

SC-900^{Q&As}

Microsoft Security Compliance and Identity Fundamentals

Pass Microsoft SC-900 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/sc-900.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

You can use dynamic groups in Azure Active Directory (Azure AD) to automate the

access
object
privileged access

lifecycle process.

Correct Answer:

Answer Area

You can use dynamic groups in Azure Active Directory (Azure AD) to automate the

access
object
privileged access

lifecycle process.

QUESTION 2

HOTSPOT

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Microsoft Purview provides sensitive data classification.	<input type="radio"/>	<input type="radio"/>
Microsoft Sentinel is a data lifecycle management solution.	<input type="radio"/>	<input type="radio"/>
Microsoft Purview can only discover data that is stored in Azure.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Microsoft Purview provides sensitive data classification.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft Sentinel is a data lifecycle management solution.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft Purview can only discover data that is stored in Azure.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes

Microsoft Purview allows you to apply sensitivity labels to assets, enabling you to classify and protect your data.

Box 2: Yes

Microsoft Sentinel content is Security Information and Event Management (SIEM) content that enables customers to ingest data, monitor, alert, hunt, investigate, respond, and connect with different products, platforms, and services in

Microsoft Sentinel.

Content sources for Microsoft Sentinel content and solutions

Each piece of content or solution has one of the following content sources:

Content hub - Content or solutions deployed by the content hub that support lifecycle management

Custom - Content or solutions you've customized in your workspace

Gallery content- Content or solutions from the gallery that don't support lifecycle management

Repositories - Content or solutions from a repository connected to your workspace

Box 3: No

Microsoft Purview provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data.

Reference:

<https://docs.microsoft.com/en-us/azure/purview/create-sensitivity-label>

<https://docs.microsoft.com/en-us/azure/sentinel/sentinel-solutions>

QUESTION 3

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

Correct Answer: A

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

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

QUESTION 4

HOTSPOT

You use project codes that have a format of three alphabetical characters that represent the project type, followed by three digits, for example Abc123.

You need to create a new sensitive info type for the project codes. How should you configure the regular expression to detect the content? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

(\s)(

▼
[aA]{3}
[abc]{3}
[alpha]{3}
[a-zA-Z]{3}

 \

▼
d{000-999}
d{123}
d{3}

) (\s)

Correct Answer:

(\s)(

▼
[aA]{3}
[abc]{3}
[alpha]{3}
[a-zA-Z]{3}

 \

▼
d{000-999}
d{123}
d{3}

) (\s)

Reference: <https://joanneklein.com/2018/08/07/build-and-use-custom-sensitive-information-types-in-office-365/>

QUESTION 5

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

In order to keep a copy of all files in a Microsoft SharePoint site for one year, even if users delete the files from the site, you should enable the Recycle Bin feature in SharePoint and set the retention period to one year.

QUESTION 6

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

Correct Answer: B

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

QUESTION 7

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

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

Correct Answer: C

QUESTION 8

HOTSPOT

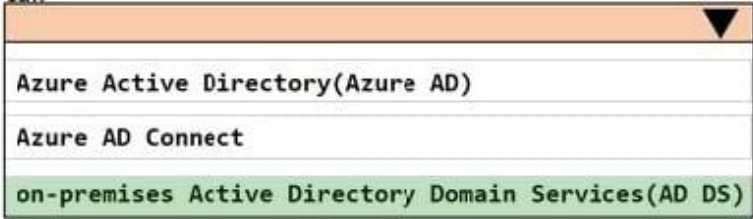
Select the answer that correctly completes the sentence.

Hot 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)

Correct Answer:

Microsoft Defender for Identity can identify advanced threats from  signals.

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.

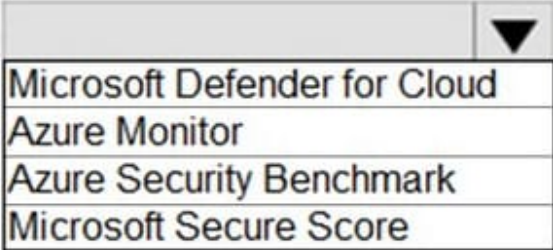
QUESTION 9

HOTSPOT

Select the answer that correctly completes the sentence.

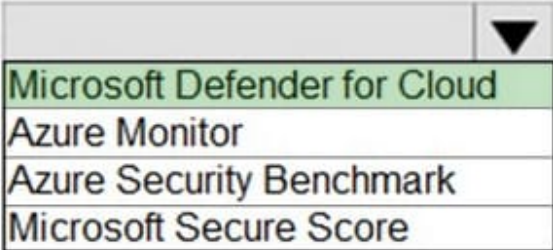
Hot Area:

Answer Area

 provides cloud workload protection for Azure and hybrid cloud resources.

Correct Answer:

Answer Area

 provides cloud workload protection for Azure and hybrid cloud resources.

Azure Defender for Cloud Microsoft Defender for Cloud is a solution for cloud security posture management (CSPM)

and cloud workload protection (CWP) that finds weak spots across your cloud configuration, helps strengthen the overall security posture of your environment, and can protect workloads across multicloud and hybrid environments from evolving threats.

Microsoft Defender for Servers is one of the plans provided by Microsoft Defender for Cloud's enhanced security features. Defender for Servers protects your Windows and Linux machines in Azure, AWS, GCP, and on-premises.

Reference: <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction>

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction>

QUESTION 10

DRAG DROP

Match the Microsoft 365 insider risk management workflow step to the appropriate task.

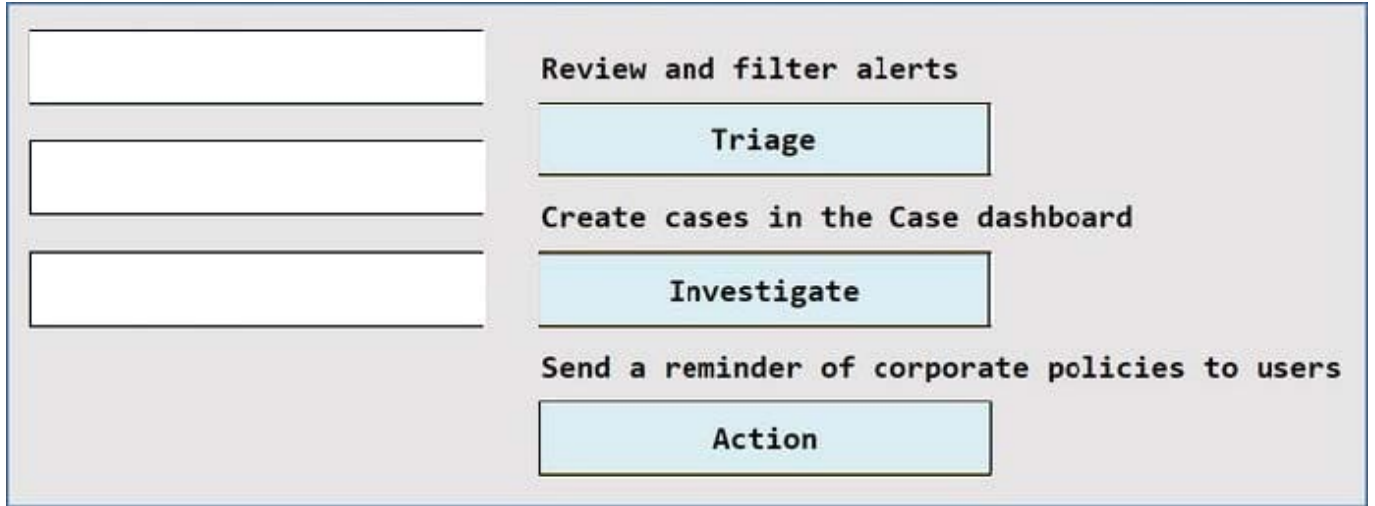
To answer, drag the appropriate step from the column on the left to its task on the right. Each step may be used once, more than once, or not at all.

NOTE: Each correct match is worth one point.

Select and Place:

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

Correct Answer:



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

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:

Statements	Yes	No
Applying system updates increases an organization's secure score in Azure Security Center.	<input type="radio"/>	<input type="radio"/>
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	<input type="radio"/>	<input type="radio"/>
Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
Applying system updates increases an organization's secure score in Azure Security Center.	<input checked="" type="radio"/>	<input type="radio"/>
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	<input checked="" type="radio"/>	<input type="radio"/>
Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	<input checked="" type="radio"/>	<input type="radio"/>

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 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	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	<input type="radio"/>	<input type="radio"/>
Windows Hello for Business can use a PIN code as an authentication method.	<input type="radio"/>	<input type="radio"/>
Windows Hello for Business authentication information syncs across all the devices registered by a user.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	<input type="radio"/>	<input checked="" type="radio"/>
Windows Hello for Business can use a PIN code as an authentication method.	<input checked="" type="radio"/>	<input type="radio"/>
Windows Hello for Business authentication information syncs across all the devices registered by a user.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No

The Microsoft Authenticator app helps you sign in to your accounts when you\\re using two-factor verification. Two-factor verification helps you to use your accounts more securely because passwords can be forgotten, stolen, or compromised.

Two-factor verification uses a second factor like your phone to make it harder for other people to break in to your account.

Box 2: Yes

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

Box 3: No

Windows Hello credentials are based on certificate or asymmetrical key pair. Windows Hello credentials can be bound to the device, and the token that is obtained using the credential is also bound to the device.

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

QUESTION 13

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

<input type="text"/>	▼
Azure Defender	
The Microsoft 365 compliance center	
The Microsoft 365 security center	
Microsoft Endpoint Manager	

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

Correct Answer:

Answer Area

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

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

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

QUESTION 14

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

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

Correct Answer: D

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

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

QUESTION 15

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

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

Correct Answer: B

Audit logs in Azure Active Directory

As an IT administrator, you want to know how your IT environment is doing. The information about your system's health enables you to assess whether and how you need to respond to potential issues.

To support you with this goal, the Azure Active Directory portal gives you access to three activity logs:

Sign-ins

[Latest SC-900 Dumps](#)

[SC-900 Practice Test](#)

[SC-900 Braindumps](#)