

Exam Questions SC-401

Administering Information Security in Microsoft 365

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



NEW QUESTION 1

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.

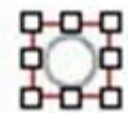
NOTE: Each correct selection is worth one point.

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 2

- (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 3

HOTSPOT - (Topic 2)

You have a new Microsoft 365 E5 tenant.

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

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

Answer Area

Action to perform:

Create an Exact Data Match (EDM) schema.

Import a data loss prevention (DLP) rule package.

Start the opt-in process.

To perform the action, assign the role of:

Compliance Administrator

Global Administrator

Security Administrator

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To create a custom trainable classifier in Microsoft Purview (formerly Microsoft Compliance Center), you must first opt into the trainable classifier feature. Before using custom trainable classifiers, Microsoft requires manual opt-in through the Microsoft Purview compliance portal. Without this step, you cannot create a new classifier.

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

NEW QUESTION 4

- (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 5

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:

Configure data classifications by using a:

- 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 6

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 7

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 8

- (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 9

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 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 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 10

- (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 14

- (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 15

- (Topic 2)

You have Microsoft 365 E5 subscription.

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

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

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

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

Answer: D

Explanation:

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

Step-by-step Analysis:

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

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

NEW QUESTION 20

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 | v

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 24

- (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 28

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 30

.....

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