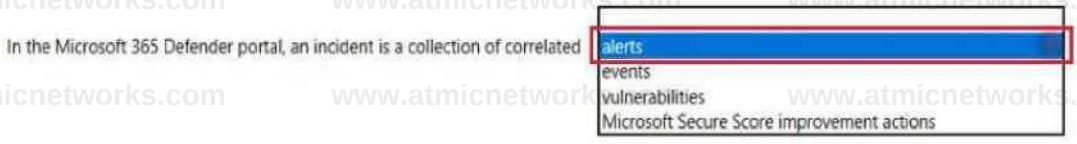
HOTSPOT

Select the answer that correctly completes the sentence.

In the Microsoft 365 Defender portal an incident is a collection of correlated events [alerts / vulnerabilities / Microsoft Secure Score improvement actions]

Answer:

Explanation:



Question: 121

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.		

Answer:

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 Good can evaluate the security of workloads deployed to Azure ■• or on-premises.		

Question: 122

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.		

Answer:

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.		

Question: 123

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: B, C

Explanation:

Question: 124

HOTSPOT

Select the answer that correctly completes the sentence.

Azuie Active Directory (Azure AD) Privileged Identity Management (PIM)
Microsoft Defender for Cloud
MkrpsgftSentinel

Microsoft Defender for Cloud Apps can use conditional access policies to control sessions in real time

Answer:

Explanation:

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Microsoft Defender for Cloud
Miciosoft Sentinel
| Microsoft Defender for Cloud Apps can use conditional access policies to control sessions in real time

Question: 125

Which service includes the Attack simulation training feature?

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

Explanation:

Answer: B

Question: 126

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.

Answer:

Explanation:

You can use dynamic groups in Azure Active Directory (Azure AD) to automate the access obiect | privileged access lifecycle process.

Question: 127

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

Explanation:

Question: 128

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

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

Answer: B

Explanation:

Question: 131

You plan to move resources to the cloud.

You are evaluating the use of Infrastructure as a service (IaaS),

Platform as a service (PaaS), and Software as a service (SaaS) cloud models.

You plan to manage only the data, user accounts, and user devices for a cloud-based app.

Which cloud model will you use?

A. IaaS

B. SaaS

C. PaaS

Answer: B

Explanation:

Question: 132

You have an Azure subscription that contains a Log Analytics workspace.

You need to onboard Microsoft Sentinel.

What should you do first?

A. Create a hunting query.

B. Correlate alerts into incidents.

C. Connect to your security sources.

D. Create a custom detection rule.

Answer: C

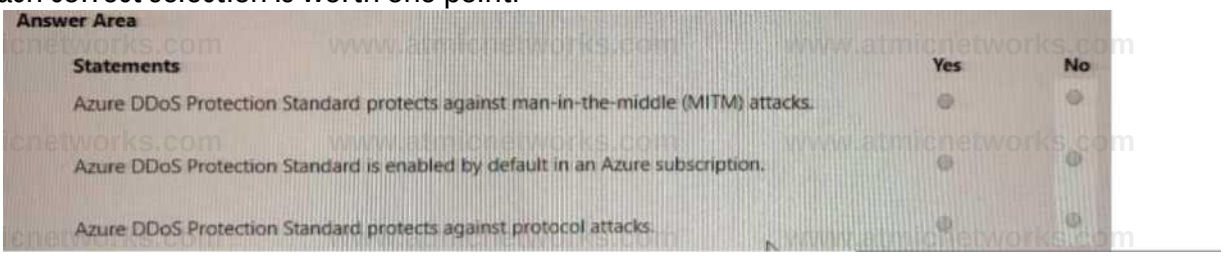
Explanation

Question: 133

HOTSPOT

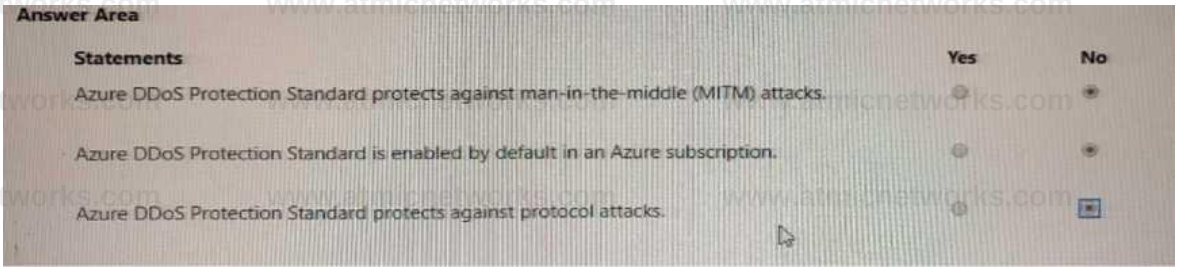
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



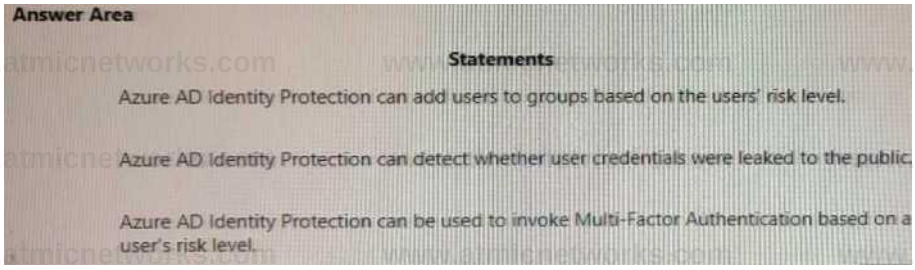
Answer:

Explanation:



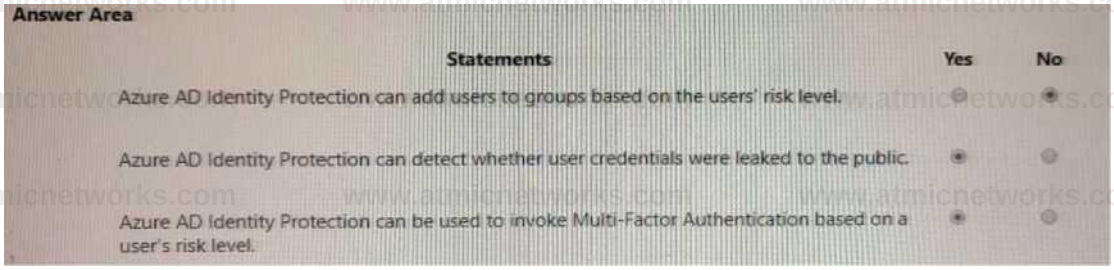
Question: 134

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:

Explanation:



Question: 135

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

Explanation:

Question: 136

Which Microsoft Defender for Cloud metric displays the overall security health of an Azure subscription?

A. resource health
B. secure score
C. the status of recommendations
D. completed controls

Answer: B

Explanation:

Question: 137

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

Explanation:

Question: 138

What is a function of Conditional Access session controls?

A. prompting multi-factor authentication (MFA)
B. enable limited experiences, such as blocking download of sensitive information
C. enforcing device compliance
D. enforcing client app compliance

Answer: A

Explanation:

Conditional Access session controls enable user app access and sessions to be monitored and controlled in real time based on access and session policies.
Based on this definition, the best answer for your question is B. enable limited experiences, such as blocking download of sensitive information.

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional- access-session

Question: 139

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 Are*

Statement!	Ye*	No
Device identity can be noted 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 u deleted automatically		

Answer:

Explanation:
Answer Area

Statement!	Yea	No
Device identity can be stereo In Azure AD	•	
A single system-essigned managed identity ran 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		•

Question: 140

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: B, C

Explanation:

Question: 141

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

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

Answer: A

Explanation:

Question: 142

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Are*

When users sign n Ir-i-vjvin yj writes then credentials to prow their identity.

Mministritian auditing

•uihentKitKin

*uthorir*non

Answer

Explanation:

Answer Area

When users sign in, authentication verifies their credentials to prove their identity.

Question: 143

What can be created in Active Directory Domain Services (AD DS)?

A. line-of-business (106) applications that require modem authentication
B. mob devices
C. computer accounts
D. software as a service (SaaS) applications that require modem authentication

Answer: C

Explanation:

Question: 144

HOTSPOT
Select the answer that correctly completes the sentence.
Answer Area

| MMQV/I >^> for Cloud * | provides doud wortdoad protection tor Azure and hytno doud resources

pMicrosott Detender for Good

Azure Monitor
Microsoft cloud security benchmark
Microsoft Secure Score

Answer:

Explanation:

Answer Area

M«r:;wft CMender tor C loud * provides doud workload protection tot Azure and hybrid doud resources

Question: 145

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

Statement!	Vw No
An enemai email MOfess on be used to authenticate self service password reset (SSPR)	
A notification to the Microsoft Authenticator app can be used to authenticate serf-service password reset (SSPR)	
To perform serf-service password reset (SSPR; a user must already be sipned m and authenticated to Azure AD	

Answer:

Explanation:

Answer Area

Statements	Yes	No
An external email address can be used to authenticate self-service password reset (SSPR)	•	
A notification to the Microsoft Authenticator app can be used to authenticate sell- sei vice password reset (SSPR)	®	O
To perform self-service password reset (SSPR), a user must already be signed in and authenticated to Microsoft Entra ID		•

Question: 146

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Mien you enable security defaults in Azure AD

Azure AD Pnw leged Idcnbty Management (PIM i * wH be enabled for all Azure AD users

Azure AD Identity Protection

Azure AD Ptnniegcd Identity Management (PIM)

mufti-tectoi authentication (MFA)

Answer

Explanation:

Answer Area

When you enable security defaults m Azure AD

Azure AD Privileged Identity Management (PIM) nil be enabled for ail Azure AD users

Question: 147

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Microsoft Sentinel proves quick insights into dau Dy using AzuirU

Azmi? Menitor workbook templates
Azure Resource Graph hplcrer
playbooks

Answer:

Explanation:

Answer Area

Microsoft Sentinel provides quick insights nto data Dy using Azure i ogi< Api

Question: 148

HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

Insider risk management is conjured from the | Microsoft Purview compkarwe portal ^
Microsoft 365 admin centei
Microsoft 365 Defender portal
Microsoft Defender for Cloud Apps portal

Answer

Explanation:

Answer Area

Insider risk management is configured from the | Microsoft Purview compliance portal.

Question: 149

HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

in the Microsoft tV.jew compliance porta you can use 1i ' IL | to remove features from tire natation pane.
Compliance Manager
■Customize navigarion
^0*Qf5
Settings

Answer:

Explanation:

Answer Area

In the Microsoft Purview compliance portal, you can use Customize navigation to remove features from the navigation pane.

Question: 150

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Ensuring that the data you retrieve a the sane as the data you stored a an example of maintaining ^.u.»t.; t, availability

confidentiality integrity transparency.

Answer:

Explanation:

Answer Area

Ensunng that the data you retrieve is the same as the data you stored ts an example of maintaining avaMxiit,

Question: 151

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Microsoft Purview Compliance Manager assesses compliance data continually T for an organization.

continually

monthly on-demand quarterly

Answer:

Explanation:

Answer Area

Microsoft Purview Compliance Manager assesses compliance data continually for an organization.

Question: 152

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.

Action Subcategories

I Corrective

Detect <ve

I Preventative

Answer Area

Encrypt data at rest

Perform a system access audit.

Make configuration changes in response to a security incident.

Answer:

Explanation:

Action Subcategories

Corrective

Detective

Preventative

Answer Area

Preventative — Encrypt data al rest

Detective — Perform a system access audit.

Corrective — Make configuration changes in response to a security incident.

Question: 153

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.		
Microsoft SharePoint Online supports communication compliance.		
Communication compliance can remediate compliance issues.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Communication compliance is configured by using the Microsoft 365 admin center.	•	
Microsoft SharePoint Online supports communication compliance.	*	
Communication compliance can remediate compliance issues.	O	t

Question: 154

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

Answer

Explanation:

Answer Area

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

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
Windows Hello for Business can use the Microsoft Authenticator app as an authentication O method.		
Windows Hello for Business can use a PIN code as an authentication method.		
Windows Hello for Business authentication information syncs across all the devices registered by a user.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	O	•
Windows Hello for Business can use a PIN code as an authentication method.	•	
Windows Hello for Business authentication information syncs across all the devices registered by a user.	O	•

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.

Answer Area

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

Answer:

Explanation:

Answer Area

Statements	Yes	No
You can create a hybrid identity in an on-premises Active Directory that syncs to Azure AD. ■		
User accounts created in Azure AD sync automatically to an on-premises Active Directory.		•
When using a hybrid model, authentication can either be done by Azure AD or by another • identity provider		

Question: 157

HOTSPOT

Select the answer that correctly completes the sentence.

Answer

Explanation:

Question: 158

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

Explanation:

Question: 159

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

Explanation:

Question: 160

Which security feature is available in the free mode of Microsoft Defender for Cloud?

A. vulnerability scanning of virtual machines
B. secure score
C. just-in-time (JIT) VM access to Azure virtual machines
D. threat protection alerts

Answer: B

Explanation:

Question: 161

HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

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

Answer:

Explanation:

Answer Area

When users attempt to access an application or a service, authentication ' controls their level of access.

Question: 162

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

Explanation:

Question: 163

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 generates risk detections once a user is authenticated.	O	O
Azure AD identity Protection assigns a risk level of low. Medium, or High to each risk event.	O	O
A user risk in Azure AD Identity Protection represents the probability that a given identity or account is compromised.	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
Azure AD identity Protection generates risk detections once a user is authenticated.	®	O
Azure AD identity Protection assigns a risk level of Low, Medium, or High to each risk event.	©	O
A user risk in Azure AD Identity Protection represents the probability that a given identity or account is compromised.	▪	O

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.

Answer Area

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	O	O
Hybrid identity requires the implementation of two Microsoft 365 tenants.	O	O
Authentication of hybrid identities requires the synchronization of Active Directory Domain Services (AD OS) and Azure AD.	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	®	O
Hybrid identity requires the implementation of two Microsoft 365 tenants.	O	®
Authentication of hybrid identities requires the synchronizationof Active Directory Domain Services (AD DS) and Azure AD,	®	O

Question: 165

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,	O	O
Windows Hello is an example of passwordless authentication.		
FIDO2 security keys are an example of passwordless authentication.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Software tokens are an example of passwordless authentication.		•

Windows Hello is an example of passwordless authentication.	■S'	0
FIDO2 security keys are an example of passwordless authentication.	®	

Question: 166

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 restrict communication between users in Exchange Online by using Information Barriers.	0	0
You can restrict accessing a SharePoint Online site by using Information Barriers.	O	O
You can prevent sharing a file with another user in Microsoft Teams by using informatton Barriers.	0	O

Answer:

Explanation:

Answer Ares

Statements	Yes	No
You can restrict communicat ion between wets in Exchange Online by using Information Barriers.	•	o
You can restrict accessing a SharePoint Online site by using Information Barriers.	@	o
You can prevent sharing a hie with another user in Microsoft Teams by using information Barriers.	•	o

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
Microsoft Sentinel uses logic apps to identify anomalies across resources.	o	o
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	0	O
tie hunting search-arid query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	o	

Answer:

Explanation:

Answer Area

Statements	Yes	No
Microsoft Sentinel uses logic apps to identify anomalies across resources.	0	9
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	0	®
The hunting search and quenr tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	e	0

Question: 168

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

Explanation:

Question: 169

HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

Answer:

Explanation:

Answer Area

Federation — T provides single sign-on (SSO} capabilities across multiple identity providers.

Question: 170

DRAG DROP

Match the types of Conditional Access signals to the appropriate definitions.

To answer, drag the appropriate Conditional Access signal type from the column on the left to its definition on the right. Each signal type may be used once, more than once, or not at all. NOTE: Each correct match is worth one point.

Conditional access signals

- Device
- Location
- Sign-in risk
- User risk

Answer Area

me probability that an Identity or account is compromised.

The probability that an authentication request isn't authorized by the identity owner.

Answer:

Conditional access signals

- Device
- Location
- Sign-in risk
- User risk

Answer Area

User risk	The probability that an identity or account is compromised.
Sign-in risk	The probability that an authentication request isn't authorized by the identity owner.

Explanation:

Question: 171

Which Microsoft Purview solution can be used to identify data leakage?

A. insider risk management B. Compliance Manager

C. communication compliance

D. eDiscovery

Answer: A

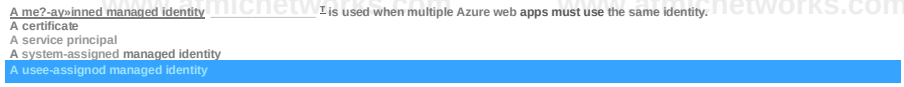
Explanation:

Question: 172

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area



Answer:

Explanation:

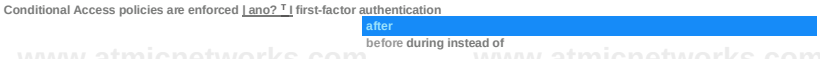
Answer Area

Question: 173

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area



Answer:

Explanation:

Answer Area

Conditional Access policies are enforced after * first factor authentication

Question: 174

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
Conditional Access is implemented by using policies In Microsoft Enba ID		
A Conditional Access policy can block or allow Microsoft Entra ID connections based upon the specific platform of a user's device	0	0
A Conditional Access policy can be applied to a Microsoft 365 group.	0	

Answer

Explanation:

Answer Area

Statements	Yes	No
Conditional Access is implemented by using policies In Microsoft Enba ID		
A Conditional Access policy can block or allow Microsoft Entra ID connections based upon the specific platform of a user's device		0
A Conditional Access policy can be applied to a Microsoft 365 group.		

Question: 175

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Microsoft Entra ID is [amdentih provider] used for authentication and authorization,

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

Answer:

Explanation:

Answer Area

Microsoft Entra ID is an identity provider ^ used for authentication and authorization.

Question: 176

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 Entra ID is deployed to an on-premises enviionment		
Microsoft Entra ID is provided as part of a Microsoft 365 subscription		
Microsoft Entra ID is an identity and access management service		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Microsoft Entra ID is deployed to an on-premises enviionment		
Microsoft Entra ID is provided as part of a Microsoft 365 subscription	«	O
Microsoft Entra ID is an identity and access management service	A	

Question: 177

Which portal contains the solution catalog?

A. Microsoft 365 Apps admin center
B. Microsoft 365 Defender portal
C. Microsoft 365 admin center
D. Microsoft Purview compliance portal

Answer: D

Explanation:

Question: 178

HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) solution.

a cloud infrastructure entitlement management (CIEM) solution.
a cloud security posture management (CSPM) solution.
a security information and event management (SIEM) solution.
an extended detection and response (XDR) solution.

Answer:

Explanation:

Answer Area

Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) solution.

Question: 179

Which solution performs security assessments and automatically generates alerts when a vulnerability is found?

A. cloud security posture management (CSPM)
B. DevSecOps
C. cloud workload protection platform (CWPP)
D. security information and event management (SIEM)

Answer: A

Explanation:

Question: 180

Which three authentication methods can Microsoft Entra users use to reset their password? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. text message to a phone
B. certificate
C. mobile app notification

D. security questions
E. picture password

Answer: A, C, D

Explanation:

Question: 181

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 Entra ID Protection can add users to groups based on the users' risk level.		
Microsoft Entra ID Protection can detect whether user credentials were leaked to the public,		
Microsoft Entra ID Protection can be used to invoke Multi-Factor Authentication based on a . user's risk level		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Microsoft Entra ID Protection can add users to groups based on the users' risk level	O	■
Microsoft Entra ID Protection can detect whether user credentials were leaked to the public,	•	
Microsoft Entra ID Protection can be used to invoke Multi-Factor Authentication based on a user's risk level	•	

Question: 182

HOTSPOT
Select the answer that correctly completes the sentence.

The Cloud Sec urrty Posture Management (CSPM) ^ features of Microsoft Defender for Cloud block malware and other unwanted applications,) access and application control |

Cloud Security Posture Management (CSPM)

container security | vulnerability assessment |

while reducing the network attack surface on Azure virtual machines.

Answer

Explanation:

Answer Area

The Cloud Security Posture Management (CSPM) ^ features of Microsoft Defender for Cloud block malware and other unwanted applications, while reducing the network attack surface on Azure virtual machines.

Question: 183

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

A security information and event management [SIEM) system is a tool that collects data from multiple systems,

A security orchestration automated response (SOAR)
A Trusted Automated exchange of Indicator Information (TAXII)
An attack surface reduction (ASR)

identifies correlations or anomalies, and generates alerts and incidents.

Answer

Explanation:

Answer Area

A security information and event management (SIEM) identifies correlations or system is a tool that collects data from multiple systems, anomalies, and generates alerts and Incidents.

Question: 184

Which feature is included in Microsoft Entra ID Governance?

A. Verifiable credentials
B. Permissions Management
C. Identity Protection
D. Privileged Identity Management

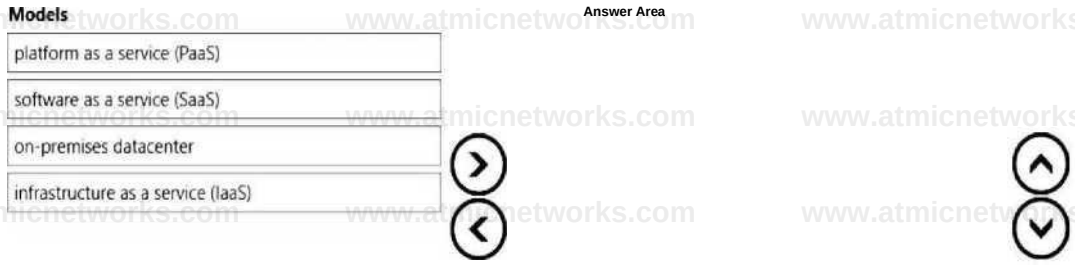
Answer: D

Explanation:

Question: 185

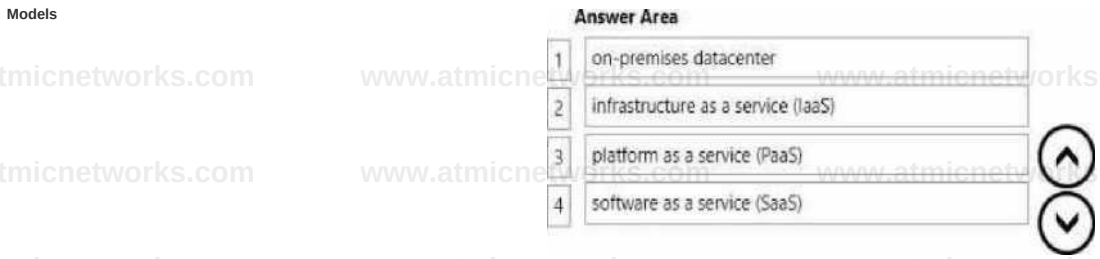
DRAG DROP

You need to identify which cloud service models place the most responsibility on the customer in a shared responsibility model.
in which order should you list the service models from the most customer responsibility (on the top) to the least customer responsibility (on the bottom)? To answer, move all models from the list of models to the answer area and arrange them in the correct order.



Answer:

Explanation:



Question: 186

You have an Azure subscription.
You need to implement approval-based time-bound role activation.
What should you use?

A. Microsoft Entra ID Protection
B. Microsoft Entra Conditional access
C. Microsoft Entra Privileged Management
D. Microsoft Entra Access Reviews

Answer: A

Explanation:

Question: 187

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
Conditional access policies always enforce the use of multi-factor authentication (MFA)		Q
Conditional access policies can be used to block access to an application based on the location of the user.	o	O
Conditional access policies only affect users who have Microsoft Entra joined devices.	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA)		•
Conditional access policies can be used to block access to an application based on the location of the user.	®	O
Conditional access policies only affect users who have Microsoft Entra joined devices.	O	•

Question: 188

What feature supports email as a method of authenticating users?

A. Microsoft Entra ID Protection
B. Microsoft Entra Multi-Factor Authentication (MFA)
C. self-service password reset (SSPR)
D. Microsoft Entra Password Protection

Answer: B

Explanation:

Question: 189

What Microsoft Purview feature can use machine learning algorithms to detect and automatically protect sensitive items?

A. eDiscovery
B. Data loss prevention
C. Information risks
D. Communication compliance

Answer: B

Explanation:

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	
eDiscovery (Standard) search results can be exported.	
eDiscovery (Standard) can be integrated with insider risk management.	
eDiscovery (Standard) can be used to search Microsoft Exchange Online public folders	

Answer:

Explanation:

Answer Area

Statements	
eDiscovery (Standard) search results can be exported.	
eDiscovery (Standard) can be integrated with insider risk management.	
eDiscovery (Standard) can be used to search Microsoft Exchange Online public folders	

Question: 191

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Microsoft provides the Microsoft Purview compliance portal as a public site tor publishing audit reports and . Azure EA portal

Microsoft Purview compliance portal

Microsoft Purview governance portal

Microsoft Service Trust Portal other compliance-related information associated with Microsoft cloud services,

Answer:

Explanation:

Answer Area

Microsoft provides the Microsoft Purview compliance portal ¥ as a public site for publishing audit reports and other compliance-related information associated with Microsoft cloud services

Question: 192

What should you create to search and export content preserved in an eDiscovery hold?

A. a Microsoft SharePoint Online site
B. a case
C. a Microsoft Exchange Online public folder
D. Azure Files

Answer: B

Explanation:

Question: 193

Which Microsoft Purview data classification type supports the use of regular expressions?

A. exact data match (EDM)
B. fingerprint classifier
C. sensitive information types (SITs)
D. trainable classifier

Answer: C

Explanation:

Question: 194

Which two types of devices can be managed by using Endpoint data loss prevention (Endpoint DLP)? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Windows 11
B. Linux
C. iOS
D. macOS
E. Android

Answer: A, D

Explanation:

Question: 195

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 Entra Connect can be used to implement hybrid identity.	O	O
Hybnd identity requires the implementation of two Microsoft 365 tenants	O	O
Authentication of hybrid identities requires the synchronization of Active Directory Domain 0 Services (AD DS) and a Microsoft Entra tenant		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Microsoft Entra Connect can be used to implement hybrid identity.	®	
Hybnd Identity requires the implementation of two Microsoft 365 tenants	O	#
Authentication of hybrid identities requires the synchronization of Active Directory Domain • Services |AD DS) and a Microsoft Entra tenant.		

Question: 196

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 Entra ID Protection generates nsk detections once a user is authenticated	0	

Microsoft Entra ID Protection assigns a risk level of low, Medium, or High to each risk event (

A user risk in Microsoft Entra ID Protection represents the probability that a given identity or account is compromised O

Answer:

Explanation:

Answer Area

Statements	Yes	No
Microsoft Entra ID Protection generates nsk detections once a user is authenticated	•	
Microsoft Entra ID Protection assigns a risk level of Low, Medium, or High to each risk event	•	
A user risk in Microsoft Entra ID Protection represents the probability that a given identity or account is compromised.	•	O

Question: 197

Which Microsoft Purview feature allows users to identify content that should be protected?

A. Sensitivity Labels
B. Insider Risks
C. Data Loss prevention
D. eDiscovery

Answer: A

Explanation:

Question: 198

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Answer:

Explanation:

Answer Area

Question: 199

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

A. Secure score
B. Reports
C. Hunting
D. Incidents

Answer: B

Explanation:

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
Microsoft Entra Access Review evaluates user and group permissions for Azure resources.		
A user can be removed from a group automatically after a Microsoft Entra Access Review evaluation.		
The Microsoft Entra Access Review feature is available in all Microsoft Entra ID service plans.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Microsoft Entra Access Review evaluates user and group permissions for Azure resources.	•	
A user can be removed from a group automatically after a Microsoft Entra Access Review evaluation.	•	
The Microsoft Entra Access Review feature is available in all Microsoft Entra ID service plans.		•

Question: 201

To which three locations can a data loss prevention (DLP) policy be applied? Each correct answer presents a complete solution.
NOTE: Each correct answer is worth one point.

A. Microsoft Exchange Online email
B. Microsoft OneDrive accounts

C. Microsoft Exchange Online public folders
D. Microsoft Teams chat and channel messages
E. Microsoft Viva Engage

Answer: A, B, D

Explanation:

Question: 202

HOTSPOT
Select The answer that correctly completes the sentence.

Answer Area

Single sign-on (SSO) configured between multiple identity providers is an example of federation.

federation.
integration.
password hash synchronization.
pass-through authentication.

Answer:

Explanation:

Answer Area

Single sign-on (SSO) configured between multiple identity providers is an example of [federation

Question: 203

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
GitHub is a cloud-based identity provider		
Federation provides single sign-on (SSO) with multiple identity providers.		
A central identity provider manages all modern authentication services, such as authentication, authorization, and auditing		

Answer:

Explanation:

Answer Area

Statements	Yes	No
GitHub is a cloud-based identity provider	*	
Federation provides single sign-on (SSO) with multiple identity providers. *		

A central identity provider manages all modern authentication services, such 0 as authentication, authorization and auditing

Question: 204

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Microsoft Defender for Cloud assesses Azure resources continuously ' for security issues.

continuously
daily
every 15 minutes hourly

Answer:

Explanation:

Answer Area

Microsoft Defender for Cloud assesses Azure resources continuously ' for security issues.

Question: 205

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
Each network security group (NSG) rule must have a unique name.		
Network secunty group (NSG) default rules can be deleted.		
Network security group (NSG) rules can be configured to check TCP. UDP. or ICMP network protocol types.		

Answer:

Explanation:

Answer Area Statements	Yes	No
Each network security group (NSG) rule must have a unique name.	♦	
Network secunty group (NSG) default rules can be deleted.	O	•
Network security group (NSG) rules can be configured to check TCP. UDP. or ICMP network protocol types.	*	

Question: 206

Which two actions can you perform by using Azure Key Vault? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Store Azure Resource Manager (ARM) templates.

B. Implement Azure DDoS Protection.

C. Implement network security groups (NSGs).

D. Store keys.

E. Store secrets.

Answer: D, E

Explanation:

Question: 207

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 Entra Permissions Management can be managed by using the Microsoft Purview compliance portal.	0	Q
Microsoft Entra Permissions Management can be used to manage permissions in Amazon Web Services (AWS).		
Microsoft Secure Score can be reviewed from Permissions Management in the Microsoft Entra admin center.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Microsoft Entra Permissions Management can be managed by using the Microsoft Purview compliance portal.	O	@
Microsoft Entra Permissions Management can be used to manage permissions in Amazon • Web Services (AWS).		
Microsoft Secure Score can be reviewed from Permissions Management in Che Microsoft Entra admin center.	O	®

Question: 208

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

You can override ᵀ the default security rules of a network security group (NSG). copy **delete**

override

Answer:

Explanation:

Answer Area

You can override ' the default security rules of a network security group (NSG).

Question: 209

In the shared responsibility model, for what is Microsoft responsible when managing Azure virtual machines?

A. Updating the operating system.

B. Configuring the permissions for shared folders.

C. Updating the firmware of the disk controller.

D. Updating installed applications.

Answer: C

Explanation: