

Microsoft

Exam Questions SC-401

Administering Information Security in Microsoft 365



NEW QUESTION 1

- (Topic 1)

You need to meet the technical requirements for the creation of the sensitivity labels. To which user or users must you assign the Sensitivity Label Administrator role?

- A. Admin1 only
- B. Admin1 and Admin4 only
- C. Admin1 and Admin5 only
- D. Admin1, Admin2, and Admin3 only
- E. Admin1, Admin2, Admin4, and Admin5 only

Answer: D

Explanation:

To meet the requirement that all administrative users must be able to create Microsoft 365 sensitivity labels, we need to assign the Sensitivity Label Administrator role to the correct users.

Sensitivity Label Administrator Role Responsibilities

This role allows users to:

Create and manage sensitivity labels in Microsoft Purview. Publish and configure auto-labeling policies.

Modify label encryption and content marking settings.

Review of Admin Roles from the Table:

Admin	Role Assigned	Can Create Sensitivity Labels?
Admin1	Global Reader	<input type="checkbox"/> No, read-only permissions.
Admin2	Compliance Data Administrator	<input type="checkbox"/> Yes, can manage compliance data, including labels.
Admin3	Compliance Administrator	<input type="checkbox"/> Yes, has full compliance management, including labels.
Admin4	Security Operator	<input type="checkbox"/> No, this role is focused on security alerts and response.
Admin5	Security Administrator	<input type="checkbox"/> No, primarily focused on security policies and threat management.

Users that must be assigned the Sensitivity Label Administrator role: Admin2 (Compliance Data Administrator)
 Admin3 (Compliance Administrator)
 Admin1 (Global Reader) (should be assigned this role to fulfill the requirement that all admins can create labels).

NEW QUESTION 2

HOTSPOT - (Topic 1)

How many files in Site2 can User1 and User2 access after you turn on DLPpolicy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Number of files that User1 can access:

Number of files that User2 can access:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Understanding DLP Policy Impact on File Access

The DLP policy (DLPpolicy1) applies to Site2 and restricts access when: Content contains SWIFT Codes.

Instance count is 2 or more.

File Analysis (Based on SWIFT Codes Count)

File Name	SWIFT Codes Count	DLP Policy Restricts Access?
File1.docx	1	<input type="checkbox"/> No restriction (SWIFT codes < 2)
File2.bmp	4	<input type="checkbox"/> Restricted (SWIFT codes ≥ 2)
File3.txt	3	<input type="checkbox"/> Restricted (SWIFT codes ≥ 2)
File4.xlsx	7	<input type="checkbox"/> Restricted (SWIFT codes ≥ 2)

Files that remain accessible (not restricted by DLP):

File1.docx (Contains only 1 SWIFT Code Below restriction threshold) User access after DLP policy is applied:

User	Role in Site2	Access Rights	Can Access Files?
User1	Site Owner	Full Access	File1.docx, plus override access to another file
User2	Site Visitor	Read-only	File1.docx only

User1 (Site Owner):

Has higher privileges and can override DLP restrictions (through admin intervention). Can access 2 files (File1.docx + override access to another file).

User2 (Site Visitor):

Has read-only access but DLP blocks access to restricted files. Can only access 1 file (File1.docx), since all others are restricted.

NEW QUESTION 3

- (Topic 2)

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

Name	Type
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	macOS

You plan to start using Microsoft 365 Endpoint data loss protection (Endpoint DLP). Which devices support Endpoint DLP?

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

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.

From the provided table:

Device1 (Windows 11) - Supported Device2 (Windows 10) - Supported Device3 (iOS) - Not supported Device4 (macOS) - Not supported

Thus, only Device1 and Device2 support Endpoint DLP.

NEW QUESTION 4

HOTSPOT - (Topic 2)

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

Name	Platform
Config1	Windows 11
Config2	macOS
Config3	Android

Each configuration uses either Google Chrome or Firefox as a default browser.

You need to implement Microsoft Purview and deploy the Microsoft Purview browser extension to the configurations.

To which configuration can each extension be deployed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Google Chrome:

▼

Config1 only

Config2 only

Config1 and Config2 only

Config2 and Config3 only

Config1, Config2, and Config3

Firefox:

▼

Config1 only

Config2 only

Config1 and Config2 only

Config2 and Config3 only

Config1, Config2, and Config3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Microsoft Purview browser extensions for Endpoint DLP are supported on: Windows 10/11 (Config1)
 macOS (Config2)
 Not supported on Android (Config3)
 Since Microsoft Purview does not support browser extensions on Android, Config3 is excluded from both Google Chrome and Firefox.

NEW QUESTION 5

HOTSPOT - (Topic 2)

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

Name	Role group
Admin1	Insider Risk Management Admins
Admin2	Insider Risk Management Analysts
Admin3	Risk Management Investigators
Admin4	Insider Risk Management Auditors

You plan to create a Microsoft Purview insider risk management case named Case1. Which insider risk management object should you select first, and which users will be added as contributors for Case1 by default?

To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Object:

An alert

A policy

A risky user

A notice template

Forensic evidence

Users:

Admin1 and Admin2 only

Admin2 and Admin3 only

Admin3 and Admin4 only

Admin2, Admin3, and Admin4 only

Admin1, Admin2, Admin3, and Admin4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: When creating a Microsoft Purview Insider Risk Management case, you must first select a risky user to investigate. The case will be built around this specific user's activities, linking alerts and risk signals to the investigation.

Box 2: The Insider Risk Management role groups determine who can access and contribute to cases:

Admin1 (Insider Risk Management Admins) Full admin access.

Admin2 (Insider Risk Management Analysts) Analysts who review cases. Admin3 (Risk Management Investigators) Investigators who work on cases. Admin4 (Insider Risk Management Auditors) Auditors who oversee cases.

All these roles have default access to insider risk cases in Microsoft Purview, so all four admins are added as contributors.

NEW QUESTION 6

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains three DOCX files named File1, File2, and File3.

You create the sensitivity labels shown in the following table.

Name	Permission	Apply content marking
Label1	Any authenticated users: Viewer	Disabled
Label2	None	Enabled

You apply the labels to the files as shown in the following table.

File	Label
File1	None
File2	Label1
File3	Label2

You ask Microsoft 365 Copilot to summarize the files, and you receive the results shown in the following table.

Name	Based on content of
Summary1	File1, File3
Summary2	File2
Summary3	File1, File2, File3

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

	Yes	No
Summary1 has a sensitivity label applied.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Summary2 has a sensitivity label applied.	<input type="checkbox"/>	<input type="checkbox"/>
Summary3 has a sensitivity label applied.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements

	Yes	No
Summary1 has a sensitivity label applied.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Summary2 has a sensitivity label applied.	<input type="checkbox"/>	<input type="checkbox"/>
Summary3 has a sensitivity label applied.	<input type="checkbox"/>	<input type="checkbox"/>

NEW QUESTION 7

- (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 8

- (Topic 2)

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

Name	Description
User1	<ul style="list-style-type: none"> • User 1 is a regional manager. • User1 is assigned the Reader role. • Three department managers report to User1.
User2	<ul style="list-style-type: none"> • User2 is the human resources (HR) department manager. • User2 has no Microsoft Entra roles assigned. • Five HR department users report to User2.
User3	<ul style="list-style-type: none"> • User3 is a developer. • User3 reports to User2. • User3 is the only user in the compliance department. • User3 is assigned the Compliance Administrator role.
User4	<ul style="list-style-type: none"> • User4 is the assistant of User1. • User4 has no Microsoft Entra roles assigned. • User4 handles a high volume of confidential data on behalf of User1.

Which users will Microsoft Purview insider risk management flag as potential high-impact users?

- A. User1 and User2 only
- B. User2 and User3 only
- C. User1, User2, and User3 only
- D. User1, User2, User3, and User4

Answer: D

Explanation:

Microsoft Purview Insider Risk Management flags high-impact users based on various risk factors, including role, access to confidential data, and influence within an organization. Let's analyze each user:

User1 (Regional Manager, assigned Reader role, manages department managers) Risk Factors:
 Holds a managerial position (regional manager).
 Manages multiple department managers, indicating organizational influence. Access to critical business information.
 Flagged? -Yes (Managerial role and access to confidential data).

User2 (HR department manager, no Microsoft Entra roles, manages HR department users) Risk Factors:
 Manages HR department users, meaning they likely handle sensitive employee data. HR roles are often considered high-risk due to access to personal and payroll data.
 Flagged? -Yes (HR role and access to sensitive employee data).

User3 (Developer, reports to User2, only user in compliance, assigned Compliance Administrator role)
 Risk Factors:
 Compliance Administrator role grants access to sensitive security and regulatory data. Only person in the compliance department, meaning they hold a critical role. Potentially high impact on compliance and security settings.
 Flagged? -Yes (Privileged Compliance Administrator role).

User4 (Assistant to User1, no Entra roles, handles confidential data on behalf of User1)
 Risk Factors:
 Handles a high volume of confidential data on behalf of a regional manager. Assistants with access to sensitive data are considered insider risk candidates.
 Flagged? -Yes (High access to sensitive information).

Since all four users fit high-impact criteria (managerial roles, privileged compliance access, handling sensitive data), Microsoft Purview Insider Risk Management will flag all of them.

NEW QUESTION 9

- (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 10

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.

Yes No

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

Yes No

- 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 10

- (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 11

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 15

- (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 19

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	None
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 24

HOTSPOT - (Topic 2)

You have a Microsoft 365 sensitivity label that is published to all the users in your Microsoft Entra tenant as shown in the following exhibit.

Label name Rebranding	Edit
Tooltip Used for all documents containing information about the rebranding effort	Edit
Description	Edit
Encryption Advanced protection for content with this label	Edit
Content marking Watermark: INTERNAL	Edit
Endpoint data loss prevention	Edit
Auto labeling	Edit

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

Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	<input type="radio"/>	<input type="radio"/>
The sensitivity label can be applied only to documents that contain the word rebranding.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statement 1 - No. The sensitivity label includes content marking (watermark: INTERNAL), but it only applies to documents where the label is manually or automatically applied, not to all documents by default.
 Statement 2 - No. The sensitivity label only specifies a watermark, not a header. If a header marking was configured, it would explicitly appear in the label settings.
 Statement 3 - No. There is no indication that auto-labeling is configured to apply the label only to documents with the word "rebranding". Auto-labeling is an optional setting that needs explicit configuration.

NEW QUESTION 29

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to identify documents that contain patent application numbers containing the letters PA followed by eight digits, for example, PA 12345678. The solution must minimize administrative effort.

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

Answer Area

To identify the documents, use a data classification of:

Exact data match (EDM)

Sensitive info type

Trainable classifier

Configure data classifications by using a:

Keyword dictionary

Regular expression

Function

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Since you are looking for a specific pattern (PA followed by eight digits, e.g., PA 12345678), the best classification method is Sensitive Info Type. Sensitive Info Types allow pattern-based matching to identify structured data. Exact Data Match (EDM) is not needed because you're not comparing against a fixed dataset. Trainable classifier is not appropriate because this is a structured pattern, not an unstructured document classification.
 Box 2: Since PA 12345678 follows a structured pattern, the most effective method is Regular Expression (Regex). A Regular Expression (Regex) can be written to match "PA" followed by exactly eight digits (e.g., PA\s\d{8}). Keyword dictionary is not ideal because it works for predefined words, not number patterns. Function is unnecessary because there is no need for checksum validation or predefined validation rules.

NEW QUESTION 30

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 35

DRAG DROP - (Topic 2)

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

You need to create a custom sensitive info type. The solution must meet the following requirements:

Match product serial numbers that contain a 10-character alphanumeric string.

Ensure that the abbreviation of SN appears within six characters of each product serial number.

Exclude a test serial number of 1111111111 from a match.

Which pattern settings should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting 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.

Settings

Additional checks

Character proximity

Confidence level

Primary element

Supporting elements

Answer Area

Match product serial numbers that contain a 10-character alphanumeric string:

Ensure that the abbreviation of SN appears within six characters of each product serial number:

Exclude a test serial number of 1111111111 from a match:

Setting

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Settings	Answer Area	Setting
Additional checks	Match product serial numbers that contain a 10-character alphanumeric string:	Primary element
Character proximity	Ensure that the abbreviation of SN appears within six characters of each product serial number:	Character proximity
Confidence level	Exclude a test serial number of 1111111111 from a match:	Additional checks
Primary element		
Supporting elements		

NEW QUESTION 38

- (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 39

- (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 365 Endpoint data loss prevention (Endpoint DLP) settings, you add a folder path to the file path exclusions.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Adding a folder path to the file path exclusions in Microsoft 365 Endpoint DLP does not prevent Tailspin_scanner.exe from accessing protected sensitive information. Instead, it would exclude those files from DLP protection, which is not the intended outcome.

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 40

- (Topic 2)

You receive an email that contains a list of words that will be used for a sensitive information type.

You need to create a file that can be used as the source of a keyword dictionary. In which format should you save the list?

- A. an XLSX file that contains one word in each cell of the first row
- B. an XML file that contains a keyword tag for each word
- C. an ACCDB database file that contains a table named Dictionary
- D. a text file that has one word on each line

Answer: D

Explanation:

To create a keyword dictionary for a sensitive information type in Microsoft Purview Data Loss Prevention (DLP), you must use a plain text (.txt) file where each keyword is on a separate line.

Format Example (TXT file): confidential sensitive classified top secret

This format is simple, efficient, and directly compatible with Microsoft 365 DLP policies for keyword dictionaries.

How to use the keyword dictionary?

Create a text file with one keyword per line.

Upload it to Microsoft Purview under Data Classification > Sensitive Info Types. Use the dictionary in a DLP policy to identify and protect sensitive information.

NEW QUESTION 41

HOTSPOT - (Topic 2)

You have a Microsoft 365 subscription.

You plan to deploy an audit log retention policy.

You need to perform a search to validate whether the policy will be applied to the intended entries.

Which two fields should you configure for the search? To answer, select the appropriate fields in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Search

[Learn about audit](#)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To validate whether an audit log retention policy will apply to the intended entries, you should configure the following fields:

Date and time range (UTC) ensures that you are searching for audit logs within the time period when the policy should be applied. Audit logs are time-sensitive, and policies affect logs based on their timestamp.

Record types allows you to filter and search for specific audit log categories (e.g., Exchange, SharePoint, Teams, etc.) that are affected by the retention policy.

Selecting the correct record type ensures that the policy is evaluated against the relevant data.

NEW QUESTION 44

- (Topic 2)

You are planning a data loss prevention (DLP) solution that will apply to Windows Client computers.

You need to ensure that when users attempt to copy a file that contains sensitive information to a USB storage device, the following requirements are met:

If the users are members of a group named Group1, the users must be allowed to copy the file, and an event must be recorded in the audit log.

All other users must be blocked from copying the file. What should you create?

- A. one DLP policy that contains one DLP rule
- B. one DLP policy that contains two DLP rules
- C. two DLP policies that each contains one DLP rule

Answer: B

Explanation:

To meet the requirements, you need one DLP policy with two separate DLP rules to handle the different conditions:

- * 1. First DLP Rule (For Group1 Members): If the user is a member of Group1 and attempts to copy a file with sensitive data to a USB storage device. Allow the file copy but log the event in the audit log.
- * 2. Second DLP Rule (For All Other Users): If any user who is NOT in Group1 attempts to copy a file with sensitive data to a USB storage device. Block the file transfer.

NEW QUESTION 47

- (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 49

- (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-AdminAuditLogConfig -AdminAuditLogEnabled \$true -AdminAuditLogCmdlets *Mailbox* command. Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

The Set-AdminAuditLogConfig -AdminAuditLogEnabled \$true -AdminAuditLogCmdlets

Mailbox command is incorrect. This enables admin audit logging, which tracks changes to mailbox configurations (e.g., mailbox settings updates), not user activity inside the mailbox.

NEW QUESTION 54

- (Topic 2)

You have a Microsoft 365 subscription.

You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. From Microsoft Defender for Cloud Apps, create a file policy.
- B. From the SharePoint admin center, modify the Site Settings.
- C. From the SharePoint admin center, modify the records management settings.
- D. From the Microsoft Purview portal, publish a label.
- E. From the Microsoft Purview portal, create a label.

Answer: DE

Explanation:

To allow users to apply retention labels to individual documents in Microsoft SharePoint libraries, you need to create a retention label and publish the label.

In Microsoft Purview, retention labels define how long content should be retained or deleted. You must first create a label that specifies the retention rules. After creating the label, you must publish it so that it becomes available for users in SharePoint document libraries. Once published, users can manually apply the

retention label to individual documents.

NEW QUESTION 59

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription.

You receive the data loss prevention (DLP) alert shown in the following exhibit.

Sensitive info in email with subject 'Message1'

Details Sensitive info types Metadata

Event details

ID: 173fe9ac-3a65-41b0-9914-1db451bba639 Location: Exchange

Time of activity: Jun 6, 2022 8:22 PM

Impacted entities

User: Megan Bowen Email recipients: victoria@fabrikam.com

Email subject: Message1

Policy details

DLP policy matched: Policy1 Rule matched: Rule1
Sensitive info types detected: Credit Card Number (19, 85%) Actions taken: GenerateAlert
User overrode policy: Yes Override justification text: Manager approved
Sensitive info detected in: Document1.docx

Actions |

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 Area

The email was [answer choice].

delivered immediately
quarantined and undelivered
sent to a manager for approval

The sender's manager [answer choice].

approved the email by using a workflow
overrode Rule1
was uninvolved in the override process

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

The email was [answer choice].

delivered immediately
quarantined and undelivered
sent to a manager for approval

The sender's manager [answer choice].

approved the email by using a workflow
overrode Rule1
was uninvolved in the override process

NEW QUESTION 61

- (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 62

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You plan to implement insider risk management for users that manage sensitive data associated with a project.

You need to create a protection policy for the users. The solution must meet the following requirements:

Minimize the impact on users who are NOT part of the project. Minimize administrative effort.

What should you do first?

- A. From the Microsoft Purview portal, create an insider risk management policy.
- B. From the Microsoft Entra admin center, create a security group
- C. From the Microsoft Entra admin center create a User risk policy
- D. From the Microsoft Purview portal create a priority user group

Answer: B

Explanation:

To implement insider risk management for users managing sensitive project data while minimizing the impact on other users and reducing administrative effort, you should first create a security group in Microsoft Entra ID (formerly Azure AD). Security groups allow you to scope insider risk management policies to specific users instead of applying policies to all users, which helps in minimizing unnecessary alerts and reducing administrative overhead. After creating the security group, you can assign this group to a Microsoft Purview Insider Risk Management policy, ensuring that only project-related users are affected.

NEW QUESTION 65

.....

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](#)