Microsoft

Exam Questions SC-401

Administering Information Security in Microsoft 365

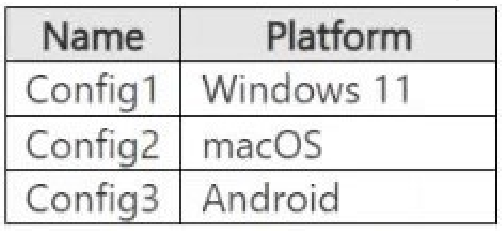
NEW QUESTION 1
- (Topic 1)
You need to meet the retention requirement for the users' Microsoft 365 data. What is the minimum number of retention policies required to achieve the goal?

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

Answer: B

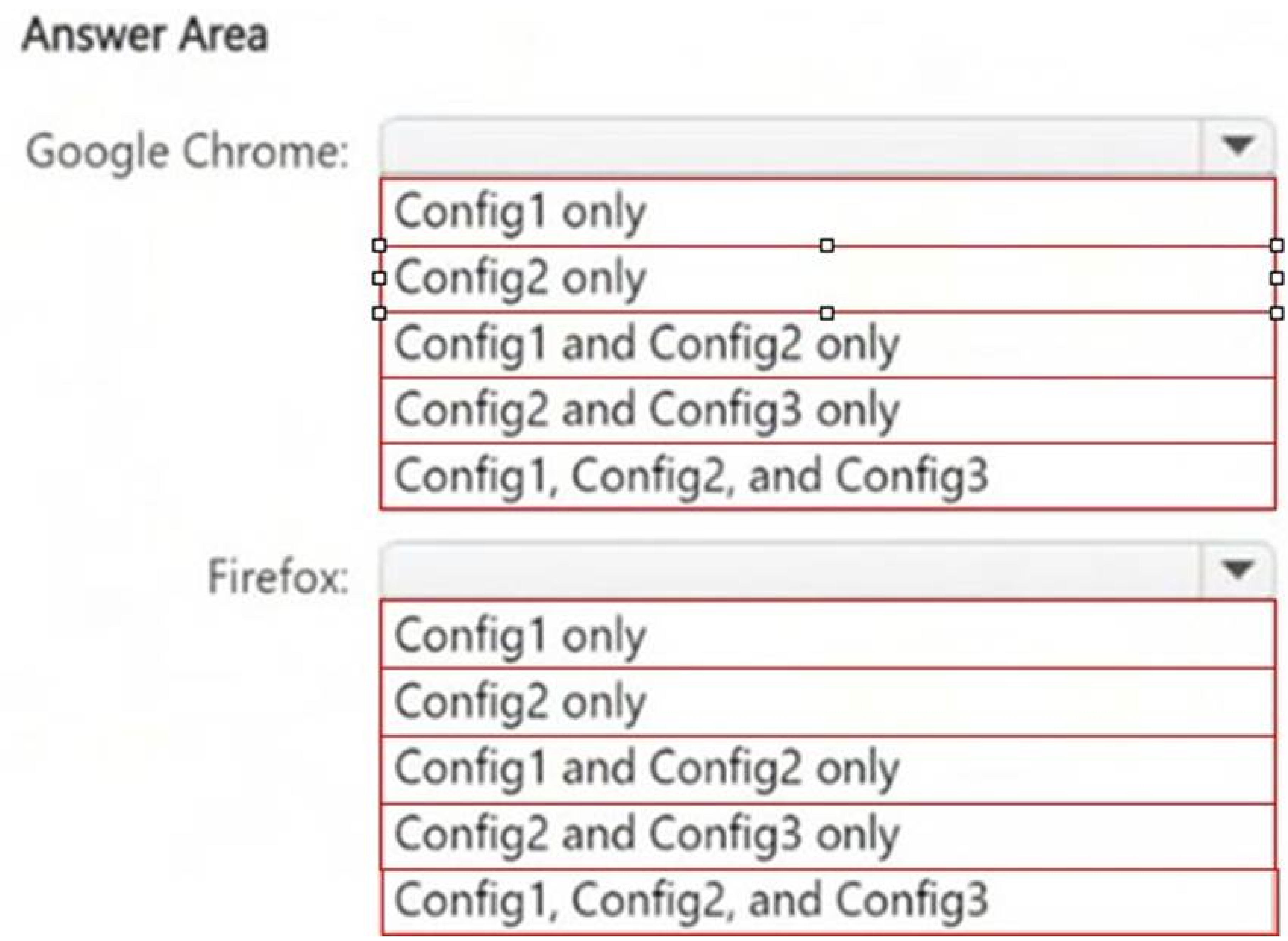
Explanation:
The requirement states that all Microsoft 365 data for users must be retained for at least one year. In Microsoft 365, retention policies must be configured for each type of data storage.
Step 1: Identifying Where Data is Stored
From the case study, users store data in the following locations: 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 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:

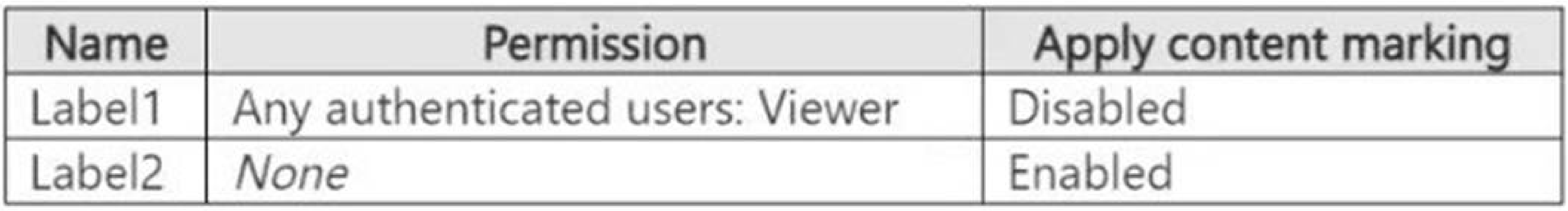
Config1 only
Config2 only
Config1 and Config2 only
Config2 and Config3 only
Config1, Config2, and Config3

A. Mastered
B. Not Mastered

Answer: A

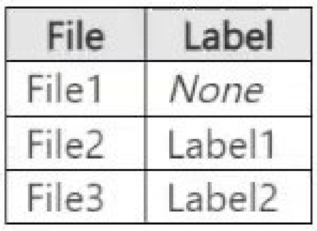
Explanation:
Microsoft Purview browser extensions for Endpoint DLP are supported on: Windows 10/11 (Config1)
macOS (Config2)
Not supported on Android (Config3)
Since Microsoft Purview does not support browser extensions on Android, Config3 is excluded from both Google Chrome and Firefox.

NEW QUESTION 3
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.



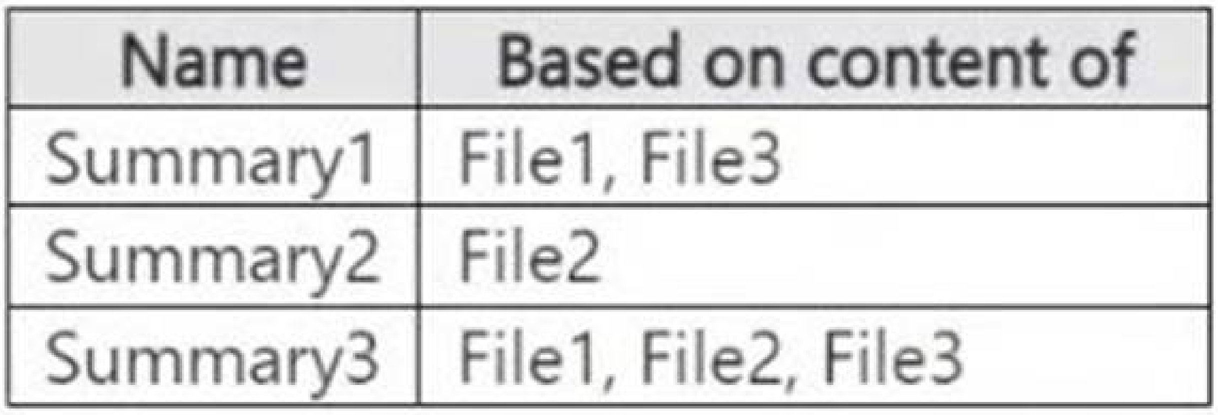
Name	Permission	Apply content marking
Label1	Any authenticated users: Viewer	Disabled
Label2	*None*	Enabled

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



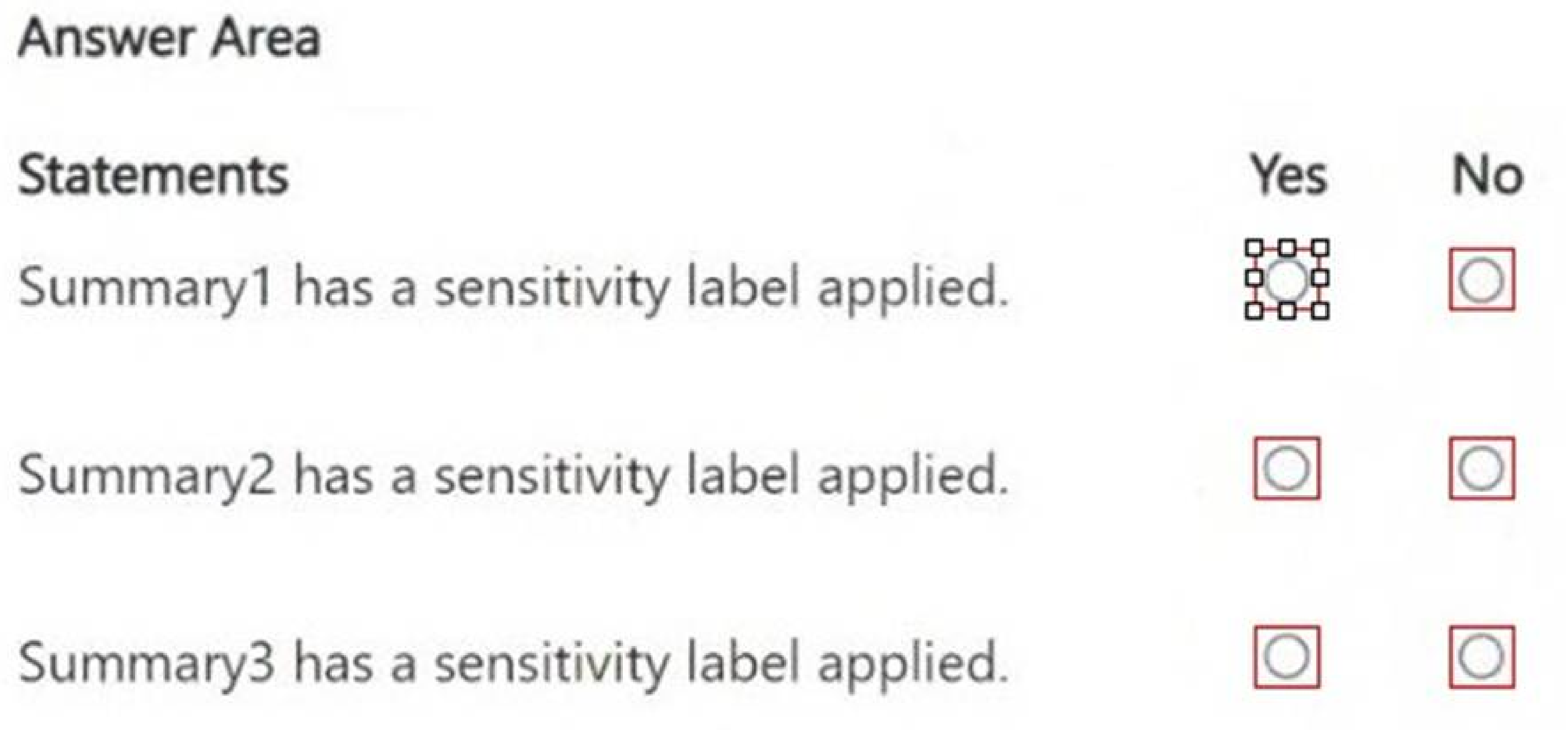
File	Label
File1	*None*
File2	Label1
File3	Label2

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.



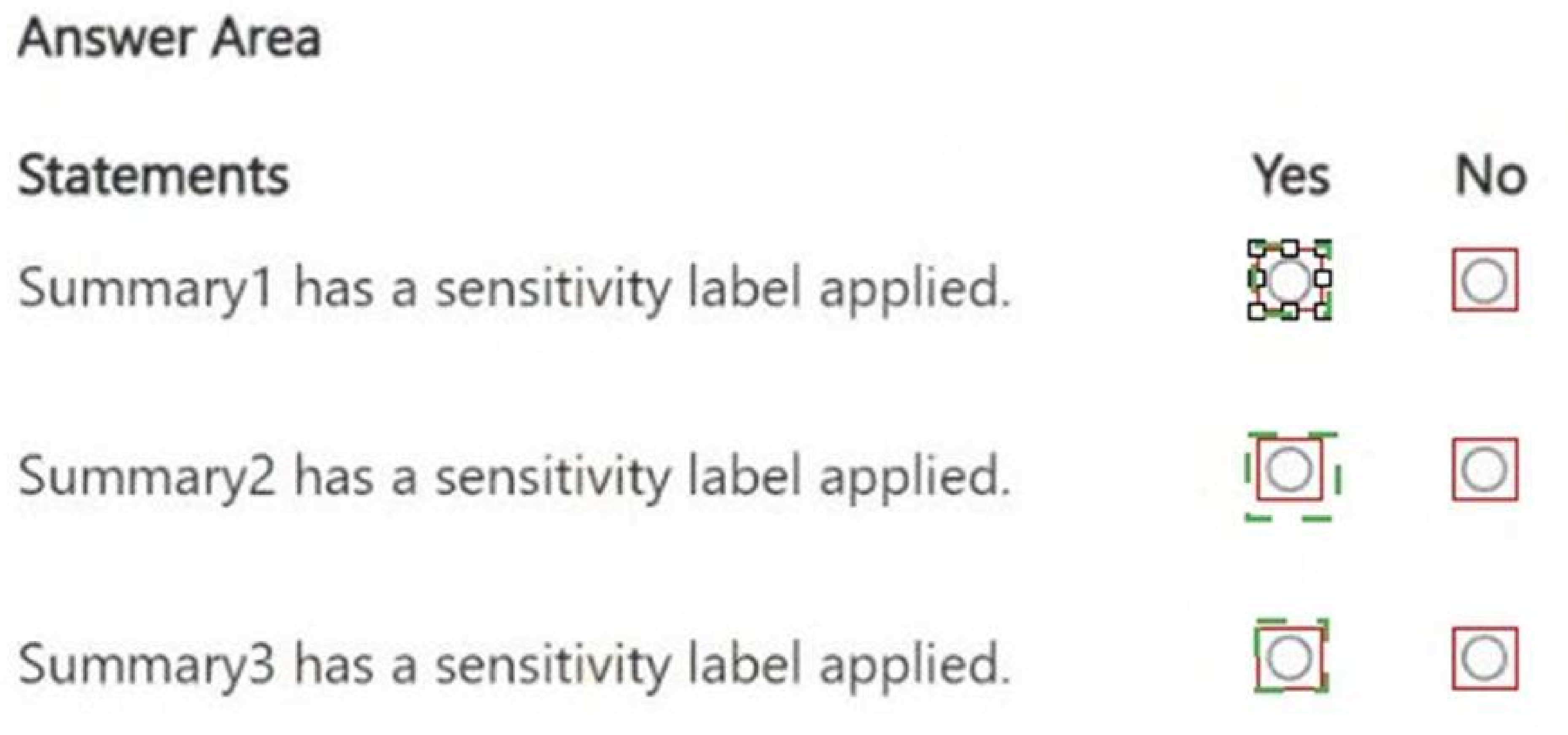
Answer Area

Statements	Yes	No
Summary1 has a sensitivity label applied.	○	○
Summary2 has a sensitivity label applied.	○	○
Summary3 has a sensitivity label applied.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements	Yes	No
Summary1 has a sensitivity label applied.	[✓ ○]	○
Summary2 has a sensitivity label applied.	[✓ ○]	○
Summary3 has a sensitivity label applied.	[✓ ○]	○

NEW QUESTION 4
- (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 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 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 6
- (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.

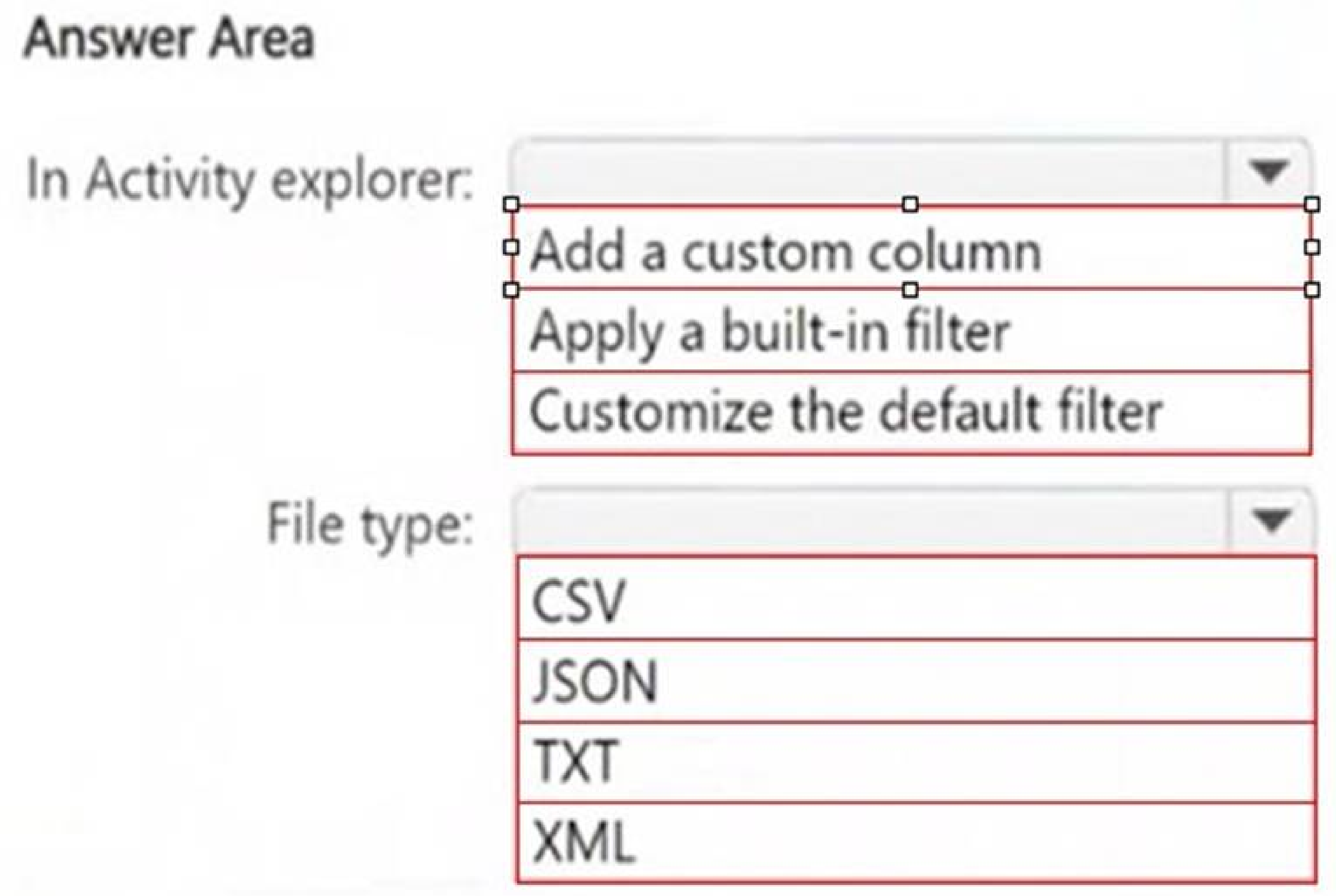
NEW QUESTION 7
- (Topic 2)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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 8
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.
You plan to export DLP activity by using Activity explorer.
The exported file needs to display the sensitive info type detected for each DLP rule match. What should you do in Activity explorer before exporting the data, and in which file format is the file exported? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.


Answer Area

In Activity explorer:
- Add a custom column
- Apply a built-in filter
- Customize the default filter

File type:
- CSV
- JSON
- TXT
- XML

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: To include the sensitive info type detected for each DLP rule match, you need to add a custom column in Activity Explorer. This ensures that the exported file contains specific details about the detected sensitive information types.
Box 2: DLP activity exports from Activity Explorer are always in CSV (Comma-Separated Values) format. This format allows for easy data analysis and reporting in Excel or other data-processing tools.

NEW QUESTION 9
- (Topic 2)
You have a Microsoft 365 E5 subscription.
You need to prevent users from uploading data loss prevention (DLP)-protected documents to the following third-party websites:
web1.contoso.com web2.contoso.com
The solution must minimize administrative effort.
To what should you set the Service domains setting for Endpoint DLP?

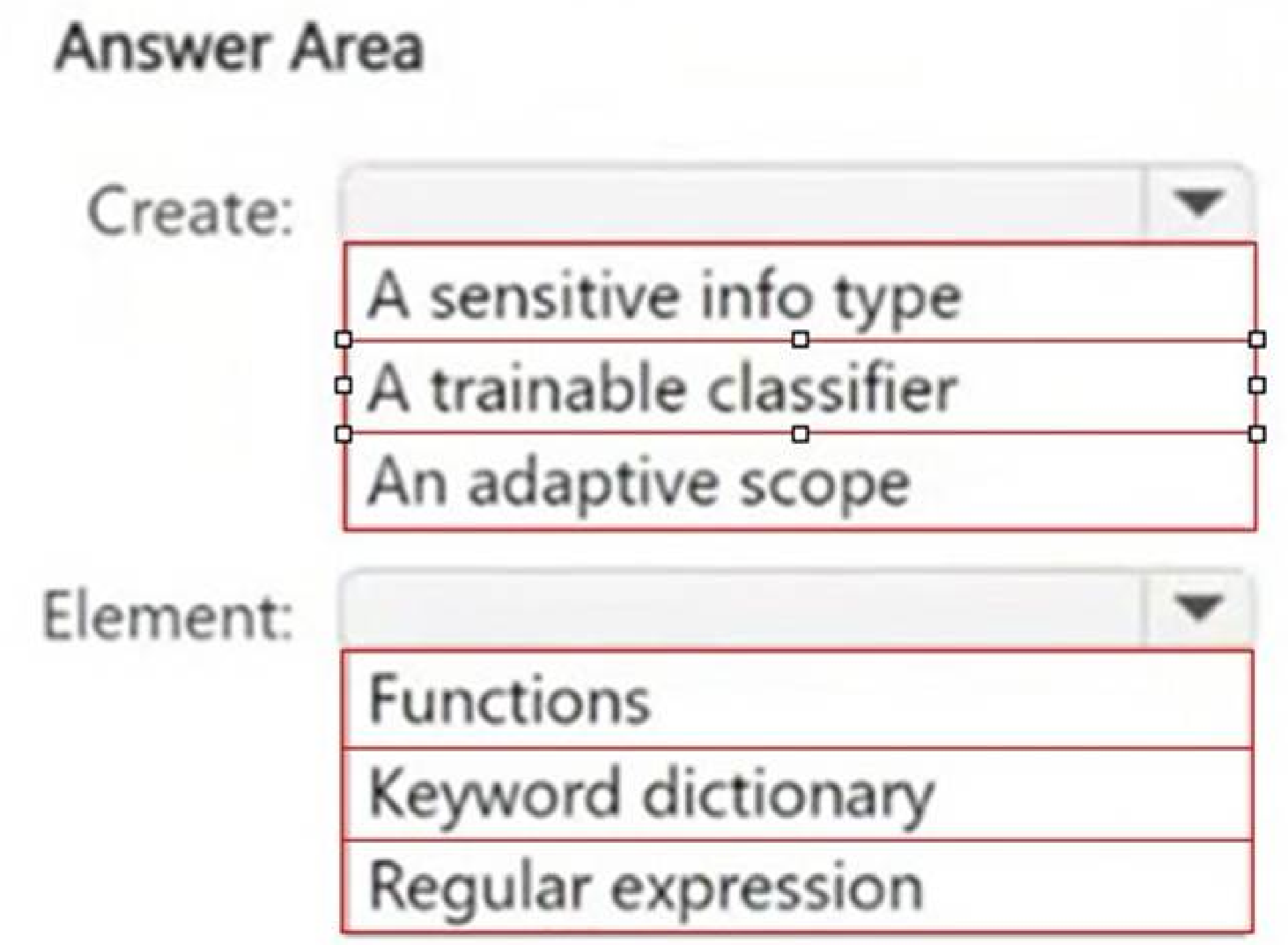
A. *.contoso.com
B. contoso.com
C. web1.contoso.com and web2.contoso.com
D. web*.contoso.com

Answer: C

Explanation:
The Service domains setting in Microsoft 365 Endpoint Data Loss Prevention (Endpoint DLP) allows administrators to block or allow specific domains for file

uploads. The goal is to prevent users from uploading DLP-protected documents to web1.contoso.com and web2.contoso.com.
Setting the Service domains to "web1.contoso.com and web2.contoso.com" precisely targets the two specific third-party websites, minimizing administrative effort while ensuring strict control.

NEW QUESTION 10
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription.
You have a file named Customer.csv that contains a list of 1,000 customer names. You plan to use Customer.csv to classify documents stored in a Microsoft SharePoint
Online library.
What should you create in the Microsoft Purview portal, and which type of element should you select? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

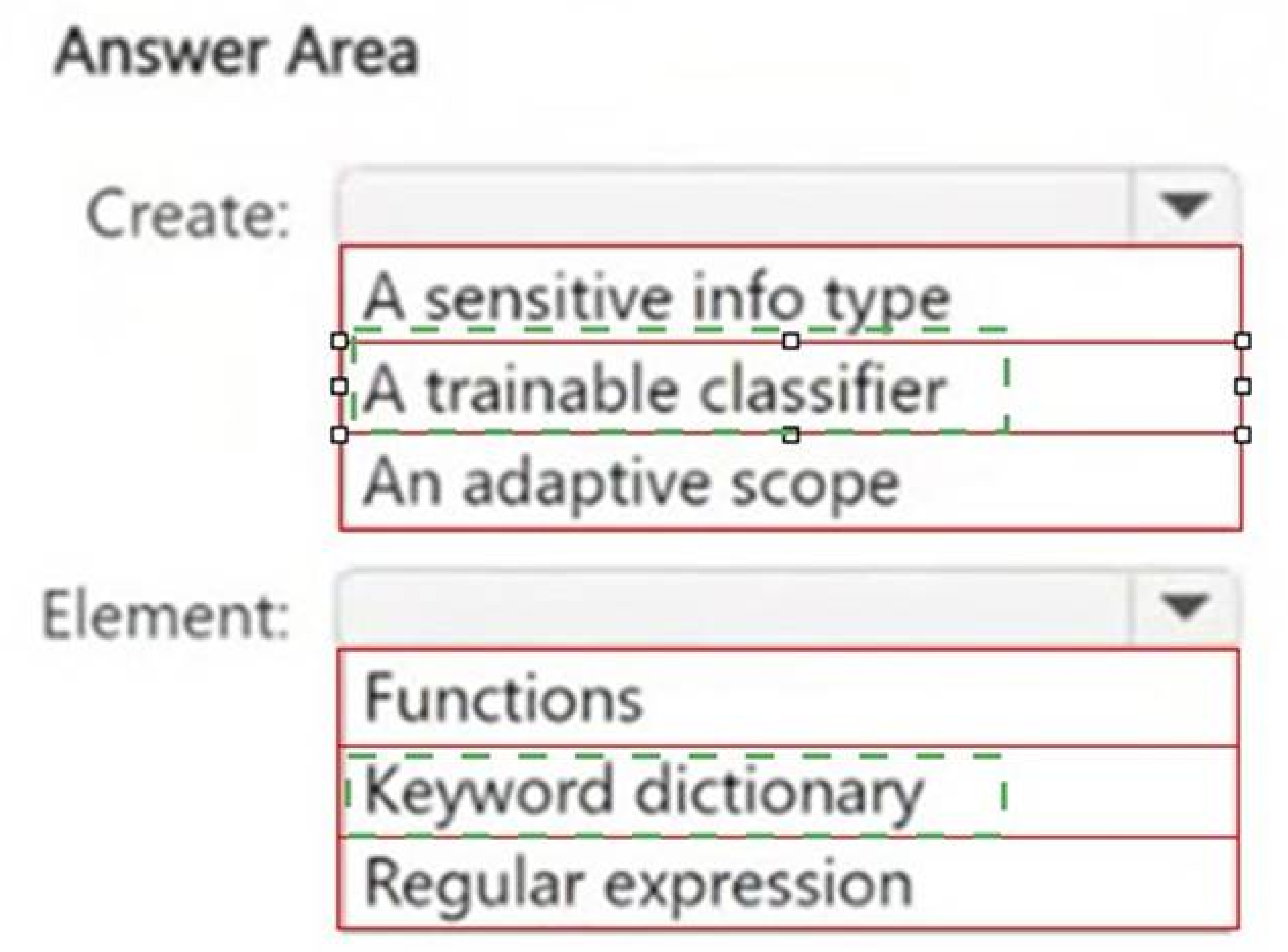
Create:
- A sensitive info type
- A trainable classifier
- An adaptive scope

Element:
- Functions
- Keyword dictionary
- Regular expression

A. Mastered
B. Not Mastered

Answer: A

Explanation:

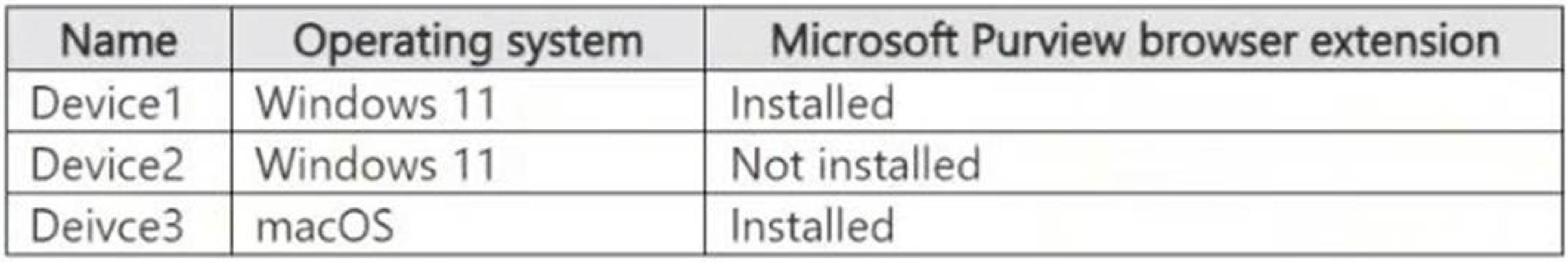


Answer Area

Create:
- A sensitive info type
- [✓ A trainable classifier]
- An adaptive scope

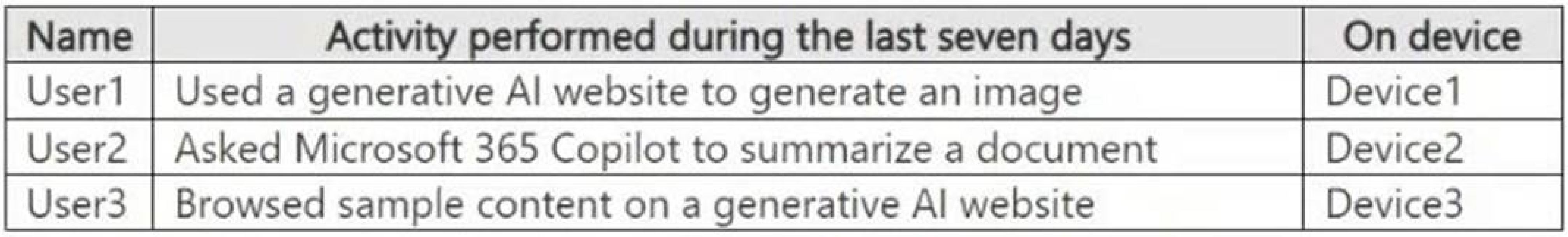
Element:
- Functions
- [✓ Keyword dictionary]
- Regular expression

NEW QUESTION 10
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.



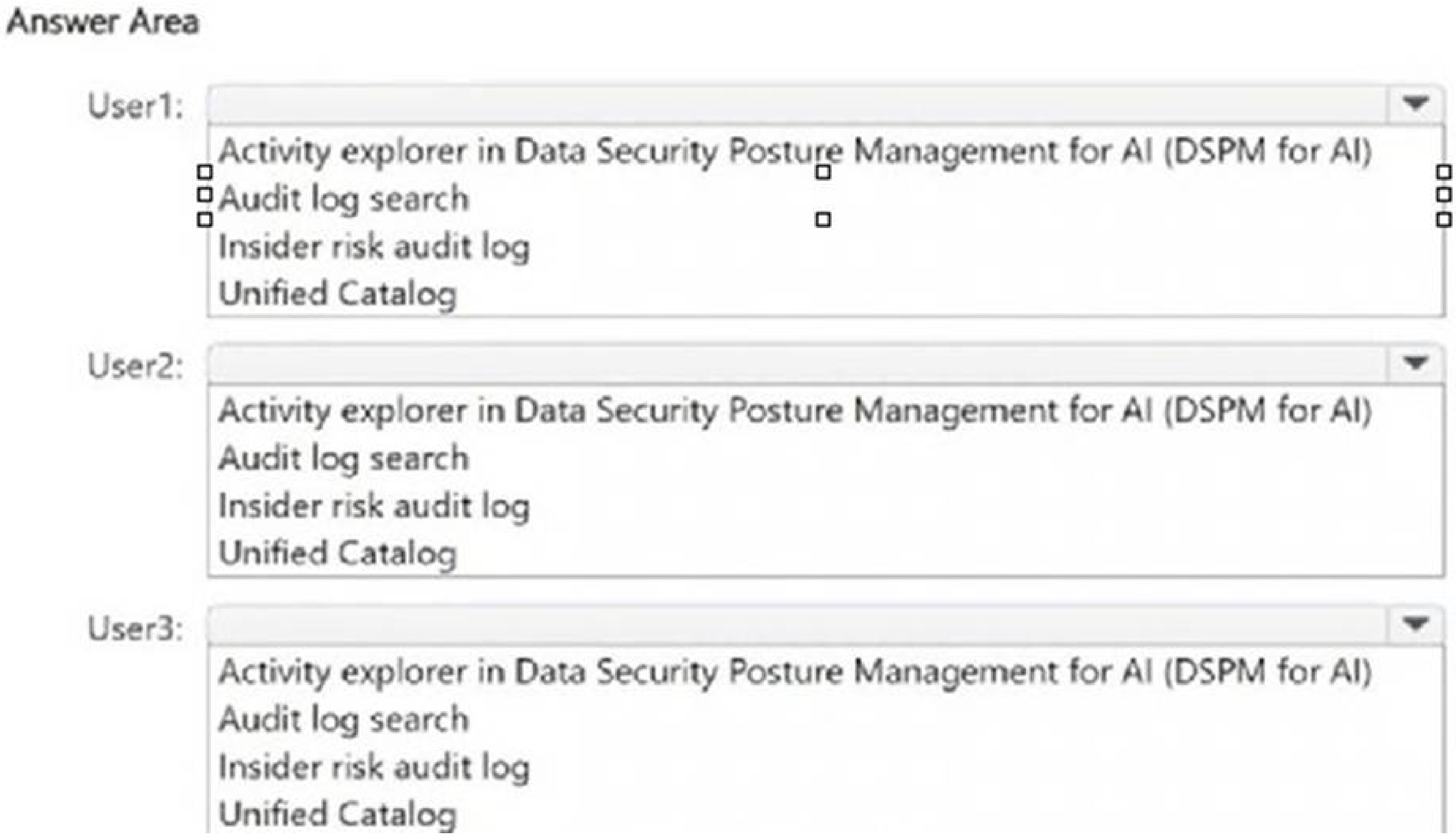
Name	Operating system	Microsoft Purview browser extension
Device1	Windows 11	Installed
Device2	Windows 11	Not installed
Deivce3	macOS	Installed

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

User1:
- Activity explorer in Data Security Posture Management for AI (DSPM for AI)
- Audit log search
- Insider risk audit log
- Unified Catalog

User2:
- Activity explorer in Data Security Posture Management for AI (DSPM for AI)
- Audit log search
- Insider risk audit log
- Unified Catalog

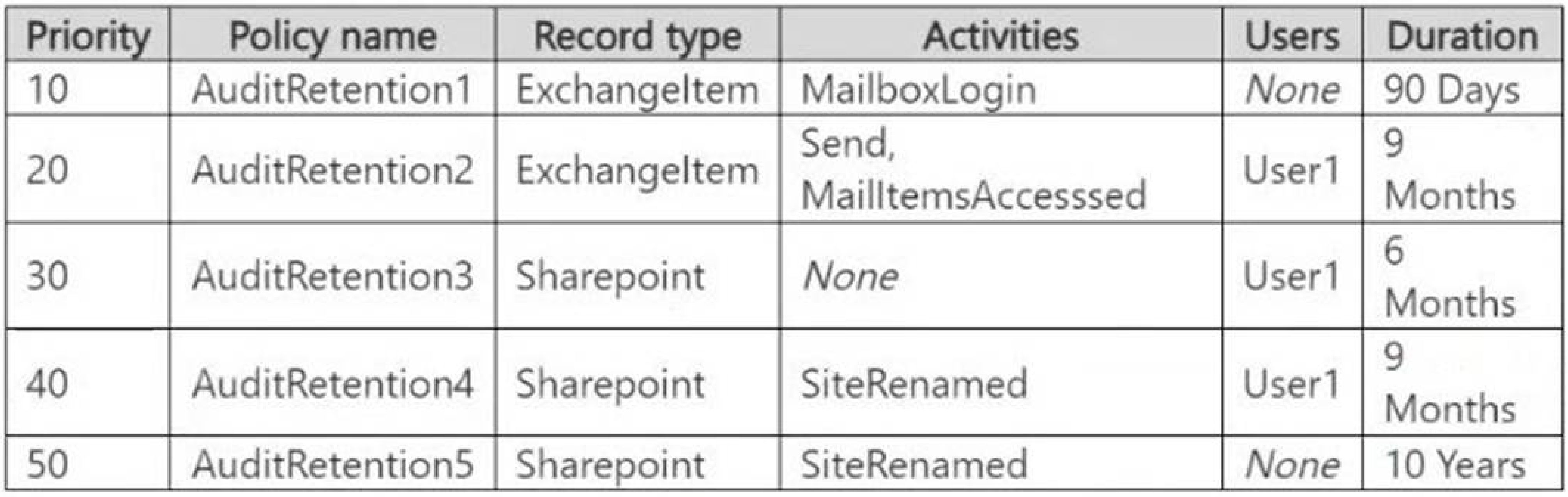
User3:
- Activity explorer in Data Security Posture Management for AI (DSPM for AI)
- Audit log search
- Insider risk audit log
- Unified Catalog

A. Mastered
B. Not Mastered

Answer: A

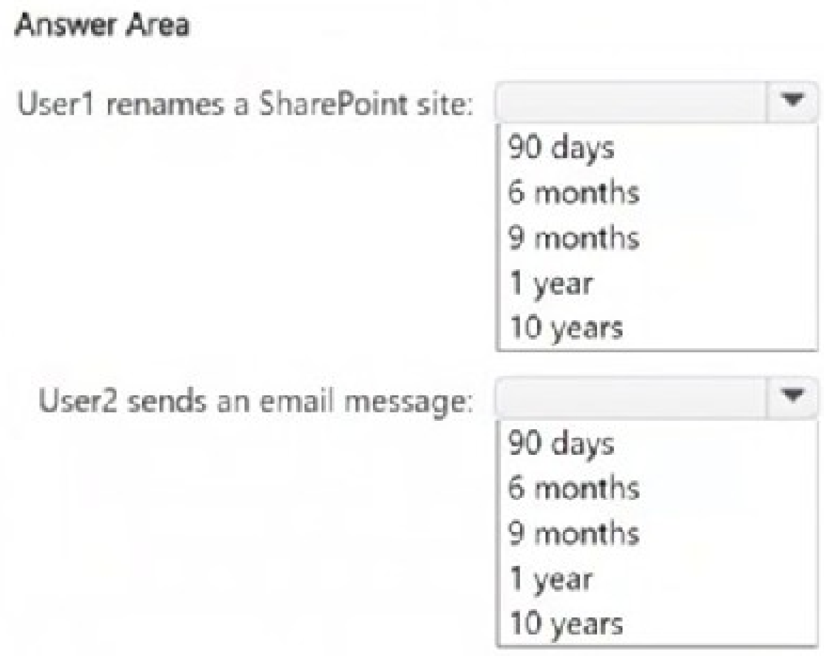
Explanation:
User1: Since the Microsoft Purview browser extension is installed on Device1, AI-related activity performed by User1 (generating an image using a generative AI website) can be reviewed in Activity explorer in DSPM for AI.
User2: Since Device2 does not have the Microsoft Purview browser extension 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 12
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.



Answer Area

User1 renames a SharePoint site:
- 90 days
- 6 months
- 9 months
- 1 year
- 10 years

User2 sends an email message:
- 90 days
- 6 months
- 9 months
- 1 year
- 10 years

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 16
- (Topic 2)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.
You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers. Tailspin_scanner.exe is installed locally on the computers.
You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.
Solution: From the Microsoft 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 18
- (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 21
- (Topic 2)
You have a Microsoft 365 E5 tenant.
You need to add a new keyword dictionary. What should you create?

A. a trainable classifier
B. a retention policy
C. a sensitivity label
D. a sensitive info type

Answer: D

Explanation:
To add a new keyword dictionary in Microsoft Purview Data Loss Prevention (DLP), you must create a Sensitive Information Type (SIT).
Sensitive Info Types (SITs) allow you to define custom detection rules, including keyword dictionaries, regular expressions, and functions for identifying sensitive content in emails, documents, and other Microsoft 365 locations. A keyword dictionary is a list of predefined words/phrases that Microsoft Purview can use to identify and classify content for DLP policies.
Steps to add a keyword dictionary:
* 1. Go to Microsoft Purview compliance portal
* 2. Navigate to Data classification > Sensitive info types
* 3. Create a new sensitive info type
* 4. Add a keyword dictionary
* 5. Save and use it in a DLP policy

NEW QUESTION 24
......