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 retention requirement for the users' Microsoft 365 data. What is the minimum number of retention policies required to achieve the goal?

A. 1
B. 2
C. 3
D. 4
E. 6

Answer: B

Explanation:
The requirement states that all Microsoft 365 data for users must be retained for at least one year. In Microsoft 365, retention policies must be configured for each type of data storage.
Step 1: Identifying Where Data is Stored
From the case study, users store data in the following locations: SharePoint Online sites
OneDrive accounts Exchange email Exchange public folders Teams chats
Teams channel messages
Since these locations fall under two broad categories: Microsoft Exchange data (Emails, Public folders)
SharePoint, OneDrive, and Teams data
Step 2: Required Retention Policies
* 1. A single retention policy can cover: SharePoint Online
OneDrive Microsoft Teams
* 2. A second retention policy is required for: Exchange (Emails & Public Folders)
Thus, the minimum number of retention policies required to meet the requirement is 2.
Microsoft 365 retention policies can be applied broadly across multiple services with just two policies:
One for Exchange & Public Folders
One for SharePoint, OneDrive, and Teams
There's no need for separate policies for each individual workload unless different retention durations are required, which is not stated in the requirement.

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

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
HOTSPOT - (Topic 1)
You need to meet the technical requirements for the confidential documents.
What should you create first, and what should you use for the detection method? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To detect and protect confidential documents, we need a custom rule to identify project codes that start with 999 (since they are classified as confidential).
Box 1: A Sensitive Info Type (SIT) allows Microsoft Purview DLP policies to recognize structured data (e.g., project codes). DLP policies require a sensitive info type to detect content based on patterns, keywords, or dictionary terms. A sensitivity label alone does not define detection logic—it is used for classification and protection after content is identified.
Box 2: Since project codes follow a structured 10-digit pattern, we should use a Regular Expression (Regex) to match project codes that start with 999.
Example Regex pattern: 999\d{7}
This pattern detects a 10-digit number starting with "999".

NEW QUESTION 4
- (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 5
- (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 6
- (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

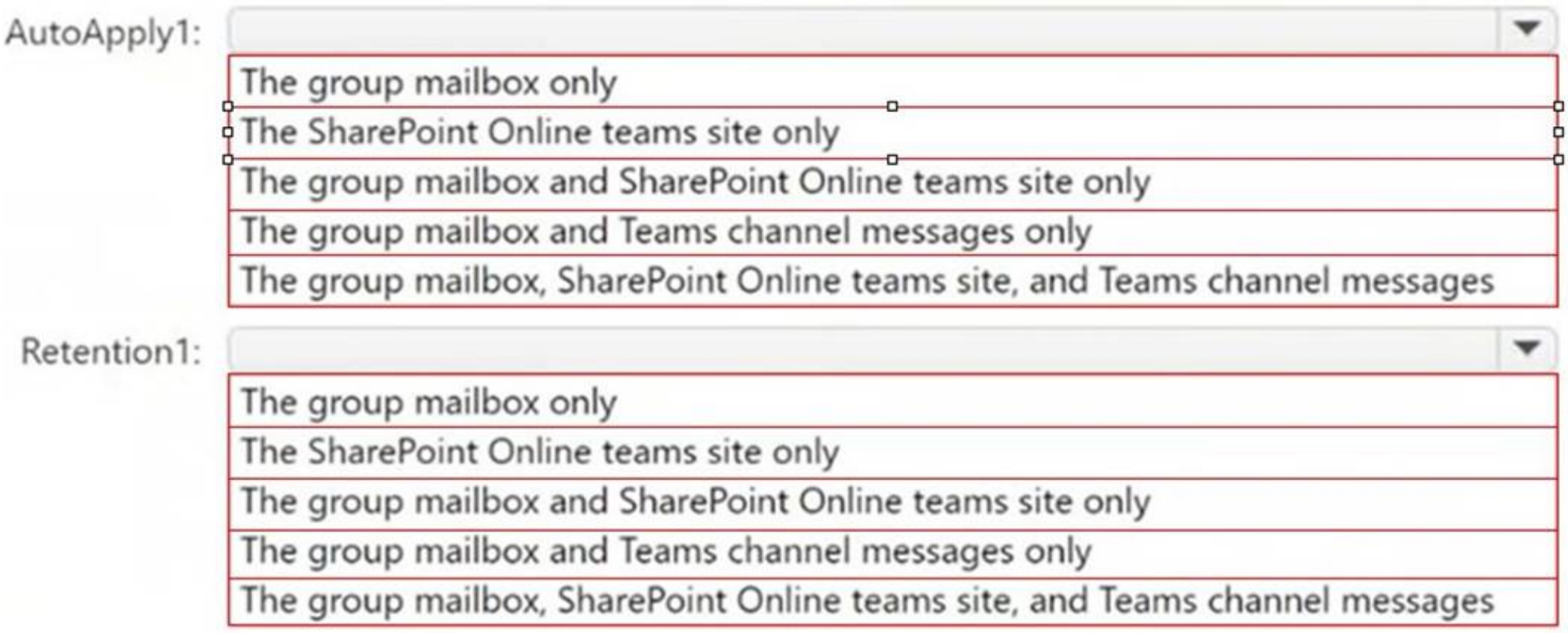
Explanation:
When configuring an advanced DLP rule in Microsoft Purview Data Loss Prevention (DLP), you can use a Sensitive Information Type (SIT) condition to detect and classify specific types of sensitive data, such as credit card numbers, Social Security numbers, or custom sensitive data patterns.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

NEW QUESTION 7
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



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 8
- (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 9
- (Topic 2)
You have a Microsoft 365 subscription. Users have devices that run Windows 11.
You plan to create a Microsoft Purview insider risk management policy that will detect when a user performs the following actions:
Deletes files that contain a sensitive information type (SIT) from their device Copies files that contain a SIT to a USB drive
Prints files that contain a SIT
You need to prepare the environment to support the policy.
What should you do?

A. Configure the physical badging connector.
B. Configure the HR data connector.
C. Create a Microsoft Purview communication compliance policy.
D. Onboard the devices to Microsoft Purview.

Answer: D

Explanation:
To ensure that Microsoft Purview Insider Risk Management can detect file deletions, USB copies, and print actions on sensitive information, you must onboard the Windows 11 devices to Microsoft Purview.

Device onboarding enables endpoint activity monitoring, allowing Purview to track and log user activities such as file deletions, USB transfers, and printing of sensitive files. Once onboarded, the Insider Risk Management policy can analyze these activities and generate risk alerts when sensitive information types (SITs) are involved.

NEW QUESTION 10
- (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

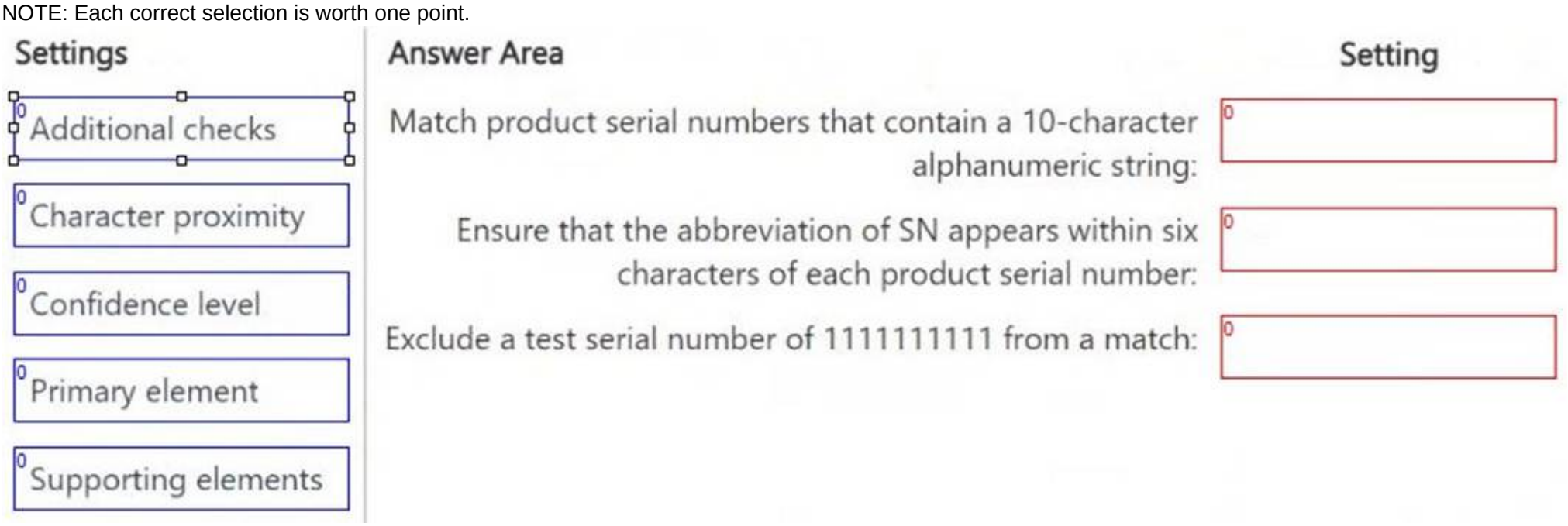
What is the maximum number of primary elements that EDM1 can have?

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.

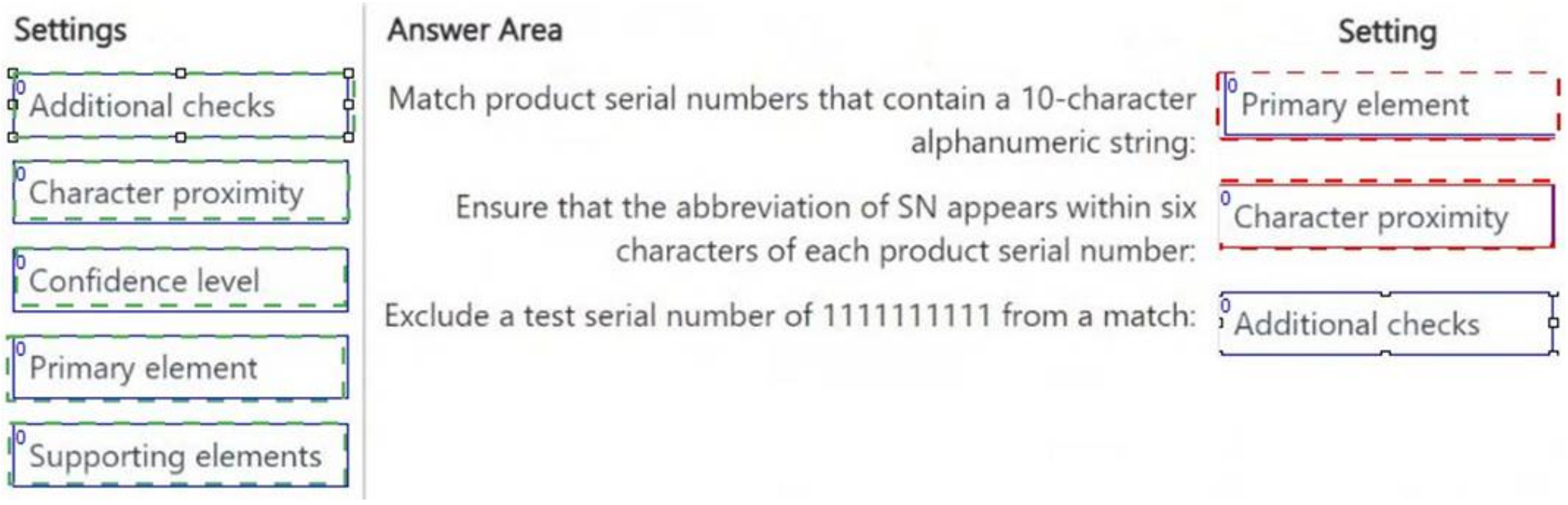
NEW QUESTION 10
DRAG DROP - (Topic 2)
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.
You need to create a custom sensitive info type. The solution must meet the following requirements:
Match product serial numbers that contain a 10-character alphanumeric string.
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 13
- (Topic 2)
You have a Microsoft 365 E5 subscription.
You need to create a sensitivity label named Label1. The solution must ensure that users can use Microsoft 365 Copilot to summarize files that have Label1 applied.
Which permission should you select for Label1?

A. Export content(EXPORT)
B. Copy and extract content(EXTRACT)
C. Edit content(DOCEDIT)
D. View rights(VIEW)

Answer: B

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

NEW QUESTION 17
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription. The subscription contains devices that are onboarded to Microsoft Purview and configured as shown in the following table.

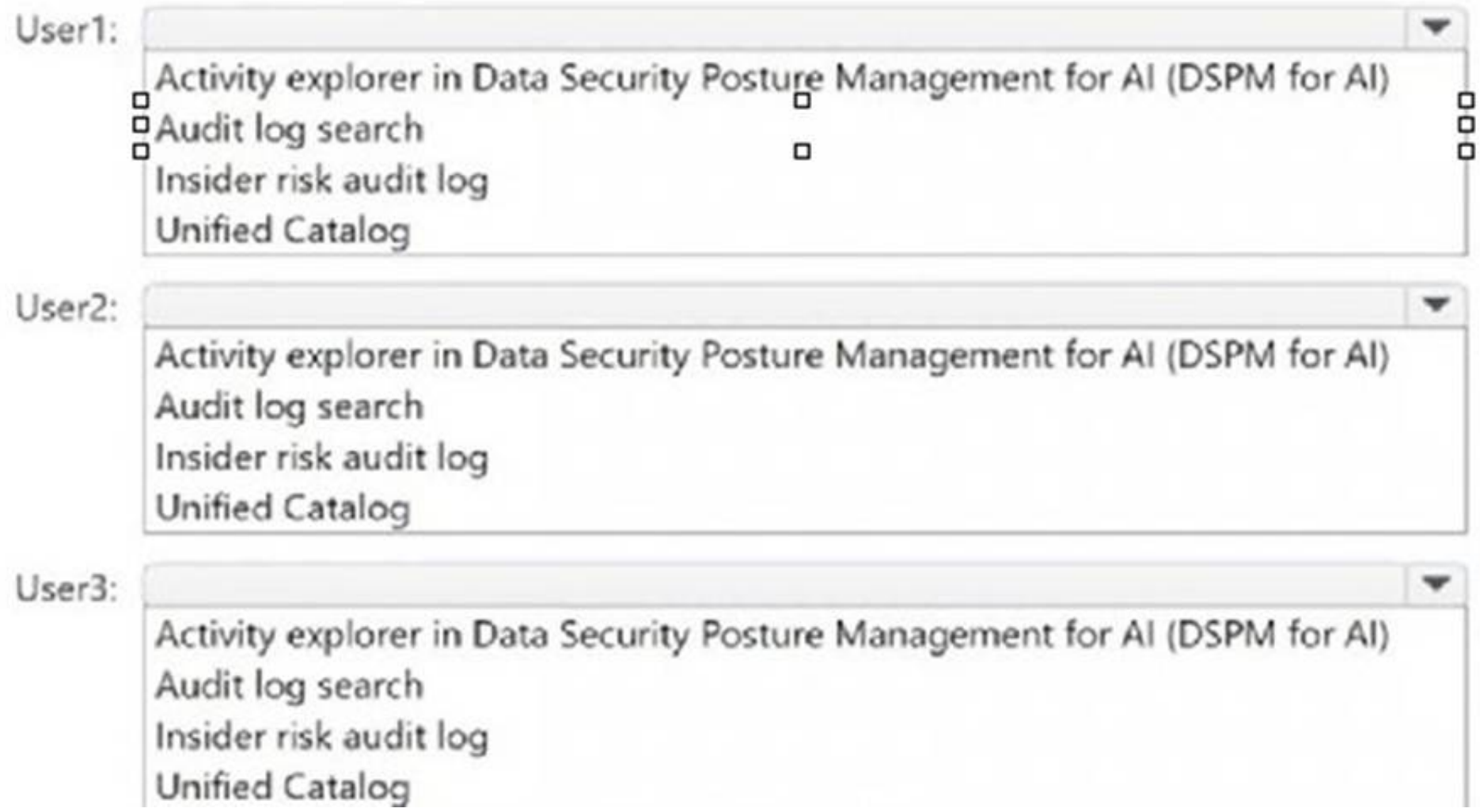
Name	Operating system	Microsoft Purview browser extension
Device1	Windows 11	Installed
Device2	Windows 11	Not installed
Deivce3	macOS	Installed

The subscription contains the users shown in the following table.

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

You need to review the activities.
What should you use for each user? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

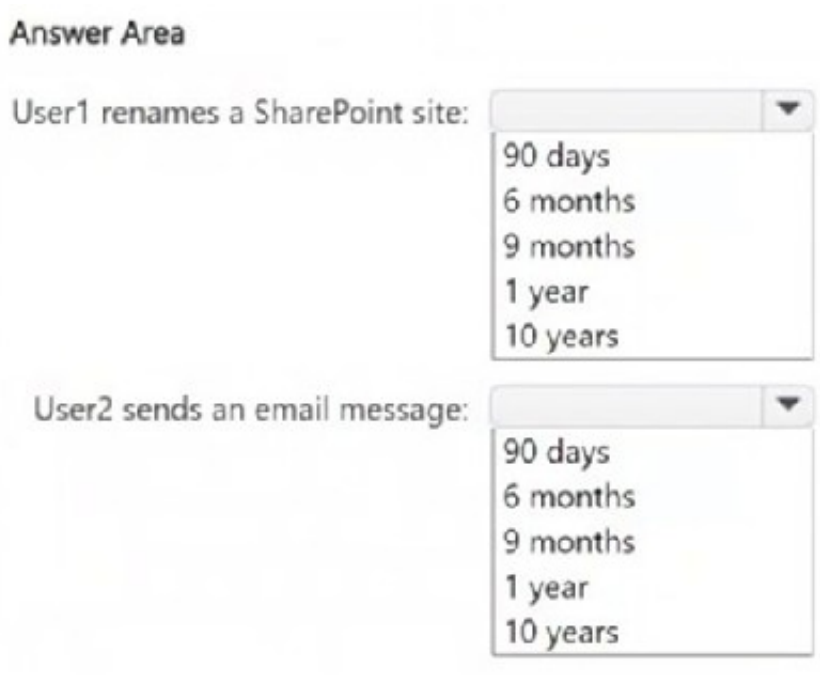
Answer: A

Explanation:
User1: Since the Microsoft Purview browser extension is installed on Device1, AI-related activity performed by User1 (generating an image using a generative AI website) can be reviewed in Activity explorer in DSPM for AI.
User2: Since Device2 does not have the Microsoft Purview browser extension installed, AI- related activity cannot be tracked in DSPM for AI. Instead, Audit log search should be used to review activity such as using Microsoft 365 Copilot.
User3: Since Device3 has the Microsoft Purview browser extension installed, AI-related activity (browsing sample content on a generative AI website) can be reviewed using Activity explorer in DSPM for AI.

NEW QUESTION 19
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. You create the audit retention policies shown in the following table.

Priority	Policy name	Record type	Activities	Users	Duration
10	AuditRetention1	ExchangeItem	MailboxLogin	*None*	90 Days
20	AuditRetention2	ExchangeItem	Send, MailItemsAccesssed	User1	9 Months
30	AuditRetention3	Sharepoint	*None*	User1	6 Months
40	AuditRetention4	Sharepoint	SiteRenamed	User1	9 Months
50	AuditRetention5	Sharepoint	SiteRenamed	*None*	10 Years

The users perform the following actions:
User1 renames a Microsoft SharePoint Online site. User2 sends an email message.
How long will the audit log records be retained for each action? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The action "SiteRenamed" for SharePoint is covered under the AuditRetention4 policy, which applies to User1 and retains logs for 9 months.
The action "Send" for ExchangeItem is covered under the AuditRetention2 policy, but this policy applies only to User1. Since User2 is not covered under a specific policy, the default retention period for audit logs in Microsoft Purview is 90 days.

NEW QUESTION 21
- (Topic 2)
You have a Microsoft 365 E5 subscription.
You need to ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days.
What should you configure first?

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

Answer: C

Explanation:
To ensure that encrypted email messages sent to external recipients can be revoked or expire within seven days, you need to configure a sensitivity label with encryption settings in Microsoft Purview Information Protection. A sensitivity label allows you to encrypt emails and documents, set expiration policies (e.g., emails expire after 7 days), and enable email revocation
How to configure it?
Go to Microsoft Purview compliance portal Information Protection Create a sensitivity label
Enable encryption and configure the content expiration policy Publish the label to users

NEW QUESTION 23
- (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 25
- (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 28
- (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 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