



Microsoft

Exam Questions SC-401

Administering Information Security in Microsoft 365

NEW QUESTION 1

DRAG DROP - (Topic 1)

You need to meet the technical requirements for the Site1 documents.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

- Create a sensitivity label.
- Wait 24 hours and then turn on the policy.
- Create a sensitive info type.
- Create a retention label.
- Create an auto-labeling policy.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The goal is to automatically label documents in Site1 that contain credit card numbers. To achieve this, we need a sensitivity label with an auto-labeling policy based on a sensitive

info type that detects credit card numbers.

Step 1: Create a Sensitive Info Type

A sensitive info type is needed to detect credit card numbers in documents.

Microsoft Purview includes built-in sensitive info types for credit card numbers, but we can also create a custom one if necessary.

Step 2: Create a Sensitivity Label

A sensitivity label is required to classify and protect documents containing sensitive information.

This label can apply encryption, watermarking, or access controls to credit card data.

Step 3: Create an Auto-Labeling Policy

An auto-labeling policy ensures that the sensitivity label is applied automatically when credit card numbers are detected in Site1.

This policy is configured to scan files and automatically apply the correct sensitivity label.

NEW QUESTION 2

HOTSPOT - (Topic 1)

You are reviewing policies for the SharePoint Online environment.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

- If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.
- If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2023.
- If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2026.

| Yes | No |
|-------------------------------------|--------------------------|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

AI-generated content may be incorrect. Understanding Site4's Retention Policies:

Site4RetentionPolicy1 deletes items older than 2 years from creation. If a file was created on January 1, 2021, it would be deleted after January 1, 2023.

Site4RetentionPolicy2 retains files for 4 years from creation. If a file was created on January 1, 2021, it will be kept until January 1, 2025, but not deleted after that (policy states "Do nothing").

Statement 1 - Yes, because Site4RetentionPolicy2 ensures files are retained for 4 years. Statement 2 - Yes, because Site4RetentionPolicy2 retains the file for 4 years (until January 1, 2025).

Statement 3 - No, because retention is only for 4 years (until January 1, 2025). After that, the policy does "nothing," meaning the file is no longer recoverable after that period.

NEW QUESTION 3

- (Topic 2)

Your company has a Microsoft 365 tenant.

The company performs annual employee assessments. The assessment results are recorded in a document named AssessmentTemplate.docx that is created by using a Microsoft Word template. Copies of the employee assessments are sent to employees and their managers.

The assessment copies are stored in mailboxes, Microsoft SharePoint Online sites, and OneDrive folders. A copy of each assessment is also stored in a SharePoint Online folder named Assessments.

You need to create a data loss prevention (DLP) policy that prevents the employee assessments from being emailed to external users. You will use a document fingerprint to identify the assessment documents. The solution must minimize effort.

What should you include in the solution?

- A. Create a fingerprint of AssessmentTemplate.docx.
- B. Create a sensitive info type that uses Exact Data Match (EDM).
- C. Import 100 sample documents from the Assessments folder to a seed folder.
- D. Create a fingerprint of 100 sample documents in the Assessments folder.

Answer: A

Explanation:

Since all employee assessments follow a specific template (AssessmentTemplate.docx), the best way to identify these documents for Data Loss Prevention (DLP) is to create a document fingerprint of that template.

Document fingerprinting allows Microsoft 365 DLP policies to recognize documents based on their structure and format, even when content inside varies (such as different employee names and results). By creating a fingerprint of AssessmentTemplate.docx, any copy derived from that template will be automatically detected by the DLP policy and blocked from being emailed externally.

Steps to implement:

Create a document fingerprint of AssessmentTemplate.docx using PowerShell and the Microsoft Purview compliance portal.

Apply a DLP policy to prevent external sharing of documents matching this fingerprint. Test the policy by attempting to email an assessment externally.

NEW QUESTION 4

HOTSPOT - (Topic 2)

You have a new Microsoft 365 E5 tenant.

You need to create a custom trainable classifier that will detect product order forms. The solution must use the principle of least privilege.

What should you do first? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Action to perform:

To perform the action, assign the role of:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To create a custom trainable classifier in Microsoft Purview (formerly Microsoft Compliance Center), you must first opt into the trainable classifier feature.

Before using custom trainable classifiers, Microsoft requires manual opt-in through the Microsoft Purview compliance portal. Without this step, you cannot create a new classifier.

The Compliance Administrator role has the necessary permissions to configure data classification, DLP policies, and trainable classifiers. Global Administrator has higher privileges but is not required for this task, violating the principle of least privilege. Security Administrator is focused on security-related settings but does not manage compliance features like classifiers.

NEW QUESTION 5

- (Topic 2)

You have a Microsoft 365 E5 subscription. The subscription contains 500 devices that are onboarded to Microsoft Purview. You select Activate Microsoft Purview Audit. You need to ensure that you can track interactions between users and generative AI websites. What should you deploy to the devices?

- A. the Microsoft Purview extension
- B. the Microsoft Purview Information Protection client
- C. the Microsoft Defender Browser Protection extension
- D. Endpoint analytics

Answer: A

Explanation:

To track interactions between users and generative AI websites in Microsoft Purview Audit, you need to deploy the Microsoft Purview browser extension to the devices. This extension enables tracking of user activities on web-based applications, including AI-related tools like ChatGPT, Microsoft Copilot, and other generative AI platforms. Microsoft Purview extension provides visibility into browser-based activities, including AI tool usage, ensuring compliance and risk management within Microsoft Purview. This extension works with Microsoft Edge and Google Chrome to track and log user interactions.

NEW QUESTION 6

- (Topic 2)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1. Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1. Solution: You run the Set-MailboxFolderPermission -Identity "User1" -User User1@contoso.com -AccessRights Owner command.

Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

The Set-MailboxFolderPermission -Identity "User1" -User User1@contoso.com - AccessRights Owner command is incorrect. This assigns folder permissions but does not enable auditing. It does not track who accessed the mailbox or deleted emails.

NEW QUESTION 7

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to review a Microsoft 365 Copilot usage report. From where should you review the report?

- A. Information Protection in the Microsoft Purview portal
- B. the Microsoft 365 admin center
- C. DSPM for AI in the Microsoft Purview portal
- D. the Microsoft Defender portal

Answer: C

Explanation:

To review a Microsoft 365 Copilot usage report, you need to use Data Security Posture Management for AI (DSPM for AI) in the Microsoft Purview portal. DSPM for AI provides insights into AI-related activities, including Copilot usage, risk assessments, and data security posture related to AI interactions within Microsoft 365.

NEW QUESTION 8

DRAG DROP - (Topic 2)

You have a Microsoft 365 subscription that contains 20 data loss prevention (DLP) policies. You need to identify the following:

Rules that are applied without triggering a policy alert The top 10 files that have matched DLP policies Alerts that are miscategorized

Which report should you use for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

| Reports | Answer Area | Report |
|-----------------------------|---|----------------------|
| DLP policy matches | Rules that are applied without triggering a policy alert: | <input type="text"/> |
| False positive and override | The top 10 files that have matched DLP policies: | <input type="text"/> |
| Incident reports | Alerts that are miscategorized: | <input type="text"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The False positive and override report helps identify rules that were applied but did not generate an actual policy alert, which means they were overridden or deemed false positives.

The DLP policy matches report provides details on files that matched DLP policies, including the top 10 files.

The Incident reports report helps analyze and review alerts, including those that may have been miscategorized.

NEW QUESTION 9

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to implement Microsoft Purview data lifecycle management. What should you create first?

- A. a sensitivity label policy
- B. a data loss prevention (DLP) policy
- C. an auto-labeling policy
- D. a retention label

Answer: D

Explanation:

To implement Microsoft Purview Data Lifecycle Management for SharePoint Online (Site1), you need to create a retention label first. Retention labels define how long content should be retained or deleted based on compliance requirements. Once a retention label is created, it can be manually or automatically applied to content in SharePoint Online, Exchange, OneDrive, and Teams. After creating a retention label, you can configure label policies to apply them to Site1 and other locations.

NEW QUESTION 10

- (Topic 2)

You have a Microsoft 365 subscription.

You need to customize encrypted email for the subscription. The solution must meet the following requirements.

Ensure that when an encrypted email is sent, the email includes the company logo. Minimize administrative effort.

Which PowerShell cmdlet should you run?

- A. Set-IRMConfiguration
- B. Set-OMEConfiguration
- C. Set-RMSTemplate
- D. New-OMEConfiguration

Answer: B

Explanation:

To customize encrypted email in Microsoft 365, including adding a company logo, you need to modify the Office Message Encryption (OME) branding settings. The Set-OMEConfiguration PowerShell cmdlet allows you to configure branding elements such as: Company logo

Custom text Background color

This cmdlet is used to update existing OME branding settings, ensuring that encrypted emails sent from your organization include the required customizations.

NEW QUESTION 10

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to prevent users from uploading data loss prevention (DLP)-protected documents to the following third-party websites:

web1.contoso.com web2.contoso.com

The solution must minimize administrative effort.

To what should you set the Service domains setting for Endpoint DLP?

- A. *.contoso.com
- B. contoso.com
- C. web1.contoso.com and web2.contoso.com
- D. web*.contoso.com

Answer: C

Explanation:

The Service domains setting in Microsoft 365 Endpoint Data Loss Prevention (Endpoint DLP) allows administrators to block or allow specific domains for file uploads. The goal is to prevent users from uploading DLP-protected documents to web1.contoso.com and web2.contoso.com.

Setting the Service domains to "web1.contoso.com and web2.contoso.com" precisely targets the two specific third-party websites, minimizing administrative effort while ensuring strict control.

NEW QUESTION 14

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to create a sensitivity label named Label1. The solution must ensure that users can use Microsoft 365 Copilot to summarize files that have Label1 applied.

Which permission should you select for Label1?

- A. Export content(EXPORT)
- B. Copy and extract content(EXTRACT)

- C. Edit content(DOCEDIT)
- D. View rights(VIEW)

Answer: B

Explanation:

To allow Microsoft 365 Copilot to summarize files that have Label1 applied, the label must grant permission to extract content from the document. The correct permission for this is Copy and extract content (EXTRACT).
 Microsoft 365 Copilot requires access to read and process content in documents to generate summaries. The EXTRACT permission allows users (and AI tools like Copilot) to copy and extract content for processing while still maintaining the protection applied by the sensitivity label.

NEW QUESTION 19

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription. The subscription contains devices that are onboarded to Microsoft Purview and configured as shown in the following table.

| Name | Operating system | Microsoft Purview browser extension |
|---------|------------------|-------------------------------------|
| Device1 | Windows 11 | Installed |
| Device2 | Windows 11 | Not installed |
| Deivce3 | macOS | Installed |

The subscription contains the users shown in the following table.

| Name | Activity performed during the last seven days | On device |
|-------|---|-----------|
| User1 | Used a generative AI website to generate an image | Device1 |
| User2 | Asked Microsoft 365 Copilot to summarize a document | Device2 |
| User3 | Browsed sample content on a generative AI website | Device3 |

You need to review the activities.

What should you use for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1: Activity explorer in Data Security Posture Management for AI (DSPM for AI)
 Audit log search
 Insider risk audit log
 Unified Catalog

User2: Activity explorer in Data Security Posture Management for AI (DSPM for AI)
 Audit log search
 Insider risk audit log
 Unified Catalog

User3: Activity explorer in Data Security Posture Management for AI (DSPM for AI)
 Audit log search
 Insider risk audit log
 Unified Catalog

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1: Since the Microsoft Purview browser extension is installed on Device1, AI-related activity performed by User1 (generating an image using a generative AI website) can be reviewed in Activity explorer in DSPM for AI.
 User2: Since Device2 does not have the Microsoft Purview browser extension installed, AI-related activity cannot be tracked in DSPM for AI. Instead, Audit log

search should be used to review activity such as using Microsoft 365 Copilot.

User3: Since Device3 has the Microsoft Purview browser extension installed, AI-related activity (browsing sample content on a generative AI website) can be reviewed using Activity explorer in DSPM for AI.

NEW QUESTION 20

HOTSPOT - (Topic 2)

You have a Microsoft SharePoint Online site that contains the following files.

| Name | Modified by | Data loss prevention (DLP) action |
|------------|-------------|-----------------------------------|
| File1.docx | Manager1 | None |
| File2.docx | Manager1 | Matched by DLP |
| File3.docx | Manager1 | Blocked by DLP |

Users are assigned roles for the site as shown in the following table.

| Name | Role |
|-------|-------------|
| User1 | Site owner |
| User2 | Site member |

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:

▼

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

▼

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

NEW QUESTION 24

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains a trainable classifier named Trainable1.

You plan to create the items shown in the following table.

| Name | Type |
|---------|-----------------------------------|
| Label1 | Sensitivity label |
| Label2 | Retention label |
| Policy1 | Retention label policy |
| DLP1 | Data loss prevention (DLP) policy |

Which items can use Trainable 1?

- A. Label2 only
- B. Label1 and Label2 only
- C. Label1 and Policy1 only
- D. Label2, Policy1, and DLP1 only
- E. Label1, Label2, Policy1, and DLP1

Answer: D

Explanation:

A trainable classifier in Microsoft Purview is used to automatically identify and classify unstructured data based on content patterns. The classifier can be used in:

* 1. Retention Labels (Label2) Supported

Trainable classifiers can be linked to retention labels to automatically classify and apply retention policies to documents.

* 2. Retention Label Policies (Policy1) Supported

Retention label policies define how and where retention labels are applied, including automatically using trainable classifiers.

* 3. Data Loss Prevention (DLP) Policies (DLP1) Supported

Trainable classifiers can be used in DLP policies to detect and protect sensitive content automatically.

NEW QUESTION 27

- (Topic 2)

You have a data loss prevention (DLP) policy configured for endpoints as shown in the following exhibit.

Create rule

Use actions to protect content when the conditions are met.

Audit or restrict activities on devices

When specified activities are detected on devices for files containing the sensitive info you're protecting, you can choose to only audit the activity, block it entirely, or block it but allow users to override the restriction.
[Learn more restricting device activity](#)

Service domain and browser activities
 Detects when protected files are blocked or allowed to be uploaded to cloud service domains based on the 'Allow/Block cloud service domains' list in endpoint DLP settings.

Upload to a restricted cloud service domain or access from an unallowed browsers Block

File activities for all apps
 Decide whether to apply restrictions for file related activity. Unless you choose different restrictions for restricted apps or app groups below, any restrictions you choose here will be enforced for all apps.

Don't restrict file activity

Apply restrictions to specific activity
 When the activities below are detected on devices for supported files containing sensitive info that matches this policy's conditions, you can choose to audit the activity, block it entirely, or block it but allow users to override the restriction

| | | |
|---|---|------------|
| <input checked="" type="checkbox"/> Copy to clipboard | i | Audit only |
| <input checked="" type="checkbox"/> Copy to a USB removable media | i | Audit only |
| <input checked="" type="checkbox"/> Copy to a network share | i | Audit only |
| <input checked="" type="checkbox"/> Print | i | Audit only |

Save
Cancel

From a computer named Computer1, a user can sometimes upload files to cloud services and sometimes cannot. Other users experience the same issue. What are two possible causes of the issue? Each correct answer presents a complete solution.
 NOTE: Each correct selection is worth one point.

- A. The unallowed browsers in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings are NOT configured.
- B. There are file path exclusions in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings.
- C. The Access by restricted apps action is set to Audit only.
- D. The Copy to clipboard action is set to Audit only.
- E. The computers are NOT onboarded to Microsoft Purview.

Answer: AB

Explanation:

The issue where users sometimes can upload files to cloud services and sometimes cannot suggests inconsistent enforcement of Endpoint DLP policies. This can be caused by the unallowed browsers in the Microsoft 365 Endpoint DLP settings are NOT configured. Also, there are file path exclusions in the Microsoft 365 Endpoint DLP settings.

Endpoint DLP can block uploads only when using unallowed browsers. If unallowed browsers are not configured, users might be able to bypass restrictions by switching to a different browser. This could explain why uploads sometimes work and sometimes don't, depending on which browser is used.

File path exclusions allow certain files or folders to be exempt from DLP restrictions. If a specific file location is excluded, files stored there won't trigger DLP policies, leading to inconsistent behavior. This could result in some uploads being blocked while others are allowed.

NEW QUESTION 30

- (Topic 2)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.

You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.

Solution: You create a data loss prevention (DLP) policy that has only the Exchange email location selected.
 Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.
 A DLP policy with Exchange email as the only location meets this requirement because it identifies sensitive data in email messages and it applies protection actions, such as encryption, blocking, or alerts.

NEW QUESTION 33

- (Topic 2)

You have Microsoft 365 E5 subscription.

You create two alert policies named Policy1 and Policy2 that will be triggered at the times shown in the following table.

| Policy | Time (hh:mm:ss) |
|---------|-----------------|
| Policy1 | 10:00:00 |
| Policy2 | 10:00:03 |
| Policy1 | 10:00:04 |
| Policy2 | 10:00:31 |
| Policy1 | 10:01:01 |
| Policy1 | 10:04:45 |

How many alerts will be added to the Microsoft Purview portal?

- A. 2
- B. 3
- C. 4
- D. 5
- E. 6

Answer: D

Explanation:

In Microsoft Purview, when multiple alert policies trigger alerts, duplicate alerts within a short period (typically 5 minutes) may be suppressed to avoid redundancy.
 Step-by-step Analysis:

| Policy | Time Triggered (hh:mm:ss) | New Alert? |
|---------|---------------------------|-----------------------------|
| Policy1 | 10:00:00 | Yes |
| Policy2 | 10:00:03 | Yes |
| Policy1 | 10:00:04 | No (Duplicate within 5 min) |
| Policy2 | 10:00:31 | No (Duplicate within 5 min) |
| Policy1 | 10:01:01 | Yes |
| Policy1 | 10:04:45 | Yes |

Policy1 at 10:00:04 is ignored because Policy1 already triggered at 10:00:00, and it's within 5 minutes.
 Policy2 at 10:00:31 is ignored because Policy2 already triggered at 10:00:03, and it's within 5 minutes.
 Policy1 at 10:01:01 is a new alert because it's over 1 minute after the previous Policy1 alert.
 Policy1 at 10:04:45 is a new alert because it's over 3 minutes after the previous Policy1 alert.

NEW QUESTION 37

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to enable support for sensitivity labels in Microsoft SharePoint Online. What should you use?

- A. the Microsoft Purview portal
- B. the Microsoft Entra admin center
- C. the SharePoint admin center
- D. the Microsoft 365 admin center

Answer: C

Explanation:

To enable support for sensitivity labels in Microsoft SharePoint Online, you must configure the setting in the SharePoint admin center.

Sensitivity labels in SharePoint Online allow labeling and protection of files stored in SharePoint and OneDrive. This feature must be enabled in the SharePoint admin center Settings Information protection to allow sensitivity labels to apply encryption and protection to stored documents.

NEW QUESTION 40

- (Topic 2)

You have Microsoft 365 E5 subscription that uses data loss prevention (DLP) to protect sensitive information.

You have a document named Form.docx.

You plan to use PowerShell to create a document fingerprint based on Form.docx. You need to first connect to the subscription.

Which cmdlet should you run?

- A. Connect-IPPSSession
- B. Connect-SPOService
- C. Connect-ExchangeOnline
- D. Connect-MgGraph

Answer: A

Explanation:

To create a document fingerprint in Microsoft 365 Data Loss Prevention (DLP), you need to use PowerShell for Microsoft Purview. The correct cmdlet to connect to the Microsoft 365 Security & Compliance Center (where DLP policies are managed) is Connect- IPPSSession. This cmdlet establishes a PowerShell session to manage DLP policies, compliance settings, and document fingerprinting.

NEW QUESTION 41

- (Topic 2)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.

You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers. Tailspin_scanner.exe is installed locally on the computers.

You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.

Solution: From the Microsoft Defender for Cloud Apps, you mark the application as Unsanctioned.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Marking Tailspin_scanner.exe as "Unsanctioned" in Microsoft Defender for Cloud Apps only blocks its usage in cloud-based activities (such as accessing SharePoint, OneDrive, or Exchange Online). However, it does not prevent a locally installed application on Windows 11 devices from accessing sensitive files.

To block Tailspin_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin_scanner.exe to the Restricted Apps list.

Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for non-sensitive content.

NEW QUESTION 42

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 tenant that contains a sensitivity label named label1. You plan to enable co-authoring for encrypted files.

You need to ensure that files that have label1 applied support co-authoring.

Which two settings should you modify? To answer, select the settings in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. [Learn more about access control settings](#)

- Remove access control settings if already applied to items
- Configure access control settings

i Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. [Learn more about this setting](#)

[Go to co-authoring setting](#)

Assign permissions now or let users decide?

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires *i*

Access expires this many days after the label is applied

Allow offline access *i*

Assign permissions to specific users and groups * *i*

0 items

Users and groups

Permissions

Edit

Delete

No data available

Use dynamic watermarking *i*

Customize text (optional)

Use Double Key Encryption *i*

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

C:\Users\Waqas Shahid\Desktop\Mudassir\Untitled.jpg

NEW QUESTION 45

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview insider risk management. You implement the HR data connector.

You need to prepare the data that will be imported by the data connector. In which format should you prepare the data?

- A. JSON
- B. CSV
- C. TSV
- D. XML
- E. PRN

Answer: B

Explanation:

When implementing Microsoft Purview Insider Risk Management and using the HR data connector, you must prepare HR data in CSV (Comma-Separated Values) format. This format is required because Microsoft Purview supports CSV files for importing user employment details, termination dates, role changes, and other HR-related attributes.

NEW QUESTION 49

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

| Name | Type |
|--------|---------------|
| Group1 | Microsoft 365 |
| Group2 | Security |

The subscription contains the resources shown in the following table.

| Name | Type |
|-------|----------------------------------|
| Site1 | Microsoft SharePoint Online site |
| Team1 | Microsoft Teams team |

You create a sensitivity label named Label1.

You need to publish Label1 and have the label apply automatically.

To what can you publish Label1, and to what can Label1 be auto-applied? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Publish to:

▼

- Site1 only
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- Group1, Group2, Site1, and Team1

Auto-apply to:

▼

- Site1 only
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- Group1, Group2, Site1, and Team1

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Publishing a Sensitivity Label

Sensitivity labels can be published to Microsoft 365 groups, security groups, SharePoint Online sites, and Microsoft Teams. Since we have: Group1 (Microsoft 365 group) - Supported Group2 (Security group) - Supported Site1 (SharePoint Online site) - Supported Team1 (Microsoft Teams team) - Supported

This means we can publish Label1 to Group1, Group2, Site1, and Team1. Box 2: Auto-Applying a Sensitivity Label

Auto-apply policies for sensitivity labels work on: SharePoint Online sites (documents)

OneDrive (documents) Exchange email (messages)

However, labels cannot be auto-applied to Microsoft 365 groups or Teams directly because labels are applied to files and emails, not to groups or Teams as entities. Since Site1 (a SharePoint Online site) supports auto-apply, it is the correct option.

NEW QUESTION 51

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SC-401 Practice Exam Features:

- * SC-401 Questions and Answers Updated Frequently
- * SC-401 Practice Questions Verified by Expert Senior Certified Staff
- * SC-401 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SC-401 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SC-401 Practice Test Here](#)