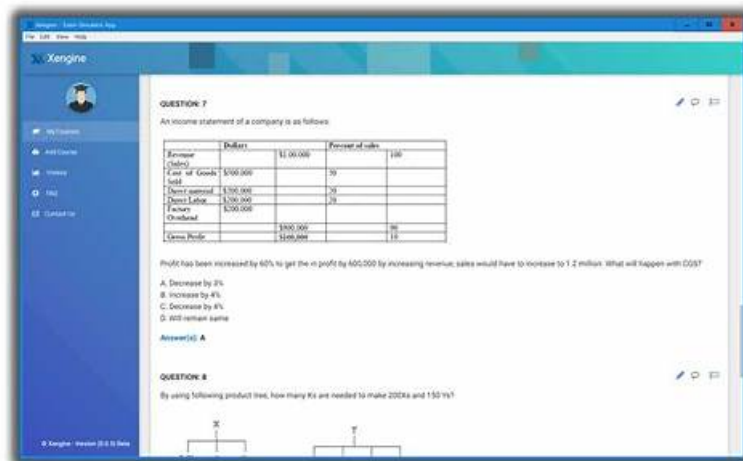


Latest SC-401 Exam Labs & SC-401 Training Tools



BONUS!!! Download part of CertkingdomPDF SC-401 dumps for free: <https://drive.google.com/open?id=16cZayKyrw3EC6bmFu2bHAbi03A8-AwO>

As long as you study with our SC-401 training braindump, then you will find that it is designed to deepened the understanding of the users and memory. Simple text messages, deserve to go up colorful stories and pictures beauty, make the SC-401 test guide better meet the zero basis for beginners, let them in the relaxed happy atmosphere to learn more useful knowledge, more good combined with practical, so as to achieve the state of unity. It is easy to pass with our SC-401 Practice Questions as our pass rate of SC-401 exam material is more than 98%.

Microsoft SC-401 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> Protect Data Used by AI Services: This section evaluates AI Governance Specialists on securing data in AI-driven environments. It includes implementing controls for Microsoft Purview, configuring Data Security Posture Management (DSPM) for AI, and monitoring AI-related security risks to ensure compliance and protection.
Topic 2	<ul style="list-style-type: none"> Manage Risks, Alerts, and Activities: This section assesses Security Operations Analysts on insider risk management, monitoring alerts, and investigating security activities. It covers configuring risk policies, handling forensic evidence, and responding to alerts using Microsoft Purview and Defender tools. Candidates must also analyze audit logs and manage security workflows.
Topic 3	<ul style="list-style-type: none"> Implement Data Loss Prevention and Retention: This section evaluates Data Protection Officers on designing and managing data loss prevention (DLP) policies and retention strategies. It includes setting policies for data security, configuring Endpoint DLP, and managing retention labels and policies. Candidates must understand adaptive scopes, policy precedence, and data recovery within Microsoft 365.
Topic 4	<ul style="list-style-type: none"> Implement Information Protection: This section measures the skills of Information Security Analysts in classifying and protecting data. It covers identifying and managing sensitive information, creating and applying sensitivity labels, and implementing protection for Windows, file shares, and Exchange. Candidates must also configure document fingerprinting, trainable classifiers, and encryption strategies using Microsoft Purview.

>> Latest SC-401 Exam Labs <<

Microsoft SC-401 Training Tools, SC-401 Test Questions Answers

We have the first-rate information safety guarantee system for the buyers who buy the SC-401 questions and answers of our company, we can ensure that the information of your name, email, or product you buy. We respect the private information of every customer, and we won't send the junk information to you to bother. Besides, you will get SC-401 Questions and answers downloading link within ten minutes, and our system will send you the update version to your mailbox.

Microsoft Administering Information Security in Microsoft 365 Sample Questions (Q161-Q166):

NEW QUESTION # 161

You have a Microsoft 365 E5 subscription that contains four users named User1, User2, User3, and User4 and a file named File1.docx.

To File1, you apply a sensitivity label that has the permissions shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Explanation:

Step 1 - Summarization in Copilot

For Microsoft 365 Copilot to summarize a file:

The user needs at least View permission.

Summarization does not require editing, copying, or ownership rights.

Looking at the exhibit:

User1 (Co-Owner) # has full access including view.

User2 (Co-Author) # has edit and view.

User3 (Reviewer) # has read-only rights.

User4 (Viewer) # has read rights.

All four users can view the document. Therefore, Copilot can summarize File1 for User1, User2, User3, and User4.

Step 2 - Referencing a file by link in Copilot

For Copilot to reference a file by link (i.e., cite or share within generated content):

The user must have rights that include resharing or exporting.

Only the Co-Owner has full rights to manage access and allow referencing by link.

From the exhibit:

User1 (Co-Owner) # Can reference by link.

User2 (Co-Author), User3 (Reviewer), User4 (Viewer) # Do not have reshare or link rights.

So, only User1 can reference File1 by link.

Reference: Sensitivity labels and Microsoft 365 Copilot

NEW QUESTION # 162

You have a Microsoft OneDrive folder that contains the files shown in the following table.

In Microsoft Defender for Cloud Apps, you create a file policy to automatically apply a classification. What is the effect of applying the policy?

- A. The policy will apply to only the .docx and .txt files. The policy will classify the files within 24 hours.
- B. The policy will apply to all the files. The policy will classify only 100 files daily.
- C. The policy will apply to only the docx and txt files. The policy will classify the files immediately.
- D. The policy will apply to only the .docx files. The policy will classify only 100 files daily.

Answer: A

NEW QUESTION # 163

You have a Microsoft 365 subscription. Auditing is enabled.

A user named User1 is a member of a dynamic security group named Group1.

You discover that User1 is no longer a member of Group1.

You need to search the audit log to identify why User1 was removed from Group1.

Which two activities should you use in the search? To answer, select the appropriate activities in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Explanation:

Step 1 - Scenario

A user named User1 was a member of a dynamic security group (Group1).

User1 is no longer a member of that group.

You need to determine why User1 was removed by searching the audit log.

Step 2 - How group membership changes are logged in Microsoft 365 audit logs Microsoft 365 audit logs record group membership activities in Azure AD. The most relevant activities for a user disappearing from a group are:

Removed member from group - Directly indicates that a user was removed from a group.

Updated group - Logged when group properties or membership rules (for dynamic groups) are modified. If Group1 is a dynamic group, changes to membership rules could have caused User1 to no longer qualify, and this would appear as an Updated group event.

Step 3 - Why not other options

Deleted user / Deleted group: Would mean the entire user or group object was deleted, not just removal.

Changed user password, Reset user password, Set license properties, Changed user license: These are account- related, not group membership-related.

Added member to group: The opposite action.

Step 4 - Microsoft Reference

From Microsoft documentation:

Audit logs include events such as when a member is added or removed from a group, and when group properties or membership rules are updated.

Reference: Search the audit log in the Microsoft Purview compliance portal

NEW QUESTION # 164

You have a Microsoft 365 E5 subscription that contains a device named Device1.

You need to enable Endpoint data loss prevention (Endpoint DLP) for Device1.

What should you do first in the Microsoft Purview portal?

- A. Create a Microsoft Purview Information Barriers (IBs) segment.
- **B. Turn on device onboarding.**
- C. Add a Microsoft Purview Information Protection scanner cluster.
- D. Enable Microsoft Privacy Risk Management.
- E. Onboard Device1 to Microsoft Purview.

Answer: B

NEW QUESTION # 165

You have a Microsoft 365 E5 tenant that has devices onboarded to Microsoft Defender for Endpoint as shown in the following table.

You plan to start using Microsoft 365 Endpoint data loss protection (Endpoint DLP).

Which devices support Endpoint DLP?

- A. Device1 and Device4 only
- **B. Device1 and Device2 only**
- C. Device1, Device2, and Device4 only
- D. Device1, Device2, Device3, and Device4
- E. Device1 only

Answer: B

Explanation:

Microsoft 365 Endpoint data loss prevention (Endpoint DLP) is supported only on Windows 10 and Windows 11 devices. It does not support macOS or iOS at this time.

