

Pass Guaranteed 2026 Trustable Microsoft SC-401 Reliable Test Guide



P.S. Free & New SC-401 dumps are available on Google Drive shared by PrepPDF: <https://drive.google.com/open?id=1Q0J0FZsgxOMq8xEy5nwZAILzhdL-HHbU>

Probably you've never imagined that preparing for your upcoming certification SC-401 could be easy. The good news is that PrepPDF's dumps have made it so! The brilliant certification exam SC-401 is the product created by those professionals who have extensive experience of designing exam study material. These professionals have deep exposure of the test candidates' problems and requirements hence our SC-401 cater to your need beyond your expectations.

Microsoft SC-401 Exam Syllabus Topics:

| Topic | Details |
|---------|--|
| Topic 1 | <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. |
| Topic 2 | <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 3 | <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 4 | <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. |

>> SC-401 Reliable Test Guide <<

Practice SC-401 Exam Fee & Printable SC-401 PDF

Our SC-401 study materials cover three versions, they can meet all your needs. You can choose different versions according to your

own needs. SC-401 PDF materials is instant access to download, if you like, it can be transformed into a paper version, you can put it into your bags. SC-401 Soft test engine and SC-401 online test engine are also can be your choice, SC-401 online test engine using the online tool and it can also provide the record for your process, and SC-401 online test engine can practice online anytime. If you have the needs like this, just choose us.

Microsoft Administering Information Security in Microsoft 365 Sample Questions (Q20-Q25):

NEW QUESTION # 20

You have a Microsoft 365 subscription that contains the devices shown in the following table.

From which devices can Microsoft Purview Insider Risk Management capture forensic evidence?

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

Answer: B

Explanation:

Forensic evidence in Microsoft Purview Insider Risk Management allows capturing screenshots/clips of user activity on endpoints.

Requirements for forensic evidence capture:

The device must be onboarded to Microsoft Purview (via Defender for Endpoint).

The Microsoft Purview client must be installed.

Supported platforms: Windows 10 and Windows 11 (macOS is not supported for forensic evidence).

Now check each device:

Device1 (Windows 11) # Client installed, but not onboarded ## Not eligible.

Device2 (Windows 10) # Onboarded and client installed ## Eligible.

Device3 (macOS) # Onboarded, but client not installed and macOS is not supported ## Not eligible.

Therefore, only Device2 qualifies.

Reference:

Microsoft Learn: Forensic evidence in insider risk management

Microsoft Learn: Onboard devices for insider risk management forensic evidence

NEW QUESTION # 21

You have a Microsoft 365 E5 subscription.

You need to create a Microsoft Defender for Cloud Apps policy that will detect data loss prevention (DLP) violations.

What should you create?

- A. an access policy
- B. a session policy
- **C. a file policy**
- D. an activity policy

Answer: C

Explanation:

To create a Data Loss Prevention (DLP) policy in Microsoft Defender for Cloud Apps, go to the Microsoft Defender Portal, navigate to Cloud Apps > Policies > Policy management, and create a new File policy. Define the conditions by selecting a file filter and configuring the Data Classification Service for content inspection, then choose an Action for violations, such as creating an alert, and optionally, implementing a governance action like moving the file to quarantine. You can optionally set a policy severity, link it to risk types, and use sensitivity labels to ensure accurate file filtering.

Reference:

<https://learn.microsoft.com/en-us/training/modules/create-configure-data-loss-prevention-policies/3-integrate-data-loss-prevention-with-microsoft-cloud-app-security>

NEW QUESTION # 22

You need to test Microsoft Purview Advanced Message Encryption capabilities for your company.

The test must verify the following information:

- The acquired default template names
- The encryption and decryption verification status

Which PowerShell cmdlet should you run?

- A. Test-OAuthConnectivity
- B. Test-Mailflow
- **C. Test-IRMConfiguration**
- D. Test-ClientAccessRule

Answer: C

Explanation:

Verify Microsoft Purview Message Encryption configuration in Exchange Online PowerShell You can verify that your Microsoft 365 tenant is properly configured to use Microsoft Purview Message Encryption in Exchange Online PowerShell.

1. Using a work or school account that has sufficient permissions in your organization, such as Compliance Administrator, start a Windows PowerShell session and connect to Exchange Online.

For instructions, see Connect to Exchange Online PowerShell.

2. Run the Get-IRMConfiguration cmdlet.

You should see a value of \$True for the AzureRMSLicensingEnabled parameter, which indicates that Microsoft Purview Message Encryption is configured in your tenant. If it is not, use Set-IRMConfiguration to set the value of AzureRMSLicensingEnabled to \$True to enable Microsoft Purview Message Encryption.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/set-up-new-message-encryption-capabilities>

NEW QUESTION # 23

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 contains three files named File1, File2, and File3.

You create the data loss prevention (DLP) policies shown in the following table.

The DLP rule matches for each file are shown in the following table.

How many DLP policy matches events will be added to Activity explorer, and how many policy matches will be added to the DLP incidents report? To answer, select the appropriate options in the answer area.

Answer:

Explanation:

Explanation:

Activity Explorer logs a DLP rule match event each time any DLP rule condition is met on a file.

File1 matches Rule11 and Rule12 # 2 events

File2 matches Rule21 and Rule22 # 2 events

File3 matches Rule11 and Rule22 # 2 events

Total events in Activity Explorer = 2 + 2 + 2 = 6.

Microsoft notes that Activity explorer shows granular DLP activities such as policy rule matches per item.

The DLP incidents report aggregates by policy match per item, not by each rule in that policy. Multiple rules from the same policy on the same item count as one incident; if different policies match the same item, each policy creates its own incident.

File1: Rules from DLP1 only # 1 incident

File2: Rules from DLP2 only # 1 incident

File3: One rule from DLP1 and one from DLP2 # 2 incidents

Total incidents = 1 + 1 + 2 = 4.

References: Microsoft Purview DLP explains that Activity explorer records detailed DLP activities, while DLP incidents are created when a policy match occurs for an item, and multiple rule matches within a single policy are consolidated into a single incident for that item.

NEW QUESTION # 24

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and

Johannesburg.

Existing Environment

Microsoft 365 Environment

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Users store data in the following locations:

- SharePoint sites
- OneDrive accounts
- Exchange email
- Exchange public folders
- Teams chats
- Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.

Site4 has the following two retention policies applied:

- Name: Site4RetentionPolicy1

Locations to apply the policy: Site4

Delete items older than: 2 years

Delete content based on: When items were created

- Name: Site4RetentionPolicy2

Locations to apply the policy: Site4

Retain items for a specific period: 4 years

Start the retention period based on: When items were created

At the end of the retention period: Do nothing

Problem Statements

Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements

Planned Changes

Contoso plans to create the following data loss prevention (DLP) policy:

- Name: DLPpolicy1

Locations to apply the policy: Site2

Conditions:

Content contains any of these sensitive info types: SWIFT Code

- Instance count: 2 to any

Actions: Restrict access to the content

Technical Requirements

Contoso must meet the following technical requirements:

- All administrative users must be able to review DLP reports.
- Whenever possible, the principle of least privilege must be used.
- For all users, all Microsoft 365 data must be retained for at least one year.
- Confidential documents must be detected and protected by using Microsoft 365.
- Site1 documents that include credit card numbers must be labeled automatically.
- All administrative users must be able to create Microsoft 365 sensitivity labels.
- After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

Hotspot Question

You need to meet the technical requirements for the confidential documents.

What should you create first, and what should you use for the detection method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

□

Answer:

Explanation:

Explanation:

Sensitive information types :

Identifies sensitive data by using built-in or custom regular expressions or a function.

Corroborative evidence includes keywords, confidence levels, and proximity.

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

NEW QUESTION # 25

.....

This helps you save your money and time as the actual Administering Information Security in Microsoft 365 SC-401 certification exam costs a high fee. Microsoft also offers 365 days free updates if the SC-401 certification exam content changes after the purchase of the Microsoft SC-401 Exam Dumps. We guarantee our valued customers that you will qualify for your Microsoft SC-401 exam, hence this saves you time and money.

Practice SC-401 Exam Fee: <https://www.preppdf.com/Microsoft/SC-401-prepaway-exam-dumps.html>

- [illegible]

What's more, part of that PrepPDF SC-401 dumps now are free: <https://drive.google.com/open?id=1Q0J0FZsgxOMq8xEy5nwZAILzhdL-HHbU>