

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	Answer Area
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.	

- 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 2)

You have a Microsoft 365 E5 subscription.

You need to implement a compliance solution that meets the following requirements:

Captures clips of key security-related user activities, such as the exfiltration of sensitive company data.

Integrates data loss prevention (DLP) capabilities with insider risk management.

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

NOTE: Each correct selection is worth one point.

Answer Area

Captures clips of key security-related user activities:

☐ Adaptive scopes
 ☐ Classifiers
 ☐ Forensic evidence
 ☐ Search

Integrates DLP capabilities with insider risk management:

☐ Adaptive Protection
 ☐ eDiscovery (Premium)
 ☐ Records management
 ☐ Trainable classifiers

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Captures clips of key security-related user activities:

☐ Adaptive scopes
 ☐ Classifiers
 ☒ Forensic evidence
 ☐ Search

Integrates DLP capabilities with insider risk management:

☒ Adaptive Protection
 ☒ eDiscovery (Premium)
 ☐ Records management
 ☐ Trainable classifiers

NEW QUESTION 3

- (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 Microsoft Defender for Cloud Apps, you create an app discovery policy. Does this meet the goal?

- A. Yes
 B. No

Answer: B

Explanation:

Creating an app discovery policy in Microsoft Defender for Cloud Apps is used for detecting and monitoring cloud application usage, but it does not prevent a

locally installed application (Tailspin_scanner.exe) from accessing sensitive files on Windows 11 devices.
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 4

- (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 5

HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription that uses Microsoft Purview and just-in-time (JIT) protection. The subscription contains the users shown in the following table.

Name	JIT protection scope
User1	Included
User2	Not configured
User3	Included

The subscription contains the devices shown in the following table.

Name	Microsoft Defender
Device1	Onboarded
Device2	Onboarded
Device3	Not onboarded

The devices contain the files shown in the following table.

Name	File classification evaluation status	Location
File1.docx	Not evaluated	Device1
File2.pdf	Evaluated	Device2
File3.xlsx	Not evaluated	Device3

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 User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.

Yes

☒

No

☐

If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.

☐☐

If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.

☐☐

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statement 1 - No. User1 is included in JIT protection. File1.docx is on Device1, which is onboarded to Microsoft Defender. However, File1.docx has not been evaluated for file classification, meaning JIT cannot enforce protection on it. If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.

Statement 2 - No. User2 is not configured for JIT protection (JIT does not apply to them). File2.pdf has been evaluated for classification, but since User2 is not included in JIT protection, no blocking occurs. If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.

Statement 3 - No. User3 is included in JIT protection. However, Device3 is not onboarded to Microsoft Defender, meaning JIT protection cannot enforce actions on it. File3.xlsx has not been evaluated, so even if the device were onboarded, JIT would not have classification data to act upon.

NEW QUESTION 6

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains two Microsoft 365 groups named Group1 and Group2. Both groups use the following resources:
 A group mailbox
 Microsoft Teams channel messages
 A Microsoft SharePoint Online teams site
 You create the objects shown in the following table.

Name	Type	Description
RLabel1	Retention label	<i>None</i>
AutoApply1	Auto-labeling policy	Applies RLabel1 to Group1
Retention1	Retention policy	Applied to Group2

To which resources will AutoApply1 and Retention1 be applied? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Answer Area

AutoApply1:

The group mailbox only

The SharePoint Online teams site only

The group mailbox and SharePoint Online teams site only

The group mailbox and Teams channel messages only

The group mailbox, SharePoint Online teams site, and Teams channel messages

Retention1:

The group mailbox only

The SharePoint Online teams site only

The group mailbox and SharePoint Online teams site only

The group mailbox and Teams channel messages only

The group mailbox, SharePoint Online teams site, and Teams channel messages

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

AutoApply1 is an auto-labeling policy that applies RLabel1 to Group1. Auto-labeling policies can apply retention labels across group mailboxes, SharePoint Online sites, and Teams channel messages if they are configured for group resources.

Retention1 is a retention policy applied to Group2. Retention policies for Microsoft 365 groups apply to all group resources, including group mailboxes, SharePoint Online teams sites, and Teams channel messages.

Since both AutoApply1 and Retention1 affect entire groups, they apply to all associated resources: group mailbox, SharePoint Online teams site, and Teams channel messages.

NEW QUESTION 7

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains a retention policy named RP1 as shown in the following table.

Setting	Value
Location	- Exchange email (All recipients) - SharePoint sites (All sites)
Retain items for a specific period	5 years (When items were created)
At the end of the retention period	Delete items automatically

You place a preservation lock on RP1. You need to modify RP1.
 Which two modifications can you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add locations to the policy.
- B. Delete the policy.
- C. Remove locations from the policy.
- D. Decrease the retention period of the policy.
- E. Disable the policy.
- F. Increase the retention period of the policy.

Answer: AF

Explanation:

A Preservation Lock in Microsoft Purview Retention Policies enforces strict compliance and prevents certain modifications to ensure data is retained according to compliance requirements.

When a Preservation Lock is applied:

- * 1. You cannot disable or delete the policy.
- * 2. You cannot remove locations from the policy.
- * 3. You cannot decrease the retention period.
- * 4. You can add locations to the policy.
- * 5. You can increase the retention period.

You can expand the retention policy to cover additional locations (e.g., more Exchange mailboxes, SharePoint sites). You can extend the retention duration (e.g., increase from 5 years to 10 years) since this aligns with stricter compliance.

NEW QUESTION 8

HOTSPOT - (Topic 2)

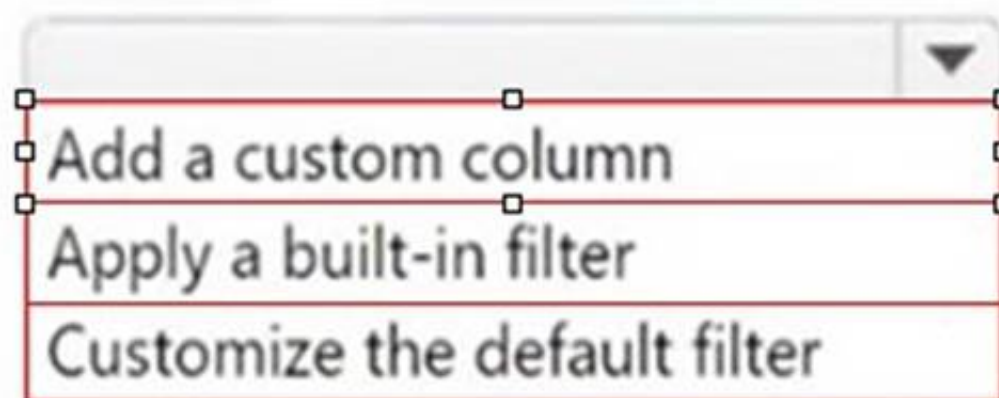
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.

You plan to export DLP activity by using Activity explorer.

The exported file needs to display the sensitive info type detected for each DLP rule match. What should you do in Activity explorer before exporting the data, and in which file format is the file exported? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

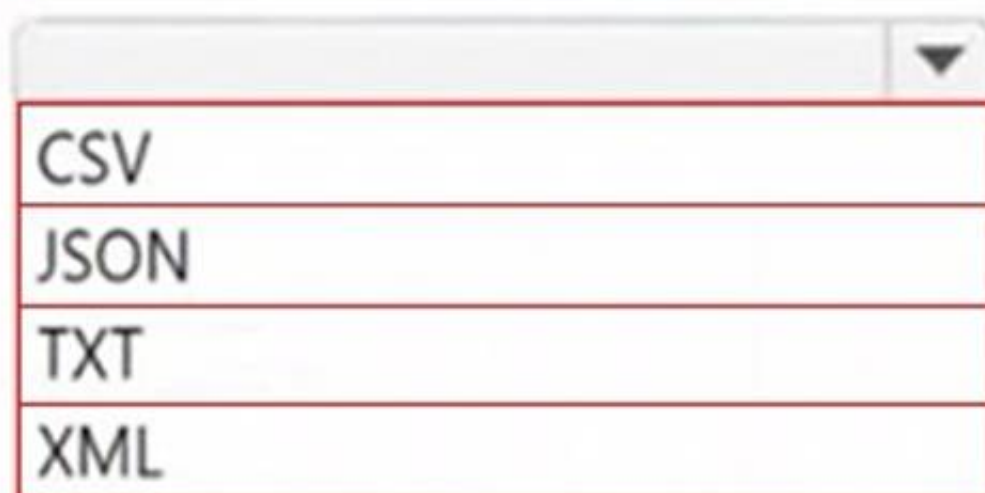
Answer Area

In Activity explorer:



☒ Add a custom column
☒ Apply a built-in filter
☐ Customize the default filter

File type:



CSV
JSON
TXT
XML

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: To include the sensitive info type detected for each DLP rule match, you need to add a custom column in Activity Explorer. This ensures that the exported file contains specific details about the detected sensitive information types.

Box 2: DLP activity exports from Activity Explorer are always in CSV (Comma-Separated Values) format. This format allows for easy data analysis and reporting in Excel or other data-processing tools.

NEW QUESTION 9

- (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 10

- (Topic 2)
You have a Microsoft 365 E5 subscription that contains a Microsoft Teams channel named Channel1. Channel1 contains research and development documents. You plan to implement Microsoft 365 Copilot for the subscription. You need to prevent the contents of files stored in Channel1 from being included in answers generated by Copilot and shown to unauthorized users. What should you use?

- A. data loss prevention (DLP)
- B. Microsoft Purview insider risk management
- C. Microsoft Purview Information Barriers
- D. sensitivity labels

Answer: D

Explanation:

To prevent the contents of files stored in Channel1 from being included in Microsoft 365 Copilot responses and ensure unauthorized users cannot access them, you should use Microsoft Purview Sensitivity Labels. Sensitivity labels allow you to classify, protect, and restrict access to sensitive files. You can configure label-based encryption and access control policies to ensure that only authorized users can access or interact with the files in Channel1. Microsoft 365 Copilot respects sensitivity labels, meaning if a file is labeled with restricted permissions, Copilot will not use it in generated responses for unauthorized users.

NEW QUESTION 10

- (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 12

- (Topic 2)
You have a Microsoft SharePoint Online site named Site1 that contains a document library. The library contains more than 1,000 documents. Some of the documents are job applicant resumes. All the documents are in the English language. You plan to apply a sensitivity label automatically to any document identified as a resume. Only documents that contain work experience, education, and accomplishments must be labeled automatically. You need to identify and categorize the resumes. The solution must minimize administrative effort. What should you include in the solution?

- A. a trainable classifier
- B. a keyword dictionary
- C. a function
- D. an exact data match (EDM) classifier

Answer: A

Explanation:

Since you need to automatically apply a sensitivity label to resumes based on their content and structure (work experience, education, accomplishments), a trainable classifier is the best choice.

Trainable classifiers use machine learning to identify unstructured data, such as resumes, contracts, or legal documents. Instead of relying on predefined patterns (like keywords or regular expressions), a trainable classifier learns from sample documents and can accurately identify resumes even if they are formatted differently.

Final Approach:

Train a trainable classifier using sample resumes. Deploy the classifier in Microsoft Purview.

Configure a sensitivity label to be automatically applied when a document matches the classifier.

NEW QUESTION 14

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days.

What should you configure first?

- A. a custom branding template
- B. a mail flow rule
- C. a sensitivity label
- D. a Conditional Access policy

Answer: C

Explanation:

To ensure that encrypted email messages sent to external recipients can be revoked or expire within seven days, you need to configure a sensitivity label with encryption settings in Microsoft Purview Information Protection. A sensitivity label allows you to encrypt emails and documents, set expiration policies (e.g., emails expire after 7 days), and enable email revocation

How to configure it?

Go to Microsoft Purview compliance portal Information Protection Create a sensitivity label

Enable encryption and configure the content expiration policy Publish the label to users

NEW QUESTION 16

- (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 21

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

 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?

Assign permissions now

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

User access to content expires 

A number of days after label is applied

Access expires this many days after the label is applied

90

Allow offline access 

Always

Assign permissions to specific users and groups * 

[Assign permissions](#)

0 items

Users and groups

Permissions

Edit

Delete

No data available

☒ Use dynamic watermarking 

 Customize text (optional)

☒ Use Double Key Encryption 

<https://sts.contoso.com>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 24

- (Topic 2)

You need to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company. What should you do?

- A. From the Microsoft Purview portal create an insider risk policy
- B. From the Microsoft Defender portal create a file policy
- C. From the Microsoft Defender portal, create an activity policy.
- D. From the Microsoft Purview portal, start a data investigation.

Answer: B

Explanation:

An activity policy in Microsoft Defender for Cloud Apps (Microsoft Defender portal) allows you to track and alert on specific user actions, such as sharing sensitive documents externally from OneDrive. This policy can detect file-sharing activities and send alerts when files are shared with external users, which meets the requirement.

NEW QUESTION 29

.....

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 First Try
- * SC-401 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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