

Exam Questions SC-401

Administering Information Security in Microsoft 365

<https://www.2passeasy.com/dumps/SC-401/>



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)

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	Yes	No
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
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.	<input type="checkbox"/>	<input type="checkbox"/>
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.	<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)

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

- (Topic 2)

You have a Microsoft 365 tenant.

You have a database that stores customer details. Each customer has a unique 13-digit identifier that consists of a fixed pattern of numbers and letters.

You need to implement a data loss prevention (DLP) solution that meets the following requirements:

Email messages that contain a single customer identifier can be sent outside your company.

Email messages that contain two or more customer identifiers must be approved by the company's data privacy team.

Which two components should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a sensitivity label
- B. a sensitive information type
- C. a DLP policy
- D. a retention label
- E. a mail flow rule

Answer: BC

Explanation:

You need to define a custom sensitive information type that recognizes the unique 13-digit identifier format for customer records. Microsoft Purview DLP policies use these types to identify and protect sensitive data.

A Data Loss Prevention (DLP) policy is required to enforce the rules. It will allow emails with a single identifier but trigger an approval workflow when two or more identifiers are detected.

NEW QUESTION 5

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 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.

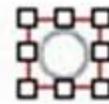
Answer Area

Statements

Summary1 has a sensitivity label applied.

Yes

No



Summary2 has a sensitivity label applied.



Summary3 has a sensitivity label applied.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

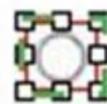
Answer Area

Statements

Summary1 has a sensitivity label applied.

Yes

No



Summary2 has a sensitivity label applied.



Summary3 has a sensitivity label applied.



NEW QUESTION 7

- (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 8

- (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 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-Mailbox -Identity "User1" -AuditEnabled \$true command. Does that meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

To track who accesses User1's mailbox, you need to enable mailbox auditing for User1. By default, Exchange mailbox auditing is not enabled per mailbox (even though it is enabled tenant-wide).

The Set-Mailbox -Identity "User1" -AuditEnabled \$true command enables audit logging for mailbox actions like:

Read emails Delete emails

Send emails as User1 Access by delegated users

Once enabled, you can search for future sign-ins and actions in the Microsoft Purview audit logs.

NEW QUESTION 10

DRAG DROP - (Topic 2)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You plan to deploy a Defender for Cloud Apps file policy that will be triggered when the following conditions are met:

A file is shared externally.

A file is labeled as internal only.

Which filter should you use for each condition? To answer, drag the appropriate filters to the correct conditions. Each filter 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.

Filters

- Access level
- Collaborators
- Matched policy
- Sensitivity label

Answer Area

When a file is shared externally.

When a file is labelled as Internal only.

Filter

-
-

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Filters

- Access level
- Collaborators
- Matched policy
- Sensitivity label

Answer Area

When a file is shared externally.

When a file is labelled as Internal only.

Filter

- Access level
- Sensitivity label

NEW QUESTION 10

- (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 13

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

	Yes	No
If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.	<input type="checkbox"/>	<input type="checkbox"/>
If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.	<input type="checkbox"/>	<input type="checkbox"/>

- 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 17

- (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 18

- (Topic 2)

You are creating a data loss prevention (DLP) policy that will apply to all available locations except Fabric and Power BI workspaces.

You configure an advanced DLP rule in the policy. Which type of condition can you use in the rule?

- A. Sensitive info type
- B. Content search query
- C. Sensitive label
- D. Keywords

Answer: A

Explanation:

When configuring an advanced DLP rule in Microsoft Purview Data Loss Prevention (DLP), you can use a Sensitive Information Type (SIT) condition to detect and classify specific types of sensitive data, such as credit card numbers, Social Security numbers, or custom sensitive data patterns. This allows you to apply protection and trigger actions based on the identified content.

NEW QUESTION 22

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 24

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains a user named User1.

You deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI). You need to ensure that User1 can perform the following actions:

View recommendations from the Recommendations page. View the user risk level for all events by using Activity explorer. The solution must follow the principle of least privilege.

To which role group should you add User1 for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

View the recommendations:

View the user risk level:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: The Insider Risk Management Investigators role allows users to view recommendations related to insider risk cases and Microsoft Purview DSPM for AI insights. This role is appropriate because it grants access to review AI-related risk recommendations without unnecessary administrative privileges.
 Box 2: The Insider Risk Management Analysts role allows users to analyze user risk levels and events using Activity Explorer. This follows the principle of least privilege, ensuring that User1 can only view risk levels and investigate but does not gain full administrative control over insider risk policies.

NEW QUESTION 25

- (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 29

- (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	<ul style="list-style-type: none"> • 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 31

HOTSPOT - (Topic 2)

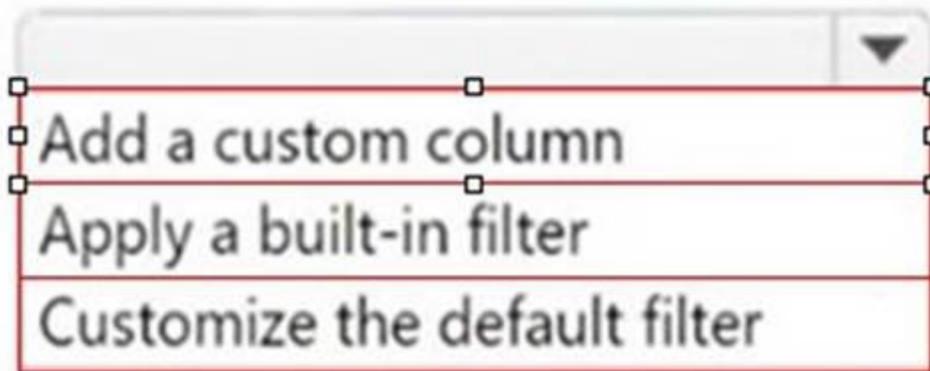
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.

You plan to export DLP activity by using Activity explorer.

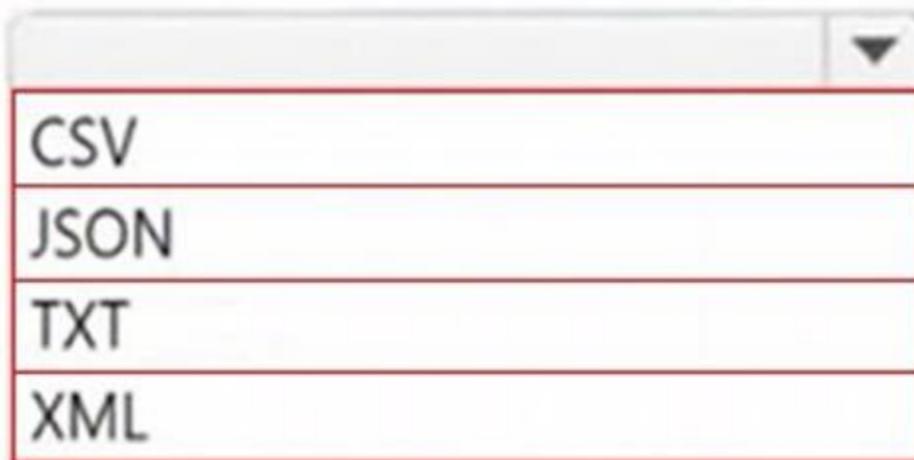
The exported file needs to display the sensitive info type detected for each DLP rule match. What should you do in Activity explorer before exporting the data, and in which file format is the file exported? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is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

Answer Area

In Activity explorer:



File type:



- 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 34

- (Topic 2)

You have a Microsoft 365 E5 subscription that uses Microsoft Purview. You are creating an exact data match (EDM) classifier named EDM1. For EDM1, you upload a schema file that contains the fields shown in the following table.

Column name	Match mode
PP	EU Passport Number
Name	All Full Names
DateOfBirth	Single-token
AccountNumber	Multi-token

What is the maximum number of primary elements that EDM1 can have?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: B

Explanation:

In Microsoft Purview Exact Data Match (EDM) classifiers, a primary element is a unique, identifying field used for data matching. EDM allows up to two primary elements per schema.

From the provided table, the Match mode indicates how data is analyzed: PP (EU Passport Number) Likely a primary element because it's unique.

Name (All Full Names) Typically not a primary element as names are common.

DateOfBirth (Single-token) Usually a secondary element, not unique. AccountNumber (Multi-token) Can be a primary element, as it's a unique identifier.

Since EDM supports a maximum of two primary elements, the correct answer is 2.

NEW QUESTION 37

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You need ensure that an incident will be generated when a user visits a phishing website. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Type of policy to create:

a Communication compliance
a Data loss prevention (DLP)
an Insider risk management

Prerequisite to complete:

Create a sensitive service domain group.
Deploy the Microsoft Defender Browser Protection extension.
Deploy the Microsoft Purview extension.
From Data Loss Prevention, configure the Service domains settings.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Insider Risk Management policies in Microsoft Purview can be configured to detect risky behavior, such as accessing phishing websites. These policies monitor user activity, generate alerts, and help organizations investigate potential security threats.
 Box 2: Microsoft Defender Browser Protection extension helps in detecting unsafe or phishing websites and integrating this detection with Insider Risk Management policies. This extension works with Microsoft Edge and Google Chrome to identify risky browsing activity and trigger alerts.

NEW QUESTION 40

- (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 41

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 44

- (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 48

- (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 53

- (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 55

- (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 configure a mail flow rule that matches a sensitive info type. Does this meet the goal?

- A. Yes
- B. No

Answer: B

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.

Mail flow rules (transport rules) can detect sensitive info, but they are limited in encryption capabilities.

DLP policies provide more advanced protection and integration with Microsoft Purview for sensitive info detection.

NEW QUESTION 60

- (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 64

- (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 69

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 72

- (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. 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 76

HOTSPOT - (Topic 2)

You plan to create a custom sensitive information type that will use Exact Data Match (EDM).

You need to identify what to upload to Microsoft 365, and which tool to use for the upload. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Upload:

▼

Data hashes

Data in the XML format

Digitally signed data

Use:

▼

Azure Storage Explorer

EDM upload agent

Microsoft Purview portal

The Set-DlpKeywordDictionary cmdlet

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

EDM does not store raw data; instead, it requires hashed versions of sensitive data for privacy and security. To upload the hashed data, Microsoft provides the EDM upload agent. This ensures that the data is securely processed and recognized by the EDM service in Microsoft 365.

NEW QUESTION 81

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-401 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-401 Product From:

<https://www.2passeasy.com/dumps/SC-401/>

Money Back Guarantee

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