Exam A

QUESTION 1
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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

Section:
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 2
What can you protect by using the information protection solution in the Microsoft 365 compliance center?

A. computers from zero-day exploits

B. users from phishing attempts

C. files from malware and viruses

D. sensitive data from being exposed to unauthorized users

Correct Answer: D

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

QUESTION 3
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

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

QUESTION 4
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 use Advanced Audit in Microsoft 365 to view billing details.	○	○
You can use Advanced Audit in Microsoft 365 to view the contents of an email message.	○	○
You can use Advanced Audit in Microsoft 365 to identify when a user uses the search bar in Outlook on the web to search for items in a mailbox.	○	○

Answer Area:

Answer Area

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

Section:
Explanation:
Box 1: No
Advanced Audit helps organizations to conduct forensic and compliance investigations by increasing audit log retention.
Box 2: No
Box 3: Yes
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/advanced-audit?view=o365-worldwide

QUESTION 5
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
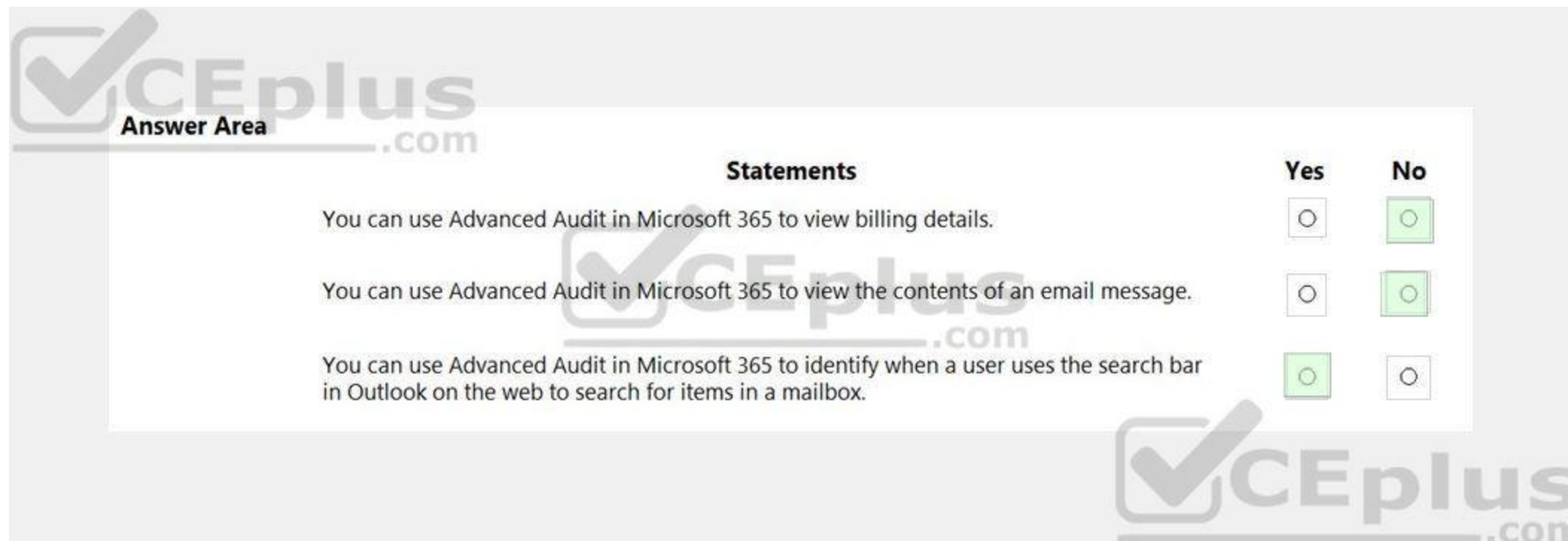NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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

Section:
Explanation:

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.

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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

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

QUESTION 7
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 verify 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.

Correct Answer: B, C, D
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/security/zero-trust/

QUESTION 8
HOTSPOT
Which service should you use to view your Azure secure score? To answer, select the appropriate service in the answer area.

Hot Area:

Microsoft Azure

🔍 Search resources, services, and docs (G+/)

···

Azure services

+

Create a resource

🟩 Alerts

💡 Application Insights

🔑 Subscriptions

⬡ Policy

🔺 Azure AD Connect Health

🛡️ Security Center

☁️ Advisor

⏱️ Monitor

→ More services

Answer Area:

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/secure-score-access-and-track
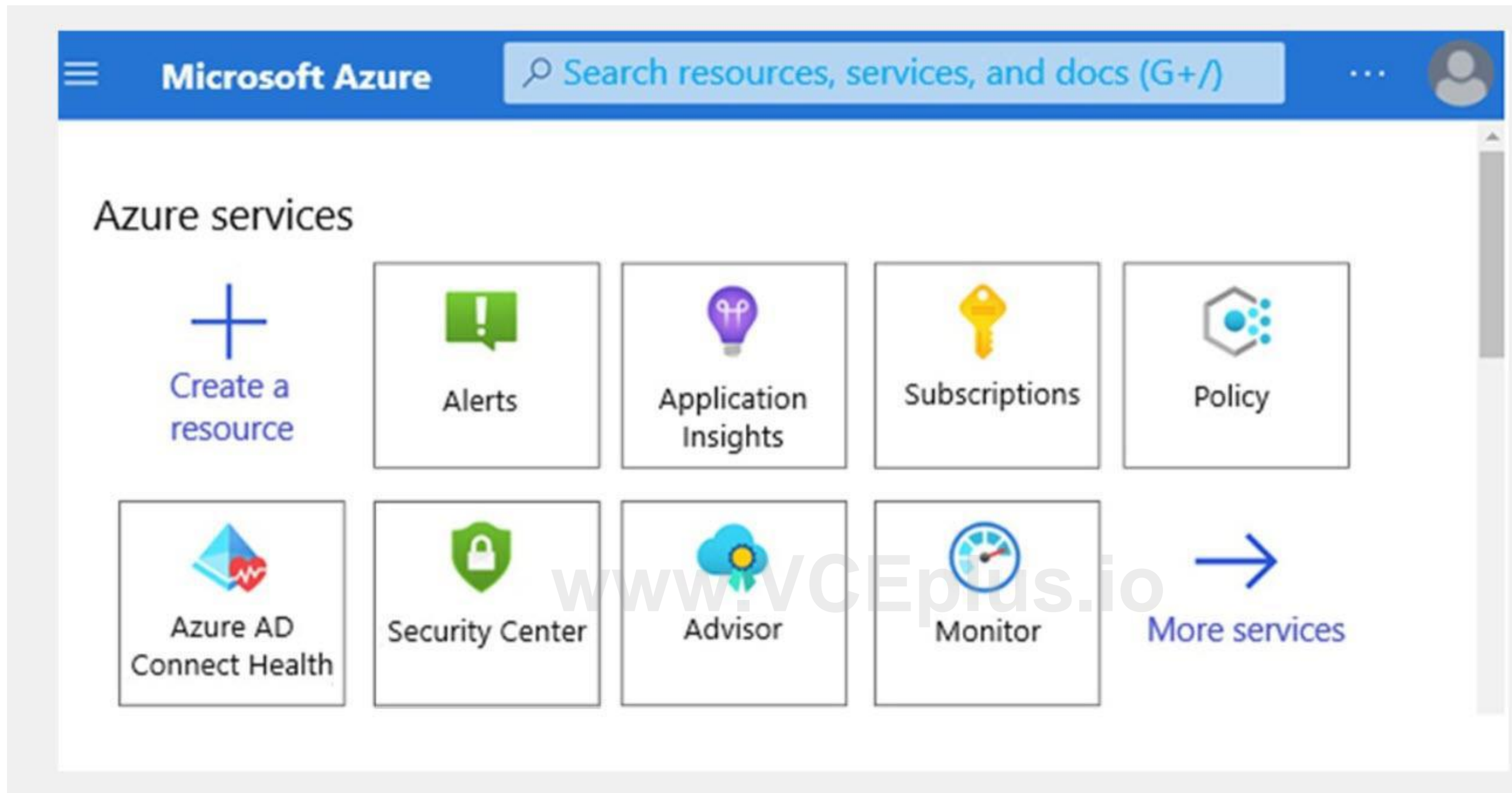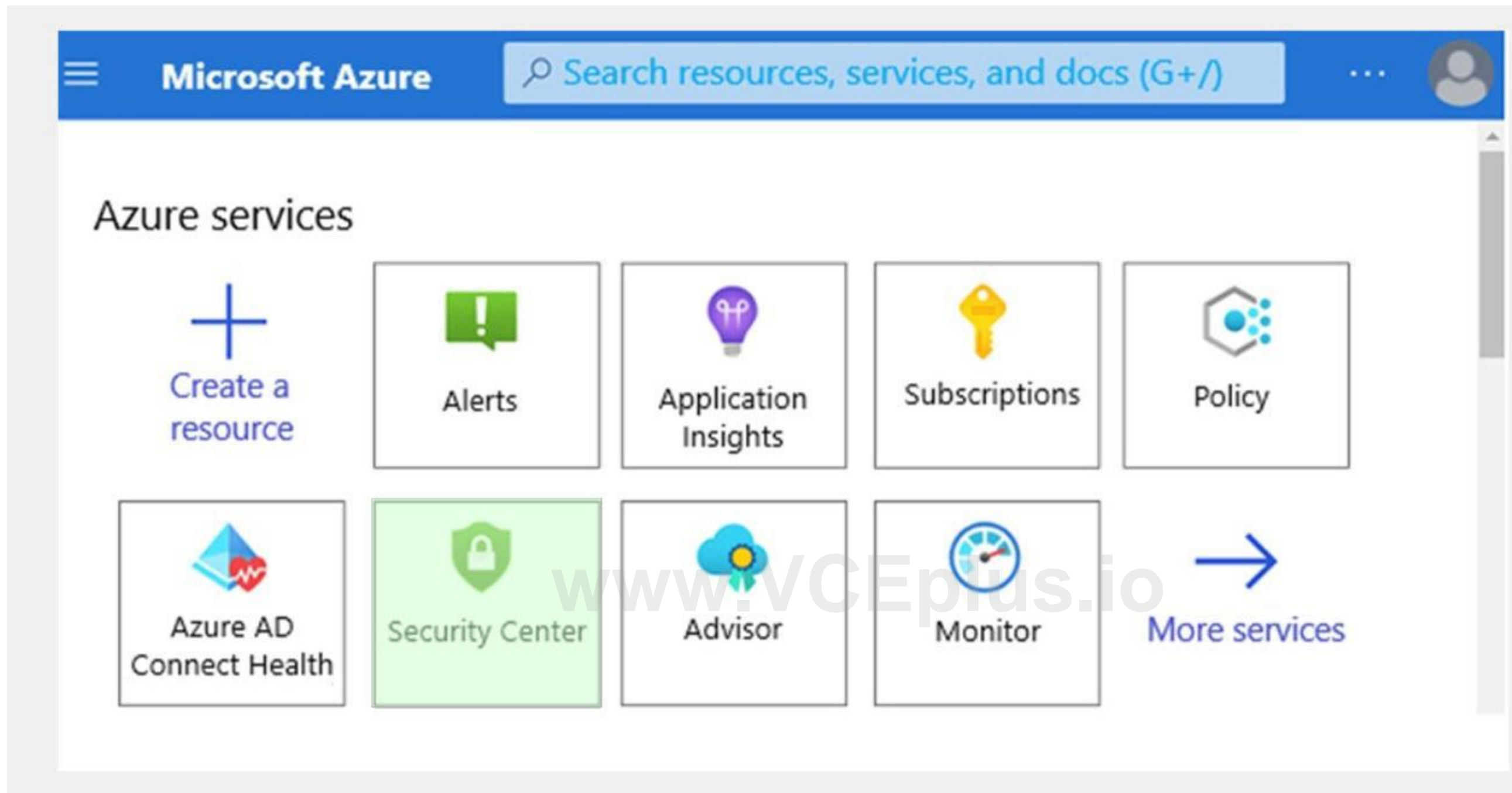
QUESTION 9
You have a Microsoft 365 E3 subscription.
You plan to audit user activity by using the unified audit log and Basic Audit.
For how long will the audit records be retained?

A. 15 days

B. 30 days

C. 90 days

D. 180 days

Correct Answer: C
Section:

QUESTION 10
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

Correct Answer: C
Section:
Explanation:
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 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	**Yes**	**No**
Azure Defender can detect vulnerabilities and threats for Azure Storage.	○	○
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	○	○
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	○	○

Answer Area:

Answer Area

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

Section:
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 12
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

You can use [dropdown ▼] in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

| Reports |
| Hunting |
| Attack simulator |
| Incidents |

Answer Area:

Answer Area

You can use [Incidents ▼] in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

Reports
Hunting
Attack simulator
Incidents

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

QUESTION 13
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
Network security groups (NSGs) can deny inbound traffic from the internet.	○	○
Network security groups (NSGs) can deny outbound traffic to the internet.	○	○
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	○	○

Answer Area:

Answer Area

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

Section:
Explanation:
You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. 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 14
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

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

QUESTION 15
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 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.	○	○

Section:
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 16
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

With Windows Hello for Business, a user's biometric data used for authentication	is stored on an external device.
	is stored on a local device only.
	is stored in Azure Active Directory (Azure AD).
	is replicated to all the devices designated by the user.

Answer Area:

Answer Area

With Windows Hello for Business, a user's biometric data used for authentication	is stored on an external device.
	is stored on a local device only.
	is stored in Azure Active Directory (Azure AD).
	is replicated to all the devices designated by the user.

Section:
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 17
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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

Section:

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 18

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

Answer Area:

Answer Area

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

Section:

Explanation:

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 19

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 one Azure Bastion per virtual network.	○	○
Azure Bastion provides secure user connections by using RDP.	○	○
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	○	○

Answer Area:

Answer Area

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

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

QUESTION 20
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 Area:

Answer Area

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

- continually
- monthly
- on-demand
- quarterly

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

QUESTION 21
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 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.	⦿	○

Section:
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 22
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

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

QUESTION 23
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
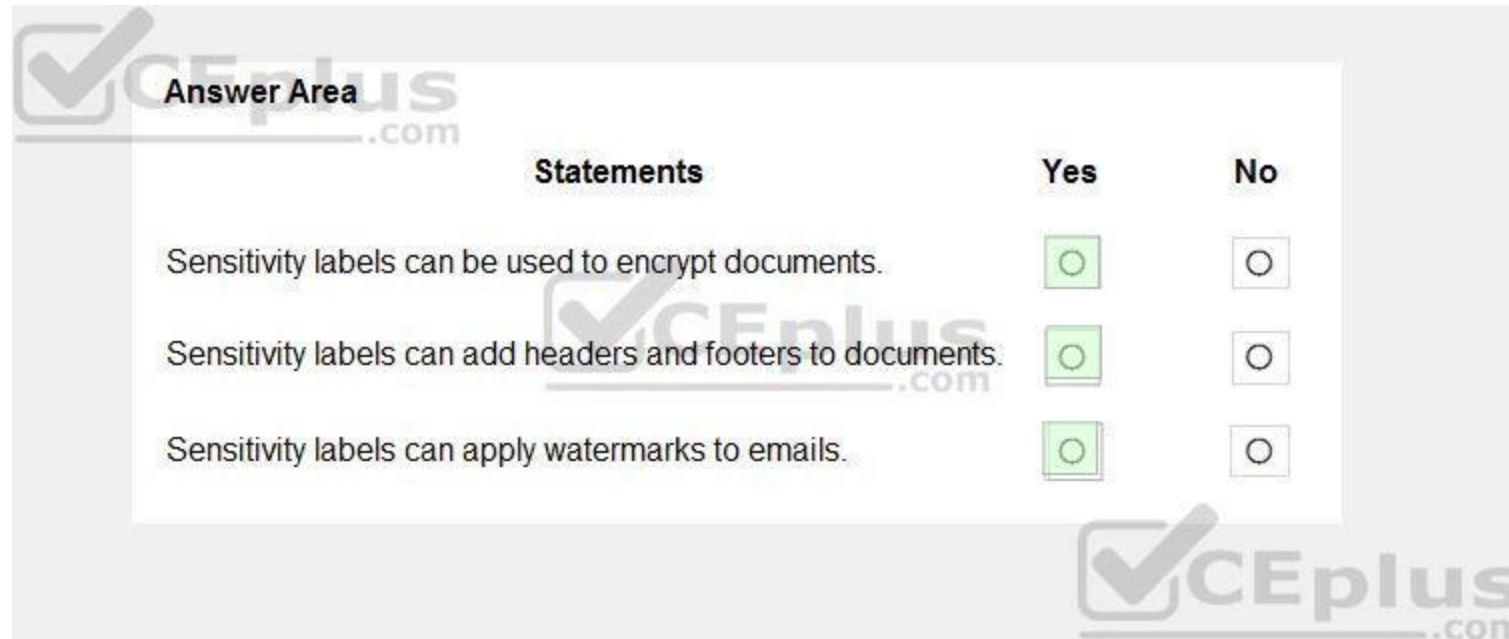NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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

Section:
Explanation:

QUESTION 24
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

Correct Answer: A

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

QUESTION 25
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 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.	○	○

Section:
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 26
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

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

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

Answer Area:

Answer Area

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

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

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

QUESTION 27
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Microsoft Defender for Identity can identify advanced threats from [⌄] signals.

| Azure Active Directory (Azure AD) |
| Azure AD Connect |
| on-premises Active Directory Domain Services (AD DS) |

Answer Area:

Answer Area

Microsoft Defender for Identity can identify advanced threats from [⌄] signals.

| Azure Active Directory (Azure AD) |
| Azure AD Connect |
| on-premises Active Directory Domain Services (AD DS) |

Section:
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 28
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 Area:

Answer Area

Azure Active Directory (Azure AD) is | [dropdown ▼]

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

used for authentication and authorization.

Section:
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 29
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

[dropdown ▼] | can use conditional access policies to control sessions in real time.

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

Answer Area:

Answer Area

▼	can use conditional access policies to control sessions in real time.
Azure Active Directory (Azure AD) Privileged Identity Management (PIM)	
Azure Defender	
Azure Sentinel	
Microsoft Cloud App Security	

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

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

Hot Area:

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 Area:

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.

Section:

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

QUESTION 31
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

You can use [dropdown ⌄] in the Microsoft 365 security center to identify devices that are affected by an alert.

| classifications |
| incidents |
| policies |
| Secure score |

Answer Area:

Answer Area

You can use [dropdown ⌄] in the Microsoft 365 security center to identify devices that are affected by an alert.

| classifications |
| incidents |
| policies |
| Secure score |

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

QUESTION 32
What can you use to provide threat detection for Azure SQL Managed Instance?

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

Correct Answer: C
Section:

QUESTION 33
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**
Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	○	○
From the Microsoft 365 security center, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	○	○
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.	○	○

Answer Area:

Answer Area		
Statements	**Yes**	**No**
Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	●	○
From the Microsoft 365 security center, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	●	○
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.	●	○

Section:
Explanation:

QUESTION 34
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

Correct Answer: C
Section:

QUESTION 35
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.

Select and Place:

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

Correct Answer:

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

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

QUESTION 36
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

Correct Answer: B
Section:
Explanation:
Microsoft Secure Score for Devices
Artikel
12.05.2022
3 Minuten Lesedauer
Applies to:
Microsoft Defender for Endpoint Plan 2
Microsoft Defender Vulnerability Management
Microsoft 365 Defender
Some information relates to pre-released product which may be substantially modified before it's commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here. To sign up for the Defender Vulnerability Management public preview or if you have any questions, contact us (mdvmtrial@microsoft.com). Already have Microsoft Defender for Endpoint P2? Sign up for a free trial of the Defender Vulnerability Management Add-on. Configuration score is now part of vulnerability management as Microsoft Secure Score for Devices.
Your score for devices is visible in the Defender Vulnerability Management dashboard of the Microsoft 365 Defender portal. A higher Microsoft Secure Score for Devices means your endpoints are more resilient from cybersecurity threat attacks. It reflects the collective security configuration state of your devices across the following categories:
Application
Operating system
Network
Accounts
Security controls
Select a category to go to the Security recommendations page and view the relevant recommendations. Turn on the Microsoft Secure Score connector
Forward Microsoft Defender for Endpoint signals, giving Microsoft Secure Score visibility into the device security posture. Forwarded data is stored and processed in the same location as your Microsoft Secure Score data. Changes might take up to a few hours to reflect in the dashboard.
In the navigation pane, go to Settings > Endpoints > General > Advanced features Scroll down to Microsoft Secure Score and toggle the setting to On. Select Save preferences.
How it works
Microsoft Secure Score for Devices currently supports configurations set via Group Policy. Due to the current partial Intune support, configurations which might have been set through Intune might show up as misconfigured. Contact your IT Administrator to verify the actual configuration status in case your organization is using Intune for secure configuration management. The data in the Microsoft Secure Score for Devices card is the product of meticulous and ongoing vulnerability discovery process. It is aggregated with configuration discovery assessments that continuously:
Compare collected configurations to the collected benchmarks to discover misconfigured assets Map configurations to vulnerabilities that can be remediated or partially remediated (risk reduction) Collect and maintain best practice configuration benchmarks (vendors, security feeds, internal research teams) Collect and monitor changes of security control configuration state from all assets

QUESTION 37
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

Correct Answer: A, D
Section:
Explanation:

QUESTION 38
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

Correct Answer: B
Section:

QUESTION 39
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

Correct Answer: B
Section:

QUESTION 40
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.

Correct Answer: A
Section:
Explanation:

QUESTION 41
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

Correct Answer: A
Section:

QUESTION 42
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
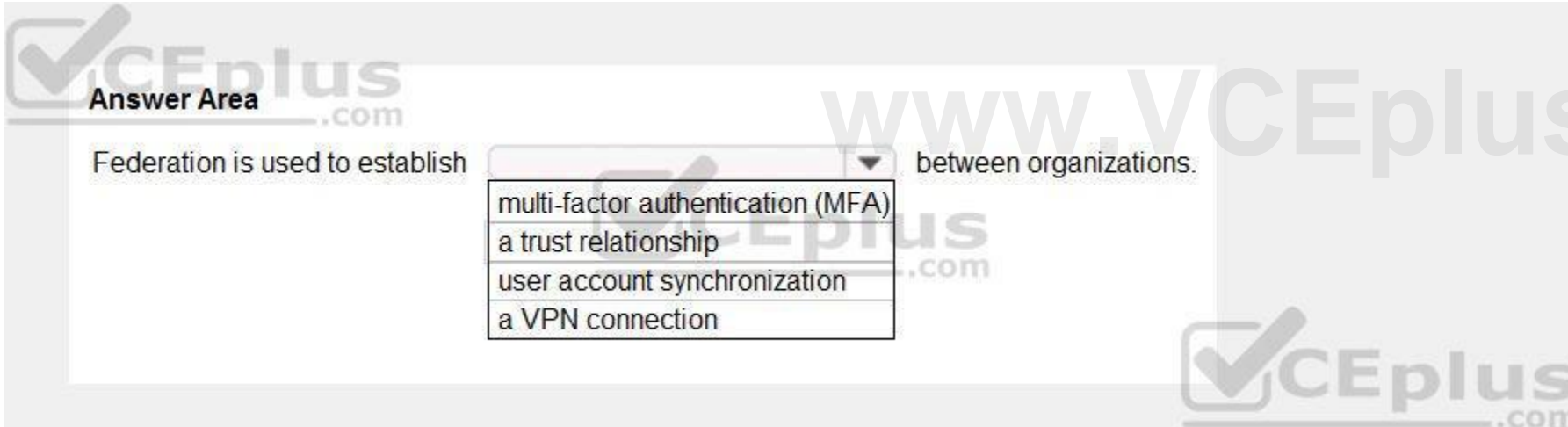
Correct Answer: A
Section:
Explanation:

QUESTION 43
HOTSPOT
Select the answer that correctly completes the sentence.
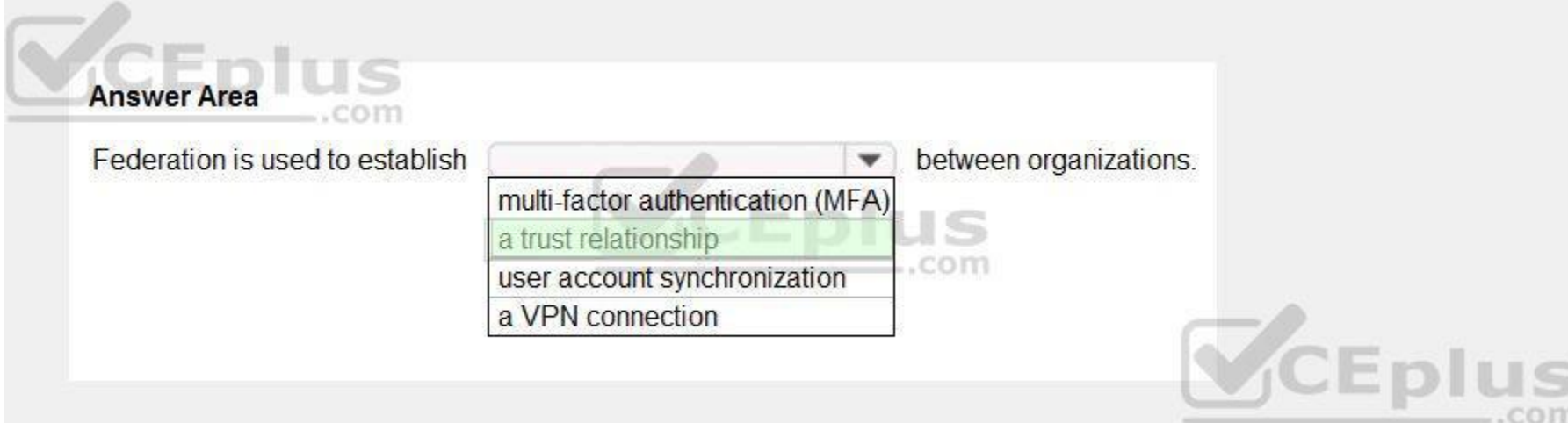
Hot Area:

Answer Area

Federation is used to establish [▼] between organizations.

| multi-factor authentication (MFA) |
| a trust relationship |
| user account synchronization |
| a VPN connection |

Answer Area:

Answer Area

Federation is used to establish [▼] between organizations.

| multi-factor authentication (MFA) |
| a trust relationship |
| user account synchronization |
| a VPN connection |

Section:

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

Answer Area:

Answer Area

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

Section:
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 45
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:

Statements	Yes	No
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 network from external threats.	○	○

Answer Area:

Answer Area

Statements	Yes	No
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 network from external threats.	○	○

Section:
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 46
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
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 Area:

Answer Area

Statements	Yes	No
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.	○	○

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

QUESTION 47
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

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 Area:

Answer Area

▼	a file makes the data in the file readable and usable to viewers that have the appropriate key.

Archiving
Compressing
Deduplicating
Encrypting

Section:
Explanation:

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.
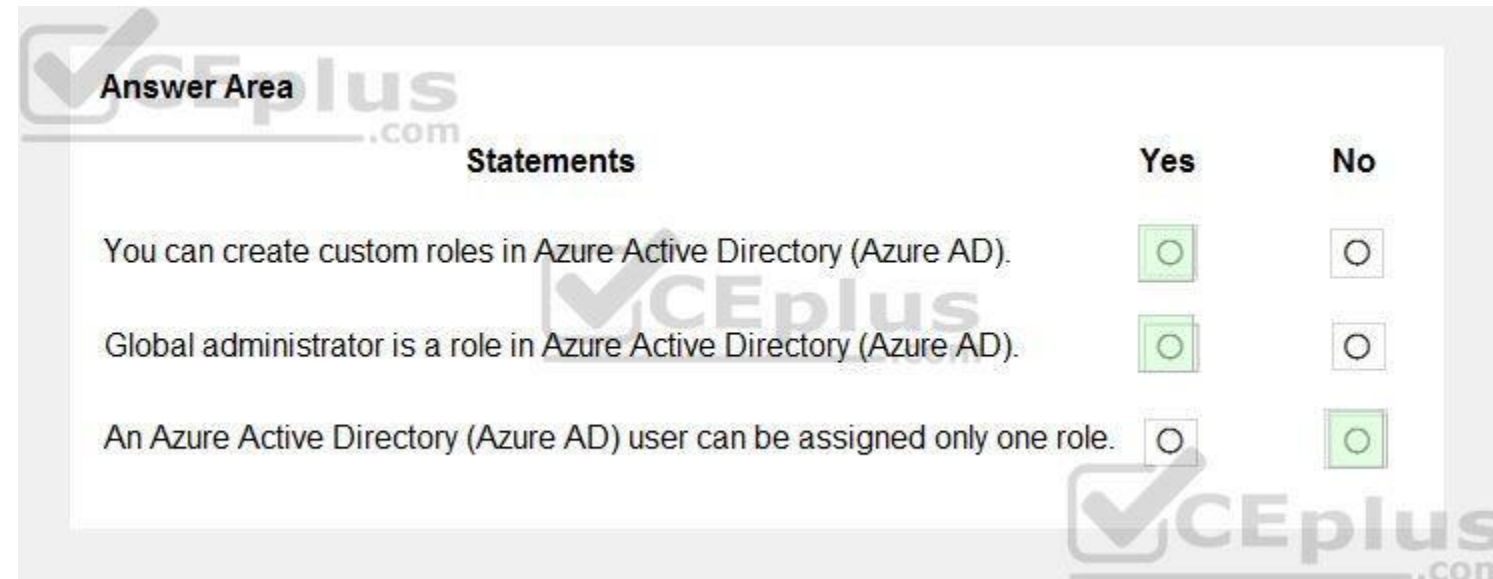
Hot Area:

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 Area:

Section:
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 49
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

Correct Answer: A
Section:

QUESTION 50
Which two cards are available in the Microsoft 365 Defender portal? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

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

Correct Answer: B, C

Section:

QUESTION 51
Which service includes the Attack simul-ation training feature?

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

Correct Answer: B
Section:

QUESTION 52
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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

Section:
Explanation:

QUESTION 53
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Insider risk management is configured from the [Microsoft Purview compliance portal. ▼]

- Microsoft 365 admin center.
- Microsoft Purview compliance portal.
- Microsoft 365 Defender portal.
- Microsoft Defender for Cloud Apps portal.

Answer Area:

Answer Area

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

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

Section:
Explanation:

QUESTION 54
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

Correct Answer: B, C
Section:

QUESTION 55
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
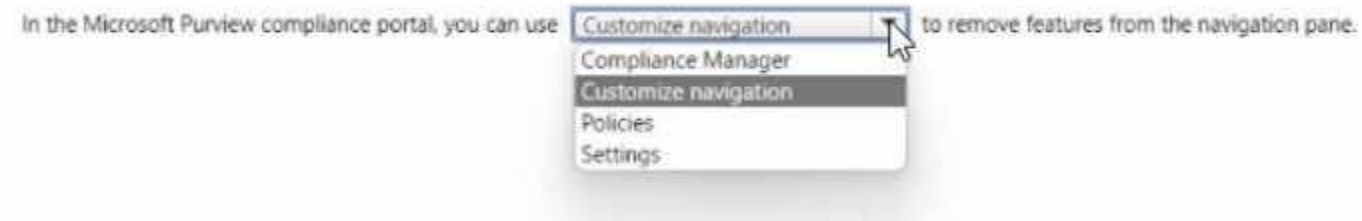
Correct Answer: D
Section:

QUESTION 56
HOTSPOT
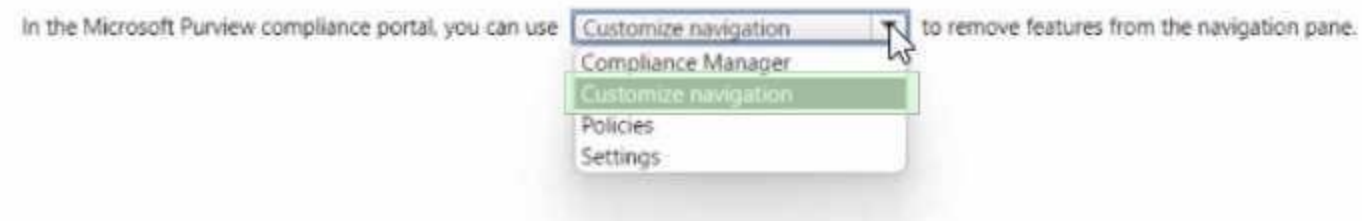Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

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

- Compliance Manager
- **Customize navigation**
- Policies
- Settings

Answer Area:

Answer Area

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

- Compliance Manager
- **Customize navigation**
- Policies
- Settings

Section:
Explanation:

QUESTION 57
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Ensuring that the data you retrieve is the same as the data you stored is an example of maintaining [availability. ▼]

- availability.
- confidentiality.
- integrity.
- transparency.

Answer Area:

Answer Area

Ensuring that the data you retrieve is the same as the data you stored is an example of maintaining [availability. ▼]

- availability.
- confidentiality.
- integrity.
- transparency.
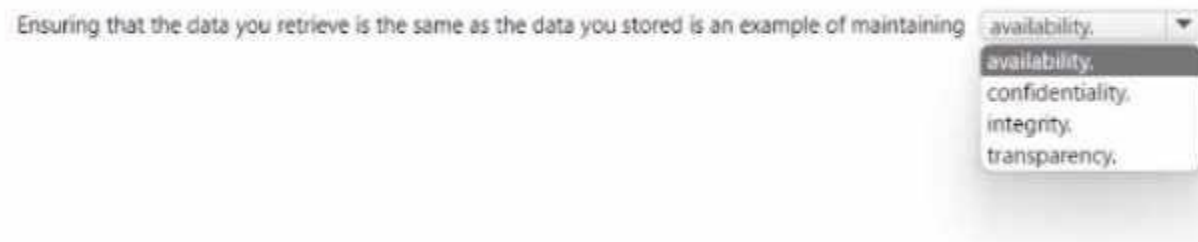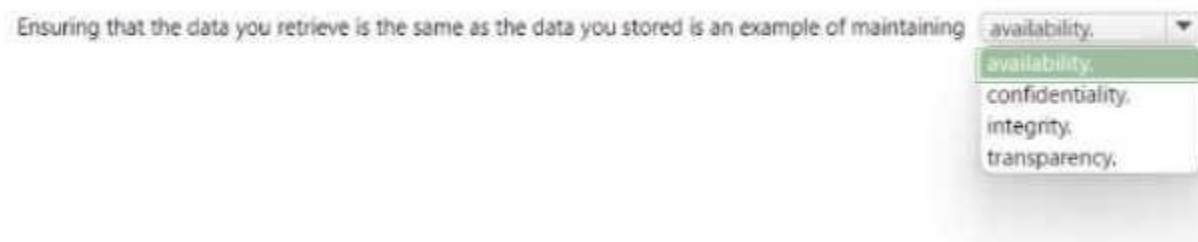
Section:
Explanation:

QUESTION 58
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

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

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

Answer Area:

Answer Area

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

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

Section:
Explanation:

QUESTION 59
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.

Hot Area:

○   er 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 self-service password reset (SSPR).	○	○
To perform self-service password reset (SSPR), a user must already be signed in and authenticated to Azure AD.	○	○

Answer Area:

○ er 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 self-service password reset (SSPR).	◉	○
To perform self-service password reset (SSPR), a user must already be signed in and authenticated to Azure AD.	○	◉

Section:
Explanation:

QUESTION 60
Which pillar of identity relates to tracking the resources accessed by a user?

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

Correct Answer: A
Section:

QUESTION 61
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:
Answer Area

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

administration
auditing
authentication
authorization

Answer Area:

Answer Area

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

administration
auditing
authentication
authorization

Section:
Explanation:

QUESTION 62
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

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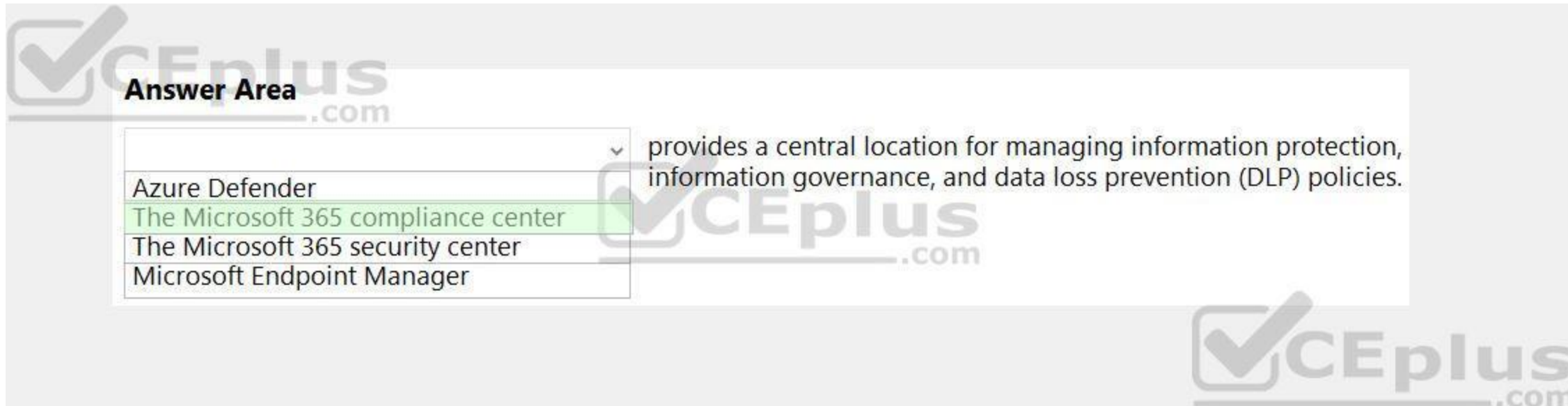
Azure Defender
The Microsoft 365 compliance center
The Microsoft 365 security center
Microsoft Endpoint Manager

Answer Area:

Answer Area

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

Dropdown options:
- Azure Defender
- **The Microsoft 365 compliance center** (selected)
- The Microsoft 365 security center
- Microsoft Endpoint Manager

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

QUESTION 63
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

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

QUESTION 64
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area:

Answer Area

| 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. |

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

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

QUESTION 65
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.

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

QUESTION 66
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

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

QUESTION 67
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 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 Area:

Answer Area

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.	☑	○

Section:
Explanation:
Box 1: Yes
Phishing scams are external threats.
Box 2: Yes
Insider risk management is a compliance solution in Microsoft 365.
Box 3: No
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 violationsReference:https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365- worldwidehttps://docs.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance- center?view=o365-worldwide

QUESTION 68
What are three uses of Microsoft Cloud App Security? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. to discover and control the use of shadow IT

B. to provide secure connections to Azure virtual machines

C. to protect sensitive information hosted anywhere in the cloud

D. to provide pass-through authentication to on-premises applications

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

Correct Answer: A, C, E
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

QUESTION 69
HOTSPOT
Select the answer that correctly completes the sentence.

Answer Area

When you enable security defaults in Azure AD,

| Azure AD Privileged Identity Management (PIM) ▼ | will be enabled for all Azure AD users. |

Azure AD Identity Protection

Azure AD Privileged Identity Management (PIM)

multi-factor authentication (MFA)

Answer Area:

Answer Area

When you enable security defaults in Azure AD,

| Azure AD Privileged Identity Management (PIM) ▼ | will be enabled for all Azure AD users. |

Azure AD Identity Protection

Azure AD Privileged Identity Management (PIM)

multi-factor authentication (MFA)

Section:

Explanation:

Answer Area

When you enable security defaults in Azure AD,

| Azure AD Privileged Identity Management (PIM) ▼ | will be enabled for all Azure AD users. |

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.

Hot Area:

Answer Area

Statements	Yes	No
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 Area:

Answer Area

Statements	Yes	No
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.	○	⊙

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

QUESTION 71
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

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

QUESTION 72
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

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

- continually
- monthly
- on-demand
- quarterly

Answer Area:

Answer Area

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

- continually
- monthly
- on-demand
- quarterly

Section:
Explanation:

QUESTION 73
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.

Select and Place:

Action Subcategories

Corrective

Detective

Preventative

Answer Area

	Encrypt data at rest.

	Perform a system access audit.

	Make configuration changes in response to a security incident.

Correct Answer:

Action Subcategories

Answer Area

Preventative	Encrypt data at rest.

Detective	Perform a system access audit.

Corrective	Make configuration changes in response to a security incident.

Section:
Explanation:

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.

Hot Area:
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 Area:

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.	○	◉

Section:
Explanation:

QUESTION 75
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

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

Assessments
Improvement actions
Solutions
Templates

Answer Area:

Answer Area

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

Assessments
Improvement actions
Solutions
Templates

Section:
Explanation:

QUESTION 76
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
Windows Hello for Business can use the Microsoft Authenticator app as an authentication 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 Area:

Answer Area

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

Section:
Explanation:

QUESTION 77
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 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 Area:

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.	☑	○

Section:
Explanation:

QUESTION 78
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:
Answer Area

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

Answer Area:
Answer Area

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

Section:
Explanation:

QUESTION 79
You have an Azure subscription.
You need to implement approval-based, time-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)

Correct Answer: D

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

QUESTION 80
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
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 Area:

Answer Area

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	●	○

Section:
Explanation:
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 81
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.

Correct Answer: B, C
Section:
Explanation:
Security defaults make it easy to protect your organization with the following preconfigured security settings:
Requiring all users to register for Azure AD Multi-Factor Authentication.
Requiring administrators to do multi-factor authentication.
Blocking legacy authentication protocols.
Requiring users to do multi-factor authentication when necessary. Protecting privileged activities like access to the Azure portal.

QUESTION 82
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

Correct Answer: A, B, D
Section:

QUESTION 83
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)

Correct Answer: B
Section:
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 84
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

Correct Answer: A
Section:

QUESTION 85
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

Correct Answer: D
Section:
Explanation:
When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.
Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

QUESTION 86
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.

Correct Answer: B, C, D
Section:

QUESTION 87
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

Correct Answer: D
Section:

QUESTION 88
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

Correct Answer: A, C, D
Section:

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

Hot Area:

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 Area:

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.	◉	○

Section:
Explanation:

QUESTION 90
HOTSPOT
Select the answer that correctly completes the sentence.

Hot Area:

The Cloud Security 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 Area:

The [Cloud Security 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.

Section:
Explanation: