SC-900_46q_June_2021_By_DrunkMonk

Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Exam SC-900: Microsoft Security Compliance and Identity Fundamentals

Version 1.0

Skills measured

- Describe the concepts of security, compliance, and identity
- Describe the capabilities of Microsoft identity and access management solutions
- Describe the capabilities of Microsoft security solutions
- Describe the capabilities of Microsoft compliance solutions



Sections

1. Describe the Concepts of Security, Compliance, and Identity
2. Describe the Capabilities of Microsoft Identity and Access Management Solutions
3. Describe the Capabilities of Microsoft Security Solutions
4. Describe the Capabilities of Microsoft Compliance Solutions

Exam A

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.

Hot Area:

Answer Area

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

Answer:

Answer Area

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

Section: Describe the Concepts of Security, Compliance, and Identity

Explanation/Reference:
Explanation:

Reference:

QUESTION 2
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Azure Blueprints	provides best practices from Microsoft employees, including tools and guidance to assist in an Azure d
Azure Policy	
The Microsoft Cloud Adoption Framework for Azure	
A resource lock	

Answer:

Answer Area

Azure Blueprints	provides best practices from Microsoft employees, including tools and guidance to assist in an Azure d
Azure Policy	
The Microsoft Cloud Adoption Framework for Azure	
A resource lock	

Section: Describe the Concepts of Security, Compliance, and Identity

Explanation/Reference:
Explanation:

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

QUESTION 3
HOTSPOT

Select the answer that correctly completes the sentence.

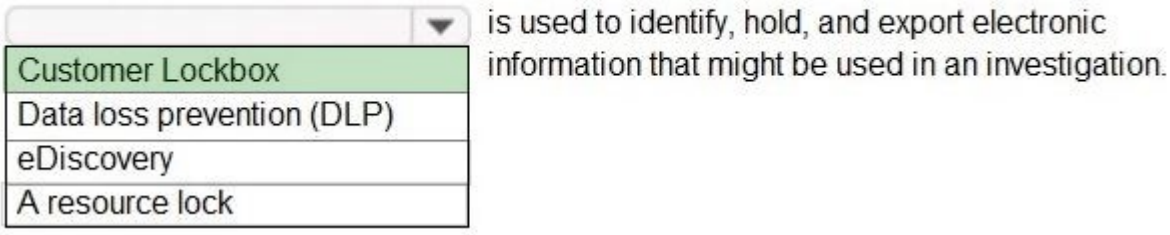
Hot Area:

Answer Area

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

Answer:

Answer Area



Section: Describe the Concepts of Security, Compliance, and Identity

Explanation/Reference:
Explanation:

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

QUESTION 4
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:



Answer:



Section: Describe the Concepts of Security, Compliance, and Identity

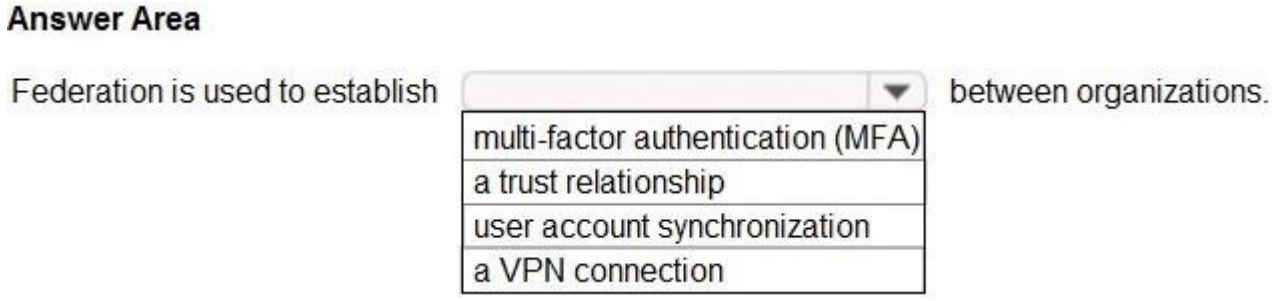
Explanation/Reference:
Explanation:

Reference:

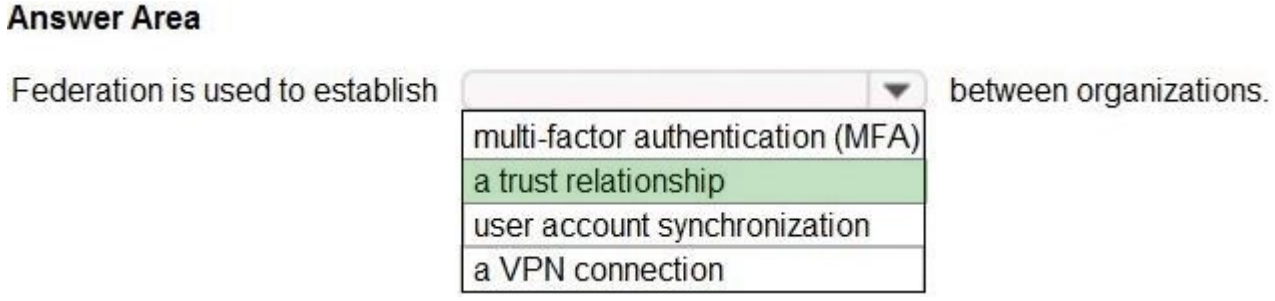
QUESTION 5
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:



Answer:



Section: Describe the Concepts of Security, Compliance, and Identity

Explanation/Reference:
Explanation:

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.

Hot Area:

Answer Area

Statements	
Applying system updates increases an organization's secure score in Azure Secu	
The secure score in Azure Security Center can evaluate resources across multipl subscriptions.	
Enabling multi-factor authentication (MFA) increases an organization's secure s Security Center.	

Answer:

Answer Area

Statements	
Applying system updates increases an organization's secure score in Azure Secu	
The secure score in Azure Security Center can evaluate resources across multipl subscriptions.	
Enabling multi-factor authentication (MFA) increases an organization's secure s Security Center.	

Section: Describe the Concepts of Security, Compliance, and Identity

Explanation/Reference:
Explanation:
Box 1: Yes
System updates reduces security vulnerabilities, and provide a more stable environment for end users. Not applying updates leaves unpatched vulnerabilities and results in environments that are susceptible to attacks.

Box 2: Yes

Box 3: Yes
If you only use a password to authenticate a user, it leaves an attack vector open. With MFA enabled, your accounts are more secure.

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
Section: Describe the Concepts of Security, Compliance, and Identity

Explanation/Reference:
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 connector

Answer: D
Section: Describe the Concepts of Security, Compliance, and Identity

Explanation/Reference:
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
Section: Describe the Concepts of Security, Compliance, and Identity

Explanation/Reference:
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
Section: Describe the Concepts of Security, Compliance, and Identity

Explanation/Reference:
Explanation:

Reference:

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.

Hot Area:

Answer Area

Statements
Verify explicitly is one of the guiding principles of Zero Trust.
Assume breach is one of the guiding principles of Zero Trust.
The Zero Trust security model assumes that a firewall secures the internal ne external threats.

Answer:

Answer Area

Statements	
Verify explicitly is one of the guiding principles of Zero Trust.	
Assume breach is one of the guiding principles of Zero Trust.	
The Zero Trust security model assumes that a firewall secures the internal ne external threats.	

Section: Describe the Concepts of Security, Compliance, and Identity

Explanation/Reference:
Explanation:
Box 1: Yes

Box 2: Yes

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

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.

Hot Area:

Answer Area

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

Answer:



Section: Describe the Concepts of Security, Compliance, and Identity

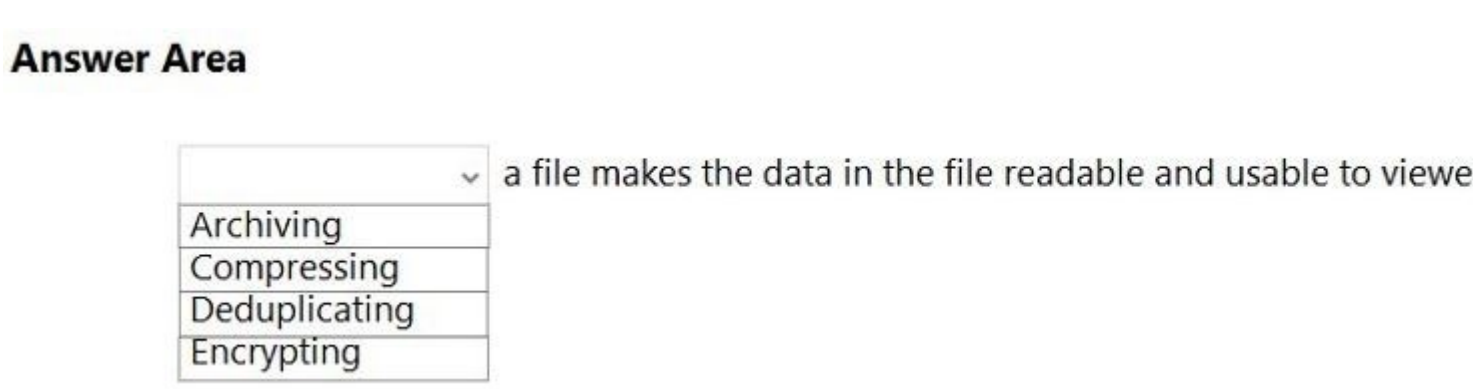
Explanation/Reference:
Explanation:

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

QUESTION 13
HOTSPOT

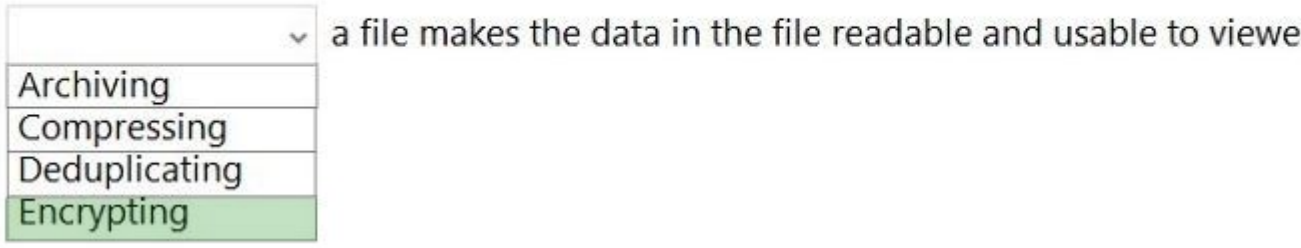
Select the answer that correctly completes the sentence.

Hot Area:



Answer:

Answer Area



Section: Describe the Concepts of Security, Compliance, and Identity

Explanation/Reference:
Explanation:

Reference:

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
Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

Explanation/Reference:
Explanation:

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

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
Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

Explanation/Reference:
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.

Hot Area:

Answer Area

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

Answer:

Answer Area

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

Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

Explanation/Reference:
Explanation:
Box 1: **Yes**
Azure AD supports custom roles.

Box 2: Yes
Global Administrator has access to all administrative features in Azure Active Directory.

Box 3: No

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.

Hot Area:

Answer Area

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

Answer:

Answer Area

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

Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

Explanation/Reference:
Explanation:
Box 1: No
Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.

Box 2: Yes
Microsoft 365 uses Azure Active Directory (Azure AD). Azure Active Directory (Azure AD) is included with your Microsoft 365 subscription.

Box 3: Yes
Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.

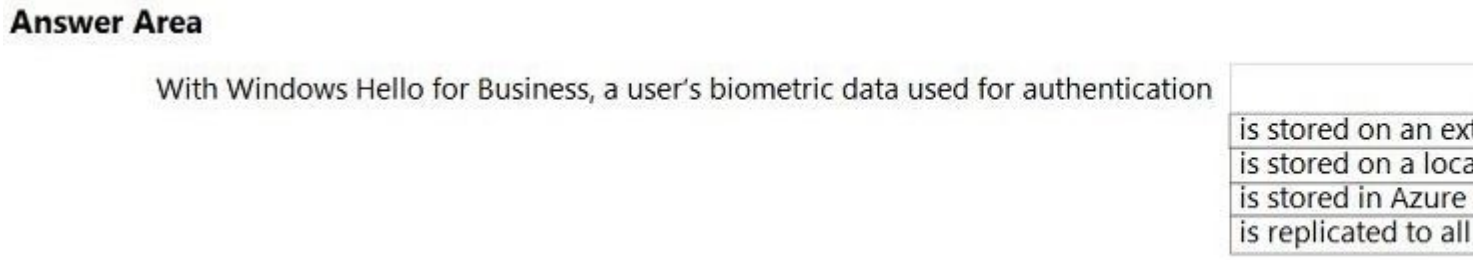
Reference:

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

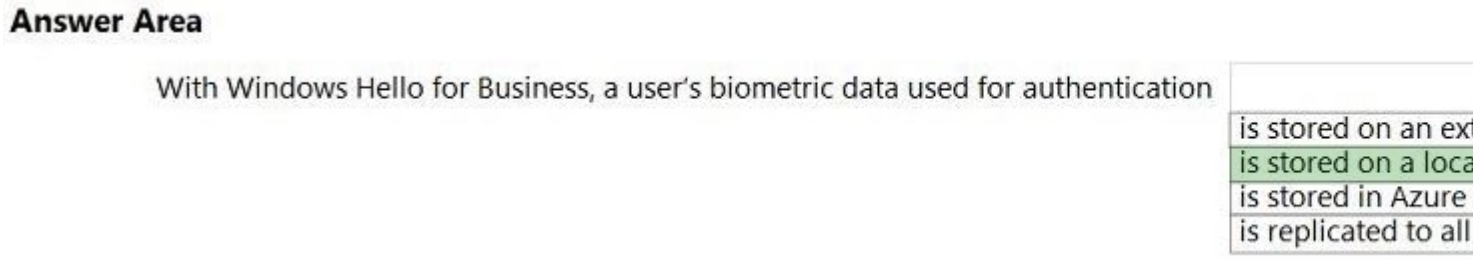
QUESTION 18
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:



Answer:



Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

Explanation/Reference:
Explanation:
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
Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

Explanation/Reference:
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
Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

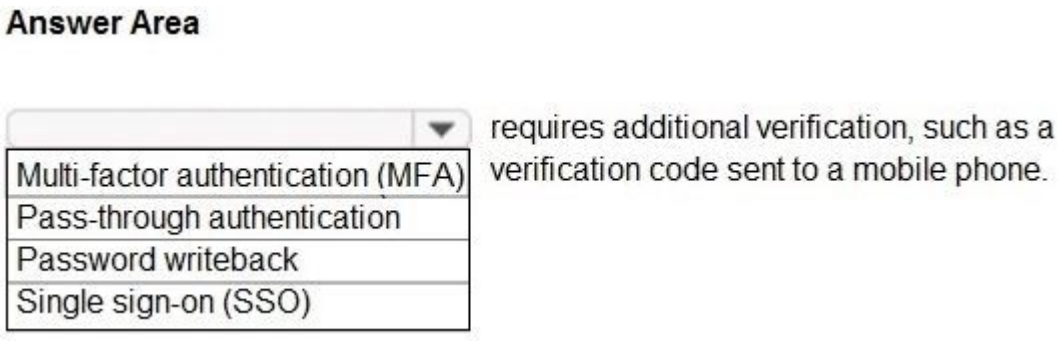
Explanation/Reference:
Explanation:
Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments.

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.

Hot Area:



Answer:

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)	

Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

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

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.

Hot Area:

Answer Area

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

Answer:

Answer Area

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

Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

Explanation/Reference:
Explanation:
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.

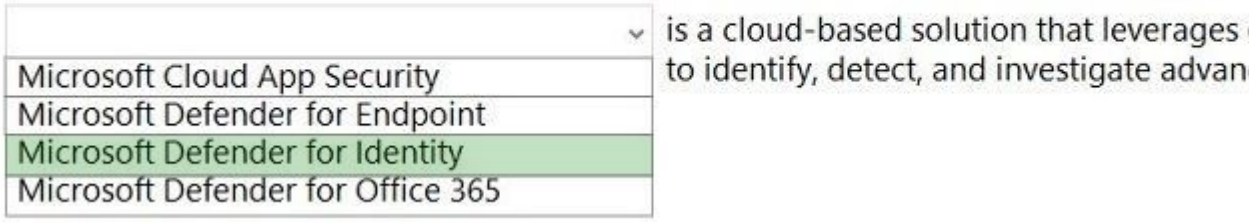
Hot Area:

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 to identify, detect, and investigate advan

Answer:

Answer Area



Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

Explanation/Reference:
Explanation:

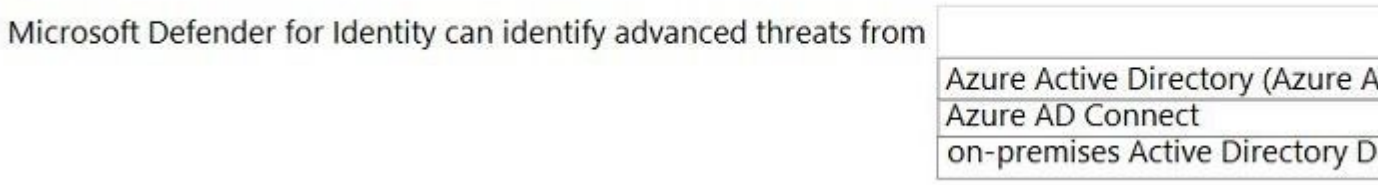
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/what-is

QUESTION 24
HOTSPOT

Select the answer that correctly completes the sentence.

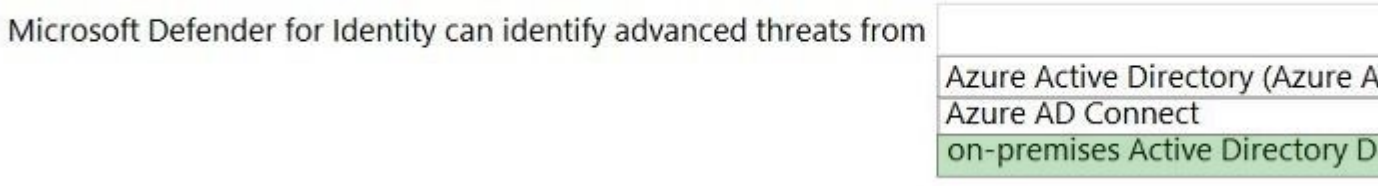
Hot Area:

Answer Area



Answer:

Answer Area



Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

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

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

QUESTION 25
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

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:

Answer Area

Azure Active Directory (Azure AD) is [an identity provider] 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

Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

Explanation/Reference:
Explanation:
Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.

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

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
Section: Describe the Capabilities of Microsoft Identity and Access Management Solutions

Explanation/Reference:

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

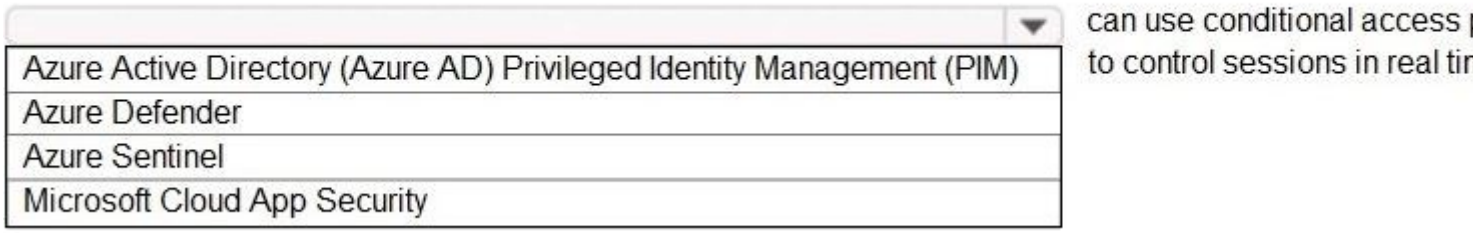
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

QUESTION 27
HOTSPOT

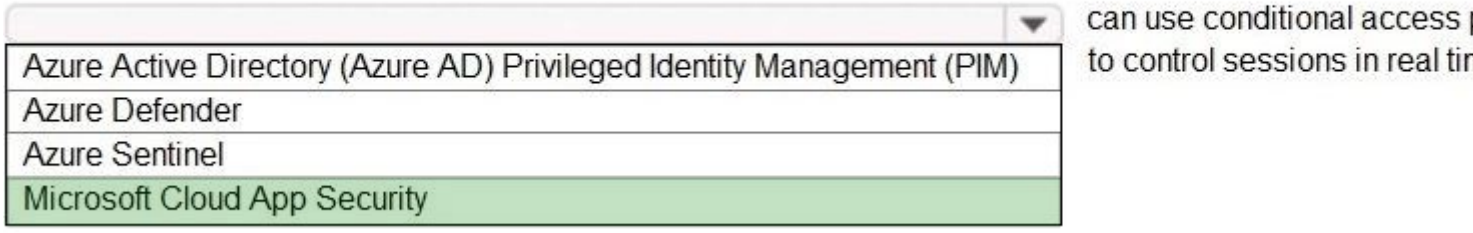
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area



Answer:
Answer Area



Section: Describe the Capabilities of Microsoft Security Solutions

Explanation/Reference:
Explanation:

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.

Hot Area:

Answer Area

Azure DDoS Protection Standard can be used to protect

- Azure Active Direc
- Azure Active Direc
- resource groups.
- virtual networks.

Answer:

Answer Area

Azure DDoS Protection Standard can be used to protect

- Azure Active Direc
- Azure Active Direc
- resource groups.
- virtual networks.

Section: Describe the Capabilities of Microsoft Security Solutions

Explanation/Reference:
Explanation:

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
Section: Describe the Capabilities of Microsoft Security Solutions

Explanation/Reference:
Explanation:

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

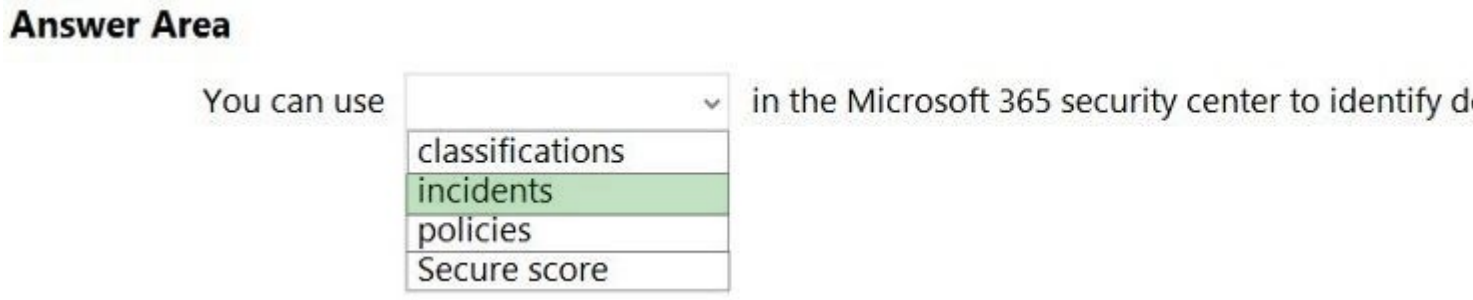
QUESTION 30
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:



Answer:



Section: Describe the Capabilities of Microsoft Security Solutions

Explanation/Reference:
Explanation:

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
Section: Describe the Capabilities of Microsoft Security Solutions

Explanation/Reference:
Explanation:

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

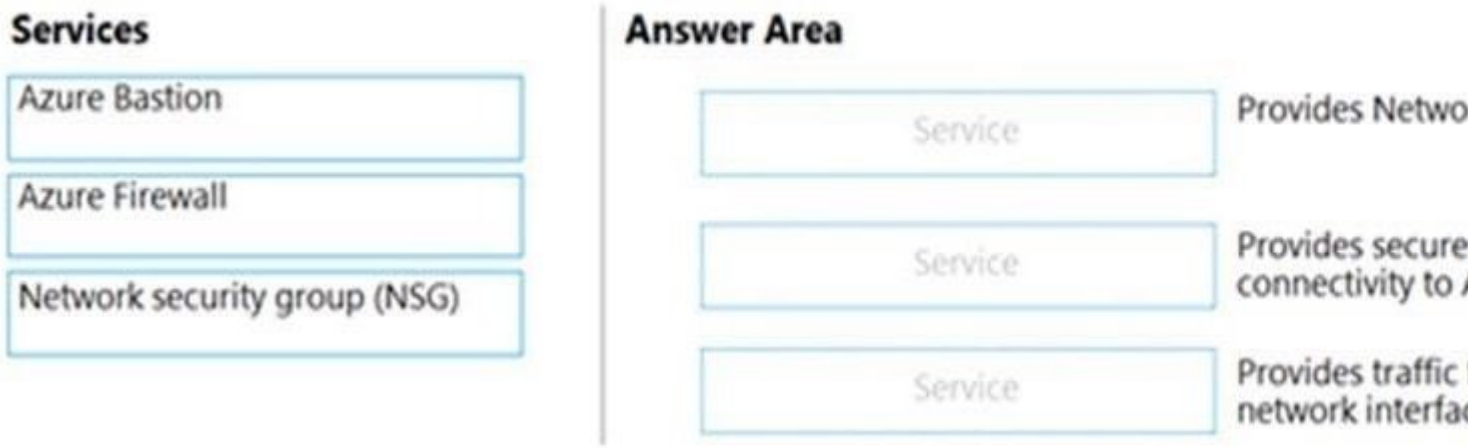
QUESTION 32
DRAG DROP

Match the Azure networking service to the appropriate description.

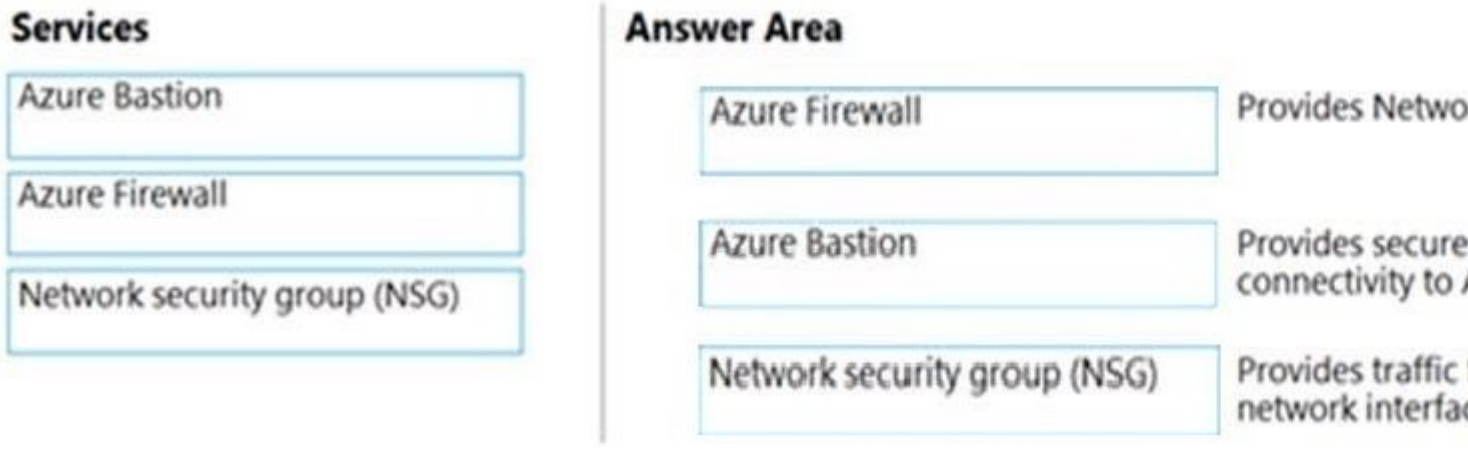
To answer, drag the appropriate service from the column on the left to its description on the right. Each service may be used once, more than once, or not at all.

NOTE: Each correct match is worth one point.

Select and Place:



Answer:



Section: Describe the Capabilities of Microsoft Security Solutions

Explanation/Reference:
Explanation:
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.

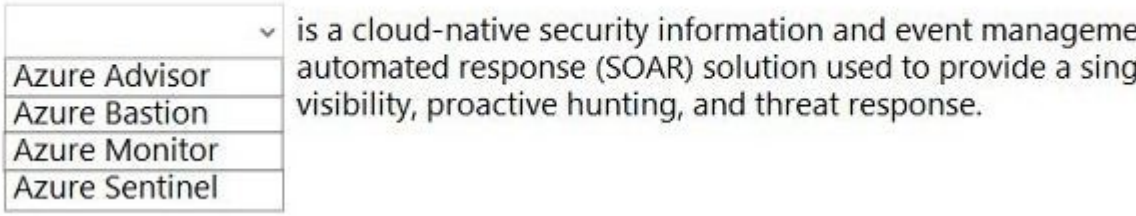
Reference:
https://docs.microsoft.com/en-us/azure/networking/fundamentals/networking-overview https://docs.microsoft.com/en-us/azure/bastion/bastion-overview
https://docs.microsoft.com/en-us/azure/firewall/features
https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

QUESTION 33
HOTSPOT

Select the answer that correctly completes the sentence.

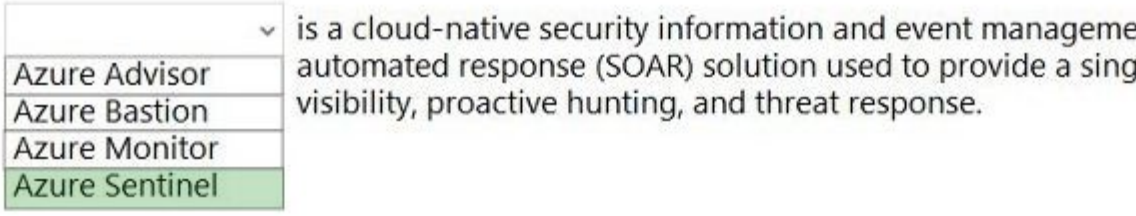
Hot Area:

Answer Area



Answer:

Answer Area



Section: Describe the Capabilities of Microsoft Security Solutions

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

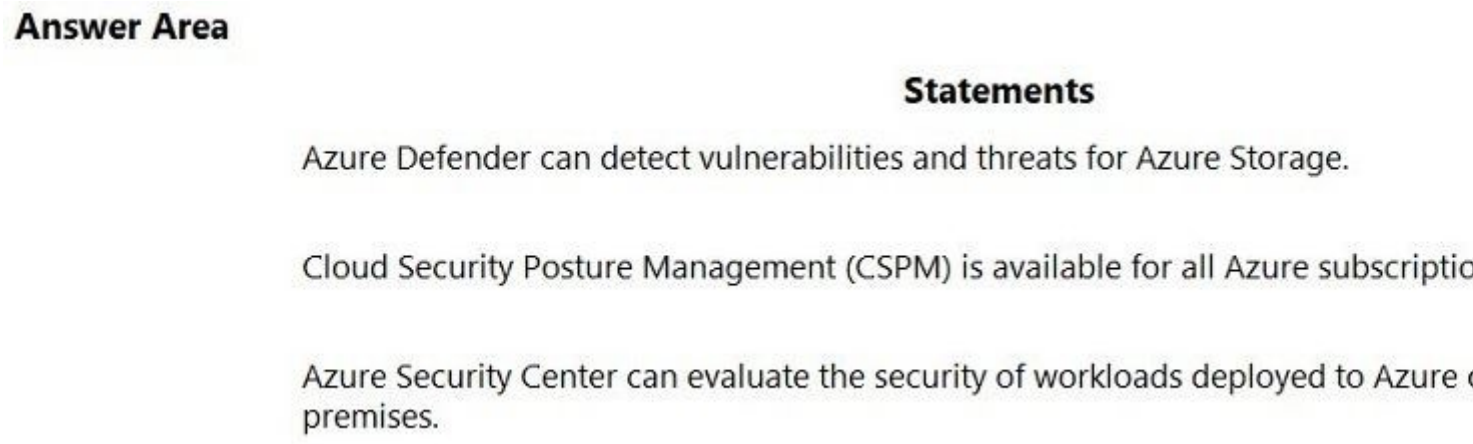
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/overview

QUESTION 34
HOTSPOT

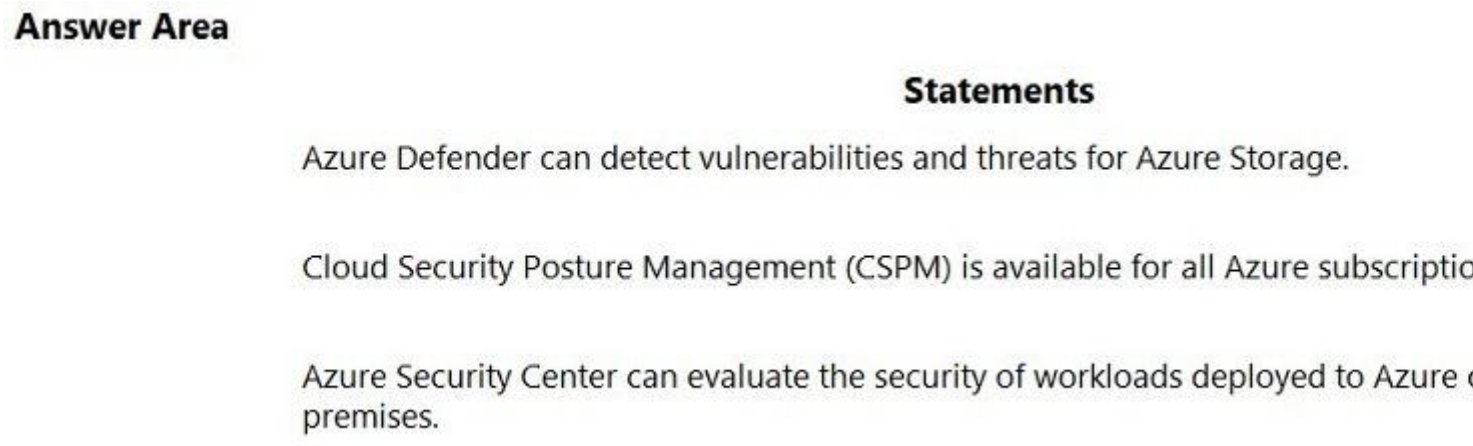
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer:



Section: Describe the Capabilities of Microsoft Security Solutions

Explanation/Reference:
Explanation:
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.

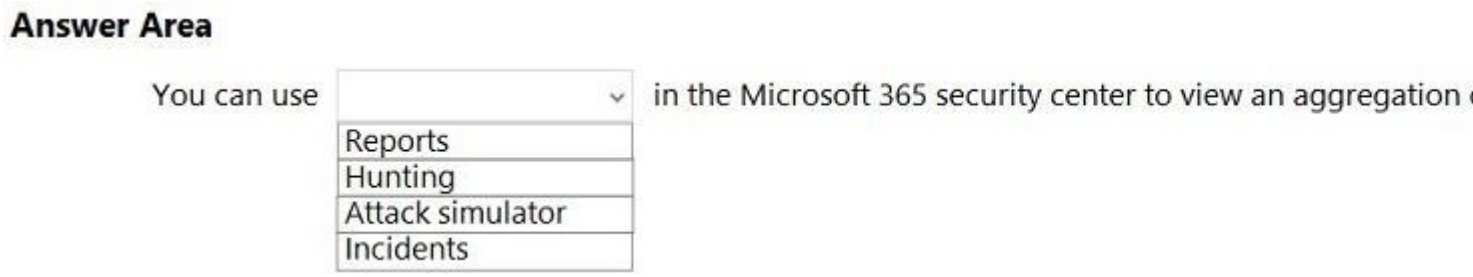
Box 3: Yes
Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

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

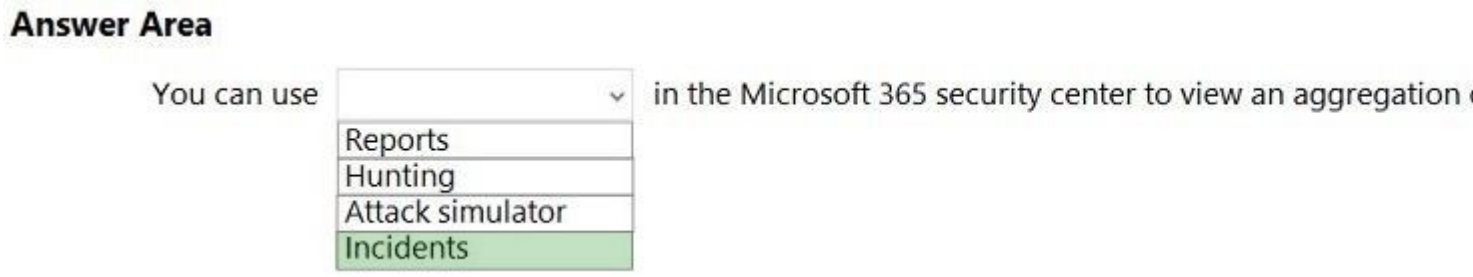
QUESTION 35
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:



Answer:



Section: Describe the Capabilities of Microsoft Security Solutions

Explanation/Reference:
Explanation:

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.

Hot Area:

Answer Area

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

Answer:

Answer Area

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

Section: Describe the Capabilities of Microsoft Compliance Solutions

Explanation/Reference:
Explanation:
Box 1: Yes
The MailItemsAccessed event is a mailbox auditing action and is triggered when mail data is accessed by mail protocols and mail clients.

Box 2: No
Basic Audit retains audit records for 90 days.
Advanced Audit retains all Exchange, SharePoint, and Azure Active Directory audit records for one year. This is accomplished by a default audit log retention policy that retains any audit record that contains the value of Exchange, SharePoint, or AzureActiveDirectory for the Workload property (which indicates the service in which the activity occurred) for one year.

Box 3: Yes
Advanced Audit in Microsoft 365 provides high-bandwidth access to the Office 365 Management Activity API.

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.

Hot Area:

Answer Area

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

Answer:

Answer Area

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

Section: Describe the Capabilities of Microsoft Compliance Solutions

Explanation/Reference:
Explanation:
Box 1: No

Box 2: Yes
Leaked Credentials indicates that the user's valid credentials have been leaked.

Box 3: Yes
Multi-Factor Authentication can be required based on conditions, one of which is user risk.

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
Section: Describe the Capabilities of Microsoft Compliance Solutions

Explanation/Reference:
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
Section: Describe the Capabilities of Microsoft Compliance Solutions

Explanation/Reference:
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.

Hot Area:

Answer Area

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

- continually
- monthly
- on-demand
- quarterly

Answer:

Answer Area

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

- continually
- monthly
- on-demand
- quarterly

Section: Describe the Capabilities of Microsoft Compliance Solutions

Explanation/Reference:
Explanation:

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.

Hot Area:

Answer Area

Statements	Yes	No
Sensitivity labels can be used to encrypt documents.	○	○
Sensitivity labels can add headers and footers to documents.	○	○
Sensitivity labels can apply watermarks to emails.	○	○

Answer:

Answer Area

Statements	Yes	No
Sensitivity labels can be used to encrypt documents.	○	○
Sensitivity labels can add headers and footers to documents.	○	○
Sensitivity labels can apply watermarks to emails.	○	○

Section: Describe the Capabilities of Microsoft Compliance Solutions

Explanation/Reference:
Explanation:
Box 1: Yes
You can use sensitivity labels to provide protection settings that include encryption of emails and documents to prevent unauthorized people from accessing this data.

Box 2: Yes
You can use sensitivity labels to mark the content when you use Office apps, by adding watermarks, headers, or footers to documents that have the label applied.

Box 3: Yes
You can use sensitivity labels to mark the content when you use Office apps, by adding headers, or footers to email that have the label applied.

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

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
Section: Describe the Capabilities of Microsoft Compliance Solutions

Explanation/Reference:
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.

Hot Area:

Answer Area

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

Answer:

Answer Area

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

Section: Describe the Capabilities of Microsoft Compliance Solutions

Explanation/Reference:
Explanation:
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.

Hot Area:

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.	○	○

Answer:

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.	○	○

Section: Describe the Capabilities of Microsoft Compliance Solutions

Explanation/Reference:
Explanation:

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: C
Section: Describe the Capabilities of Microsoft Compliance Solutions

Explanation/Reference:
Explanation:

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

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
Section: Describe the Capabilities of Microsoft Compliance Solutions

Explanation/Reference:
Explanation:

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