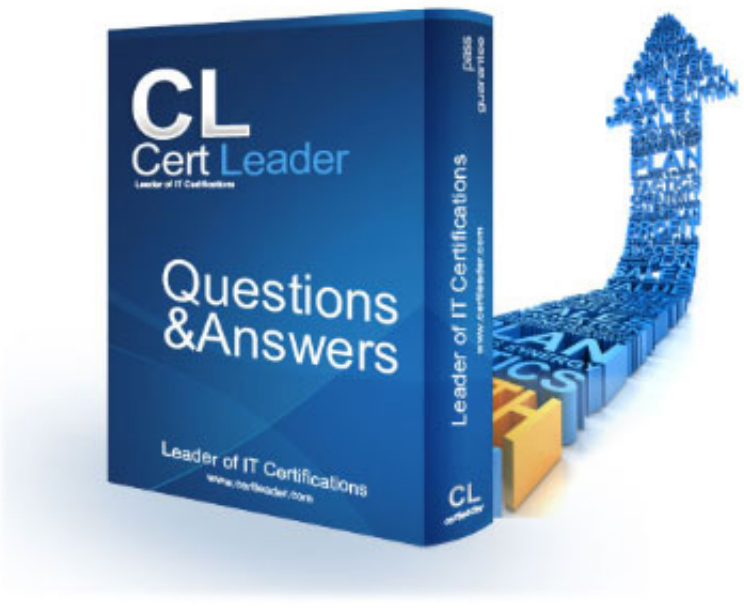
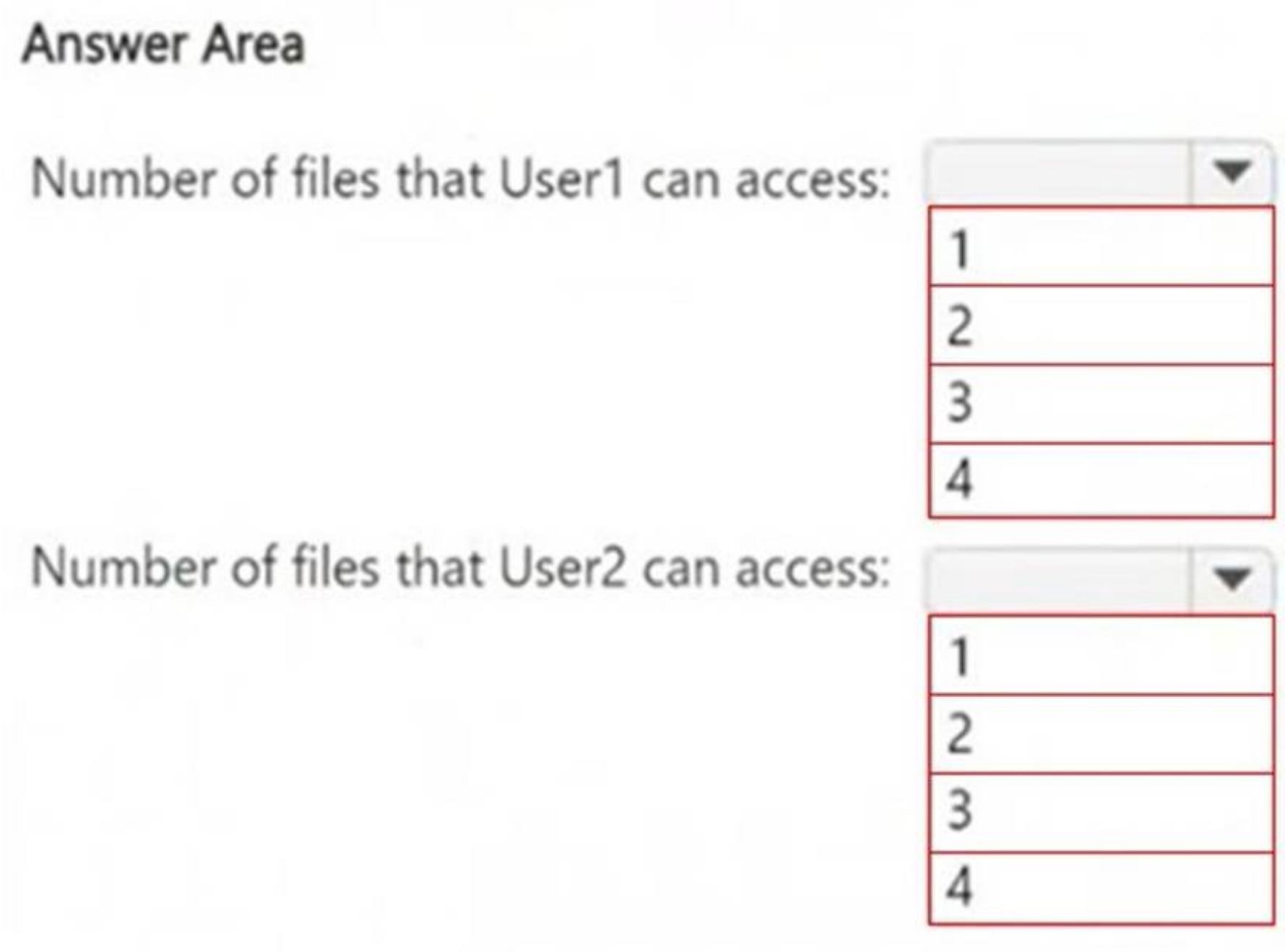
SC-401 Dumps

Administering Information Security in Microsoft 365

https://www.certleader.com/SC-401-dumps.html



NEW QUESTION 1
HOTSPOT - (Topic 1)
How many files in Site2 can User1 and User2 access after you turn on DLPpolicy1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Understanding DLP Policy Impact on File Access
The DLP policy (DLPpolicy1) applies to Site2 and restricts access when: Content contains SWIFT Codes.
Instance count is 2 or more.
File Analysis (Based on SWIFT Codes Count)

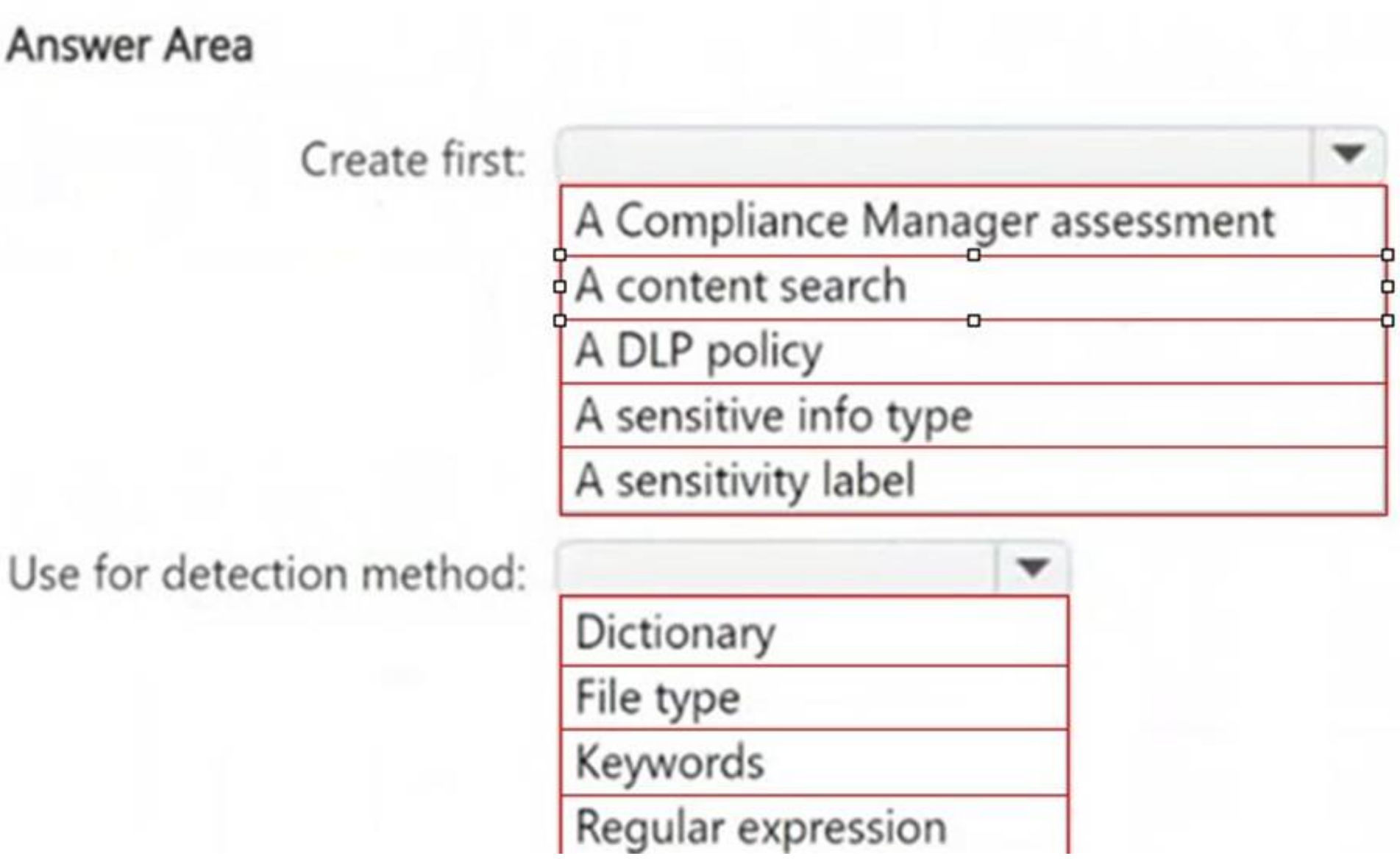
File Name	SWIFT Codes Count	DLP Policy Restricts Access?
File1.docx	1	☐ No restriction (SWIFT codes < 2)
File2.bmp	4	☐ Restricted (SWIFT codes ≥ 2)
File3.txt	3	☐ Restricted (SWIFT codes ≥ 2)
File4.xlsx	7	☐ Restricted (SWIFT codes ≥ 2)

Files that remain accessible (not restricted by DLP):
File1.docx (Contains only 1 SWIFT Code Below restriction threshold) User access after DLP policy is applied:

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

User1 (Site Owner):
Has higher privileges and can override DLP restrictions (through admin intervention). Can access 2 files (File1.docx + override access to another file).
User2 (Site Visitor):
Has read-only access but DLP blocks access to restricted files. Can only access 1 file (File1.docx), since all others are restricted.

NEW QUESTION 2
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.



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 3
- (Topic 2)
You have a Microsoft 365 E5 tenant that has devices onboarded to Microsoft Defender for Endpoint as shown in the following table.

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

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

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

Answer: B

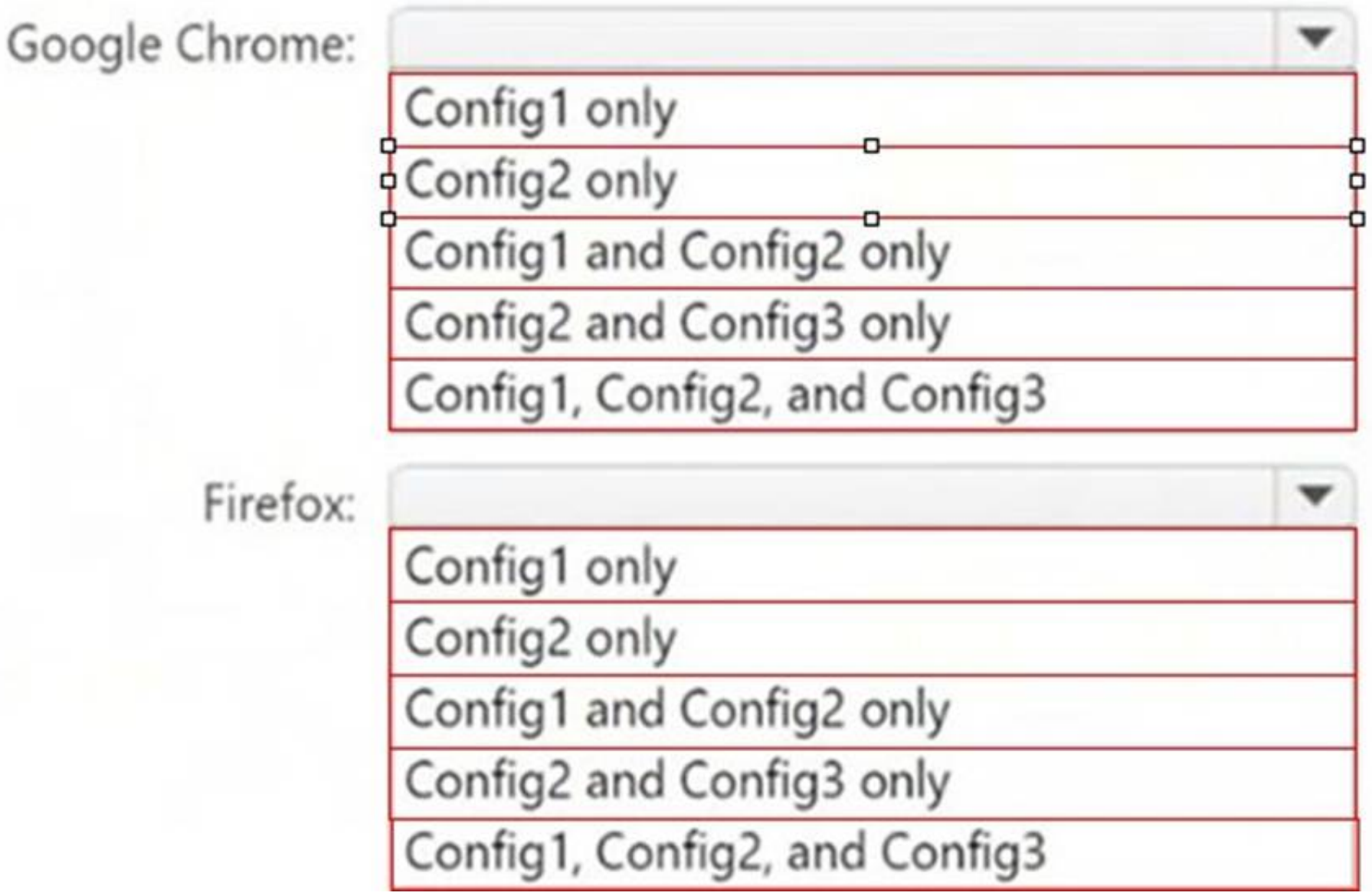
Explanation:
Microsoft 365 Endpoint data loss prevention (Endpoint DLP) is supported only on Windows 10 and Windows 11 devices. It does not support macOS or iOS at this time.
From the provided table:
Device1 (Windows 11) - Supported Device2 (Windows 10) - Supported Device3 (iOS) - Not supported Device4 (macOS) - Not supported
Thus, only Device1 and Device2 support Endpoint DLP.

NEW QUESTION 4
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription that contains the device configurations shown in the following table.

Name	Platform
Config1	Windows 11
Config2	macOS
Config3	Android

Each configuration uses either Google Chrome or Firefox as a default browser.
You need to implement Microsoft Purview and deploy the Microsoft Purview browser extension to the configurations.
To which configuration can each extension be deployed? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 5
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription that contains 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 6
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

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 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 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 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 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?

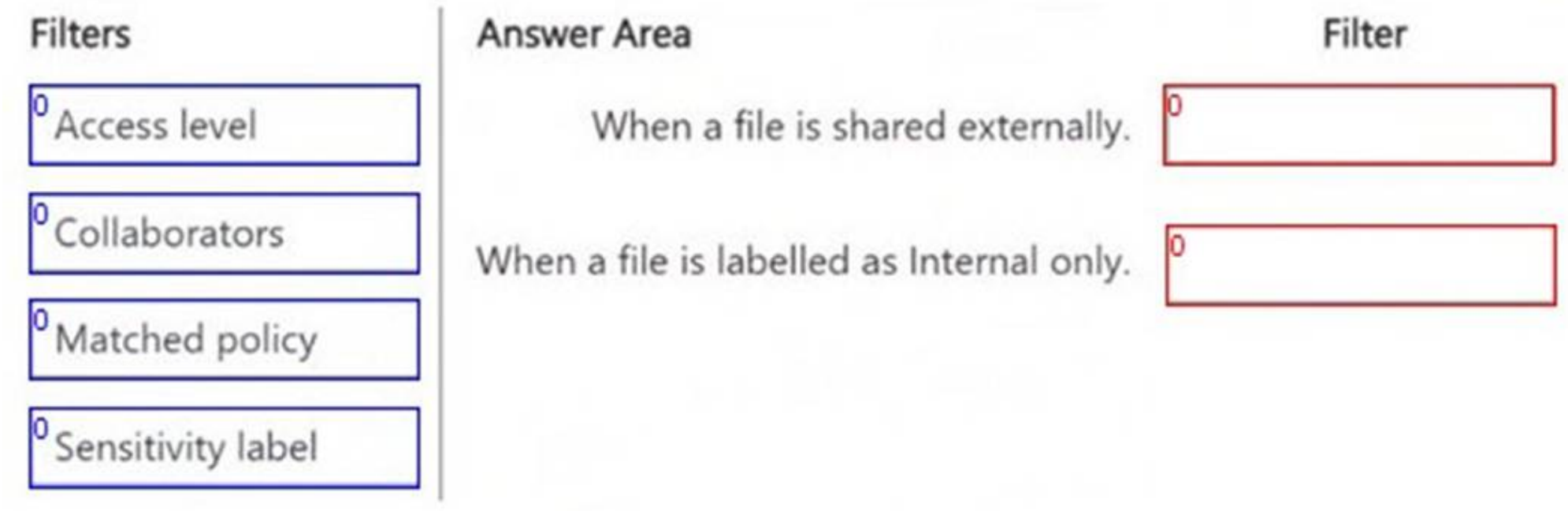
A. Yes
B. No

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.

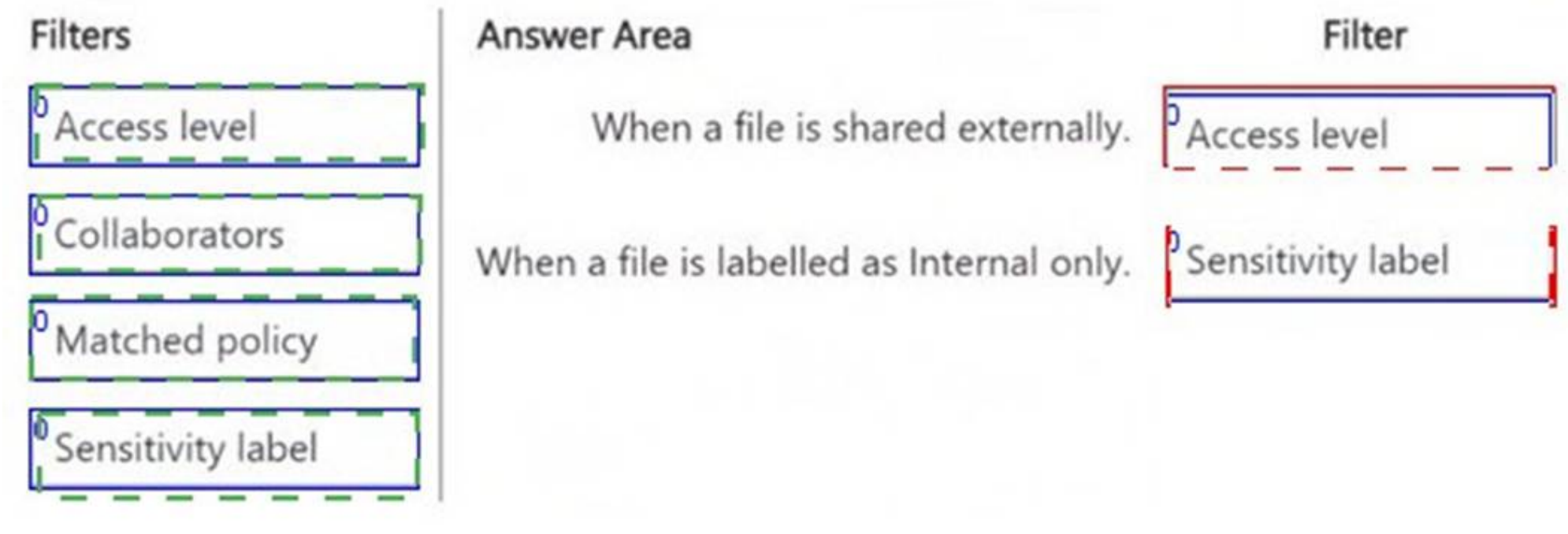
NEW QUESTION 9
DRAG DROP - (Topic 2)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You plan to deploy a Defender for Cloud Apps file policy that will be triggered when the following conditions are met:
A file is shared externally.
A file is labeled as internal 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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 10
- (Topic 2)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Description
User1	• User 1 is a regional manager. • User1 is assigned the Reader role. • Three department managers report to User1.
User2	• User2 is the human resources (HR) department manager. • User2 has no Microsoft Entra roles assigned. • Five HR department users report to User2.
User3	• User3 is a developer. • User3 reports to User2. • User3 is the only user in the compliance department. • User3 is assigned the Compliance Administrator role.
User4	• User4 is the assistant of User1. • User4 has no Microsoft Entra roles assigned. • User4 handles a high volume of confidential data on behalf of User1.

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

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

Answer: D

Explanation:
Microsoft Purview Insider Risk Management flags high-impact users based on various risk factors, including role, access to confidential data, and influence within an organization. Let's analyze each user:
User1 (Regional Manager, assigned Reader role, manages department managers) Risk Factors:
Holds a managerial position (regional manager).
Manages multiple department managers, indicating organizational influence. Access to critical business information.
Flagged? -Yes (Managerial role and access to confidential data).
User2 (HR department manager, no Microsoft Entra roles, manages HR department users) Risk Factors:
Manages HR department users, meaning they likely handle sensitive employee data. HR roles are often considered high-risk due to access to personal and payroll data.
Flagged? -Yes (HR role and access to sensitive employee data).
User3 (Developer, reports to User2, only user in compliance, assigned Compliance Administrator role)
Risk Factors:
Compliance Administrator role grants access to sensitive security and regulatory data. Only person in the compliance department, meaning they hold a critical role.
Potentially high impact on compliance and security settings.
Flagged? -Yes (Privileged Compliance Administrator role).
User4 (Assistant to User1, no Entra roles, handles confidential data on behalf of User1)
Risk Factors:
Handles a high volume of confidential data on behalf of a regional manager. Assistants with access to sensitive data are considered insider risk candidates.
Flagged? -Yes (High access to sensitive information).
Since all four users fit high-impact criteria (managerial roles, privileged compliance access, handling sensitive data), Microsoft Purview Insider Risk Management will flag all of them.

NEW QUESTION 10
- (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 13
- (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 15
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription that contains two Microsoft 365 groups named Group1 and Group2. Both groups use the following resources:
A group mailbox
Microsoft Teams channel messages
A Microsoft SharePoint Online teams site
You create the objects shown in the following table.

Name	Type	Description
RLabel1	Retention label	*None*
AutoApply1	Auto-labeling policy	Applies RLabel1 to Group1
Retention1	Retention policy	Applied to Group2

To which resources will AutoApply1 and Retention1 be applied? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area

AutoApply1:
- The group mailbox only
- The SharePoint Online teams site only
- The group mailbox and SharePoint Online teams site only
- The group mailbox and Teams channel messages only
- The group mailbox, SharePoint Online teams site, and Teams channel messages

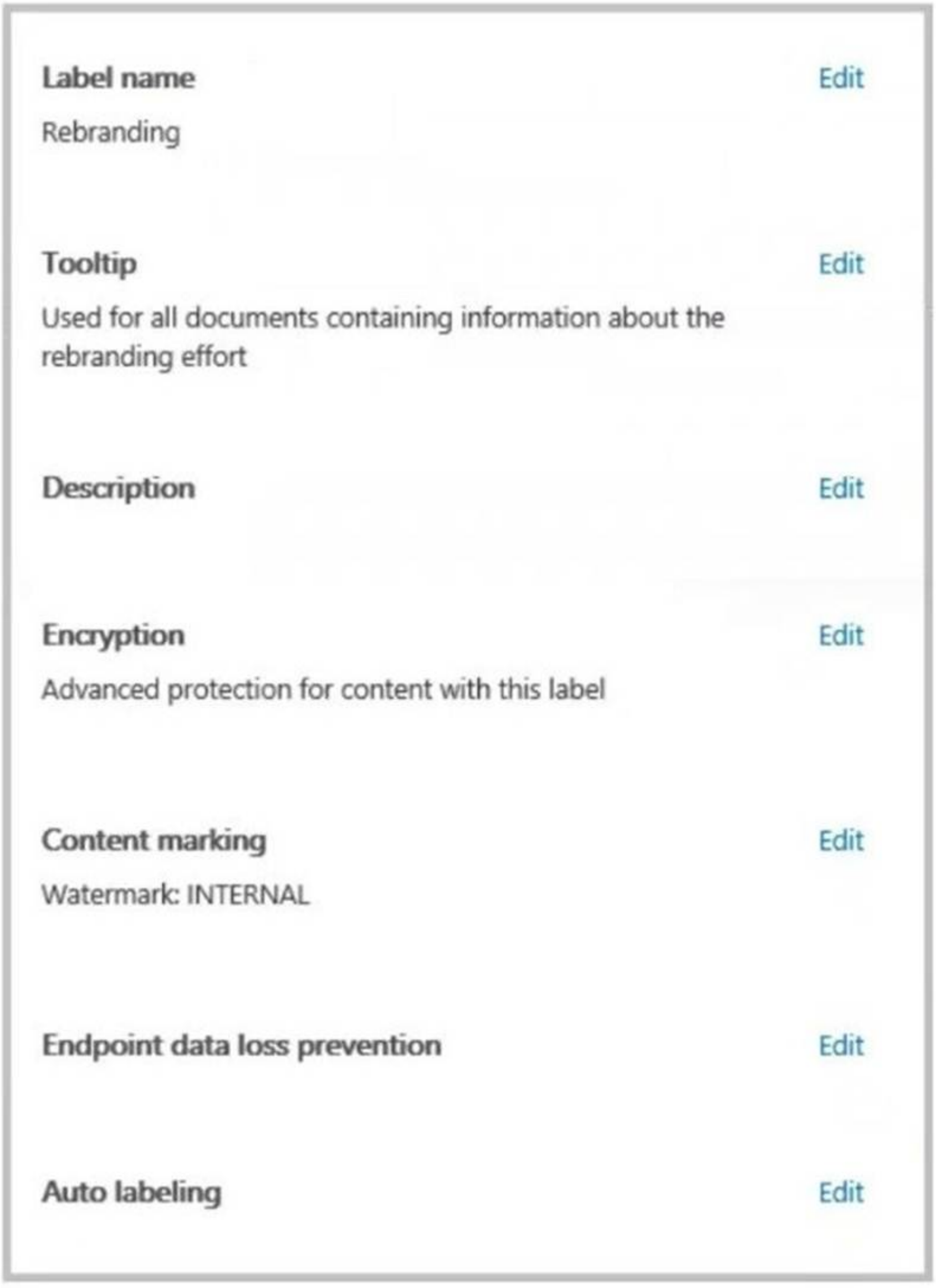
Retention1:
- The group mailbox only
- The SharePoint Online teams site only
- The group mailbox and SharePoint Online teams site only
- The group mailbox and Teams channel messages only
- The group mailbox, SharePoint Online teams site, and Teams channel messages

A. Mastered
B. Not Mastered

Answer: A

Explanation:
AutoApply1 is an auto-labeling policy that applies RLabel1 to Group1. Auto-labeling policies can apply retention labels across group mailboxes, SharePoint Online sites, and Teams channel messages if they are configured for group resources.
Retention1 is a retention policy applied to Group2. Retention policies for Microsoft 365 groups apply to all group resources, including group mailboxes, SharePoint Online teams sites, and Teams channel messages.
Since both AutoApply1 and Retention1 affect entire groups, they apply to all associated resources: group mailbox, SharePoint Online teams site, and Teams channel messages.

NEW QUESTION 20
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.



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.	○	○
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	○
The sensitivity label can be applied only to documents that contain the word rebranding.	○	○

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
- (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	• 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.

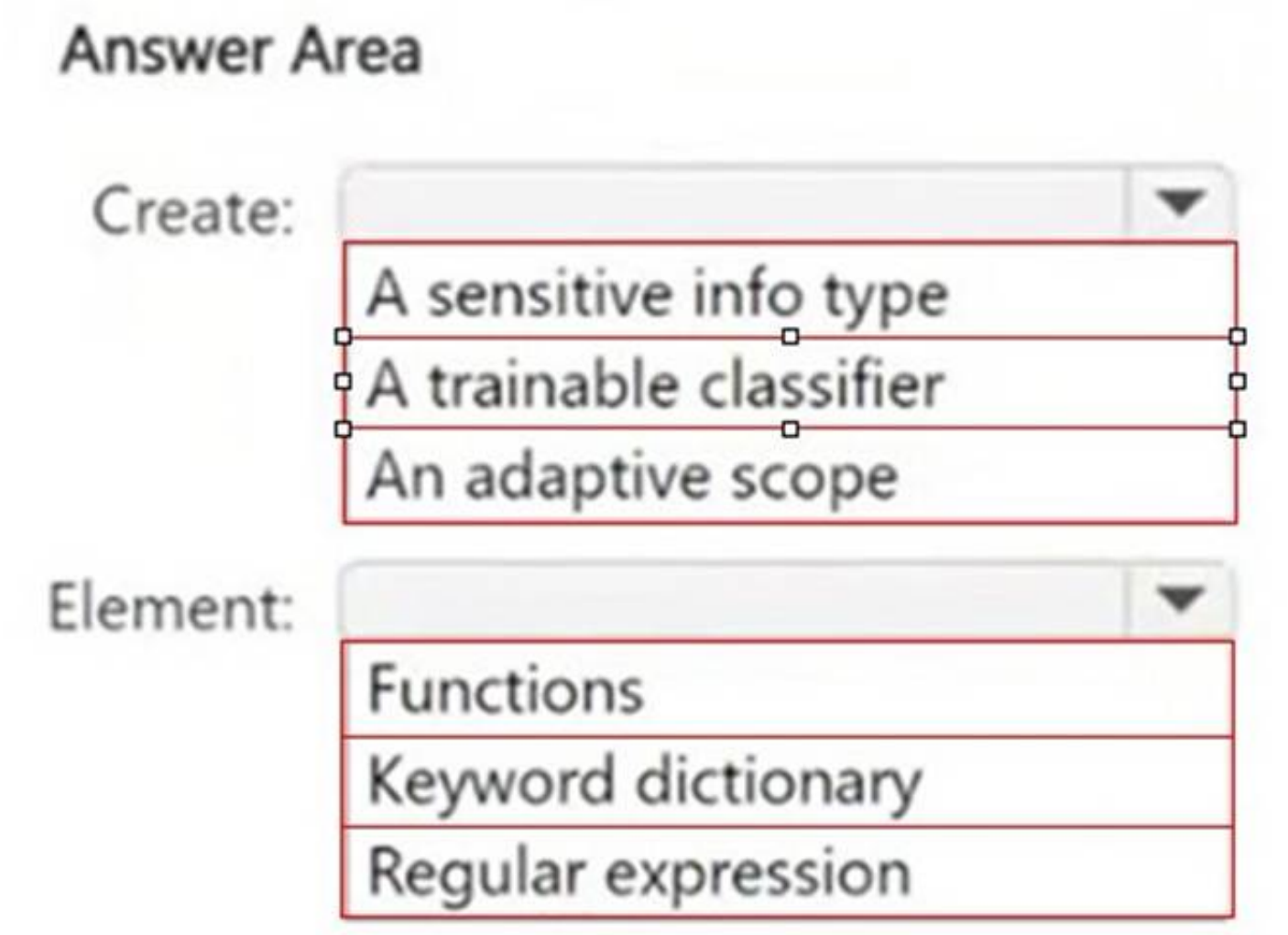
NEW QUESTION 32
- (Topic 2)
You have a Microsoft 365 E5 subscription.
You need to prevent users from uploading data loss prevention (DLP)-protected documents to the following third-party websites:
web1.contoso.com web2.contoso.com
The solution must minimize administrative effort.
To what should you set 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 36
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 41
- (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 43
- (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 44
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 45
- (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

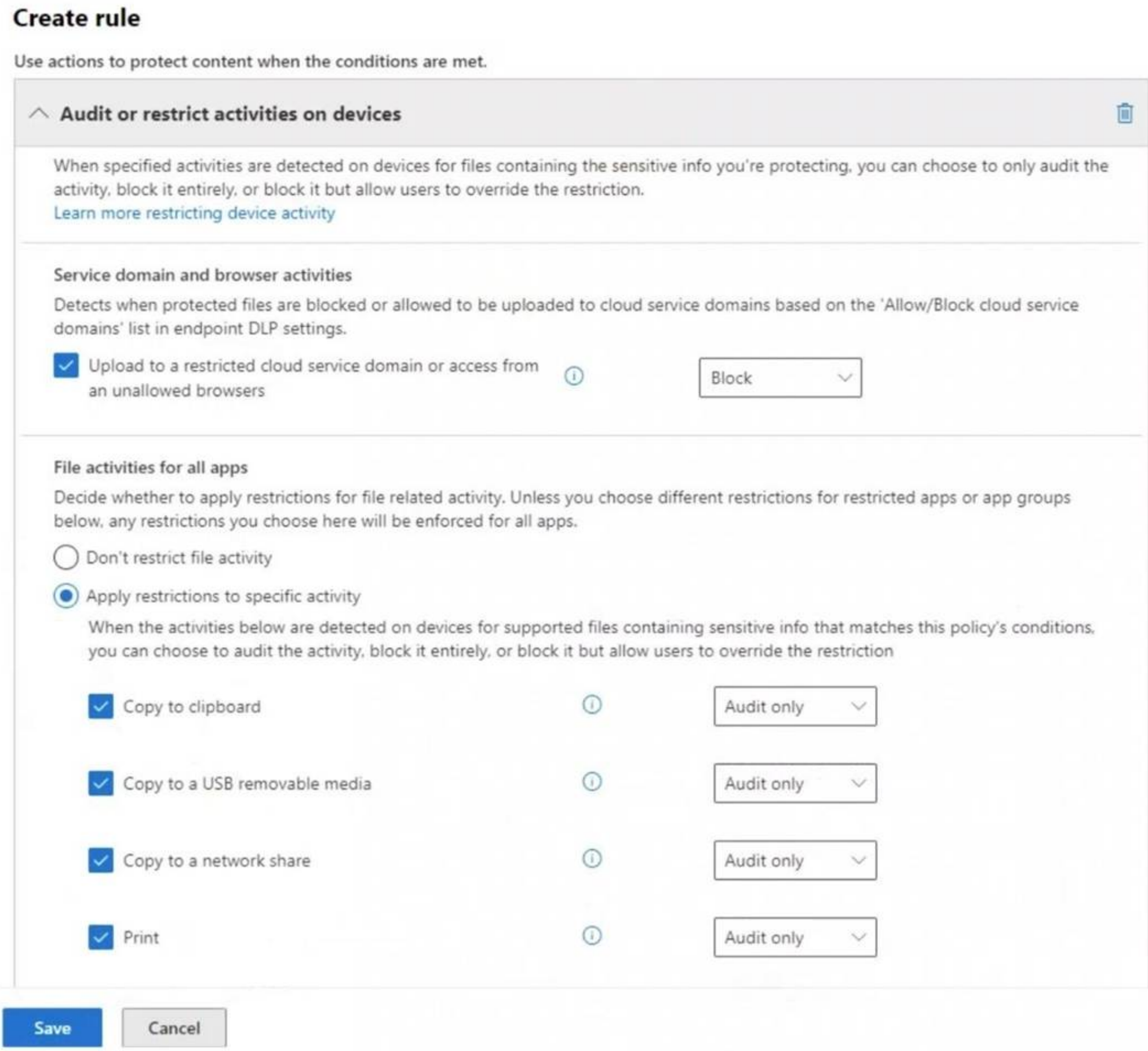
Which items can use Trainable 1?

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.



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 51
- (Topic 2)
You have a Microsoft SharePoint Online site named Site1 that contains a document library. The library contains more than 1,000 documents. Some of the documents are job applicant resumes. All the documents are in the English language.
You plan to apply a sensitivity label automatically to any document identified as a resume. Only documents that contain work experience, education, and accomplishments must be labeled automatically.
You need to identify and categorize the resumes. The solution must minimize administrative effort.

What should you include in the solution?

A. a trainable classifier
B. a keyword dictionary
C. a function
D. an exact data match (EDM) classifier

Answer: A

Explanation:
Since you need to automatically apply a sensitivity label to resumes based on their content and structure (work experience, education, accomplishments), a trainable classifier is the best choice.
Trainable classifiers use machine learning to identify unstructured data, such as resumes, contracts, or legal documents. Instead of relying on predefined patterns (like keywords or regular expressions), a trainable classifier learns from sample documents and can accurately identify resumes even if they are formatted differently.
Final Approach:
Train a trainable classifier using sample resumes. Deploy the classifier in Microsoft Purview.
Configure a sensitivity label to be automatically applied when a document matches the classifier.

NEW QUESTION 54
- (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 57
- (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 60
- (Topic 2)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1. Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1. Solution: You run the Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogCmdlets *Mailbox* command. Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogCmdlets
Mailbox command is incorrect. This enables admin audit logging, which tracks changes to mailbox configurations (e.g., mailbox settings updates), not user activity inside the mailbox.

NEW QUESTION 62
- (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 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.

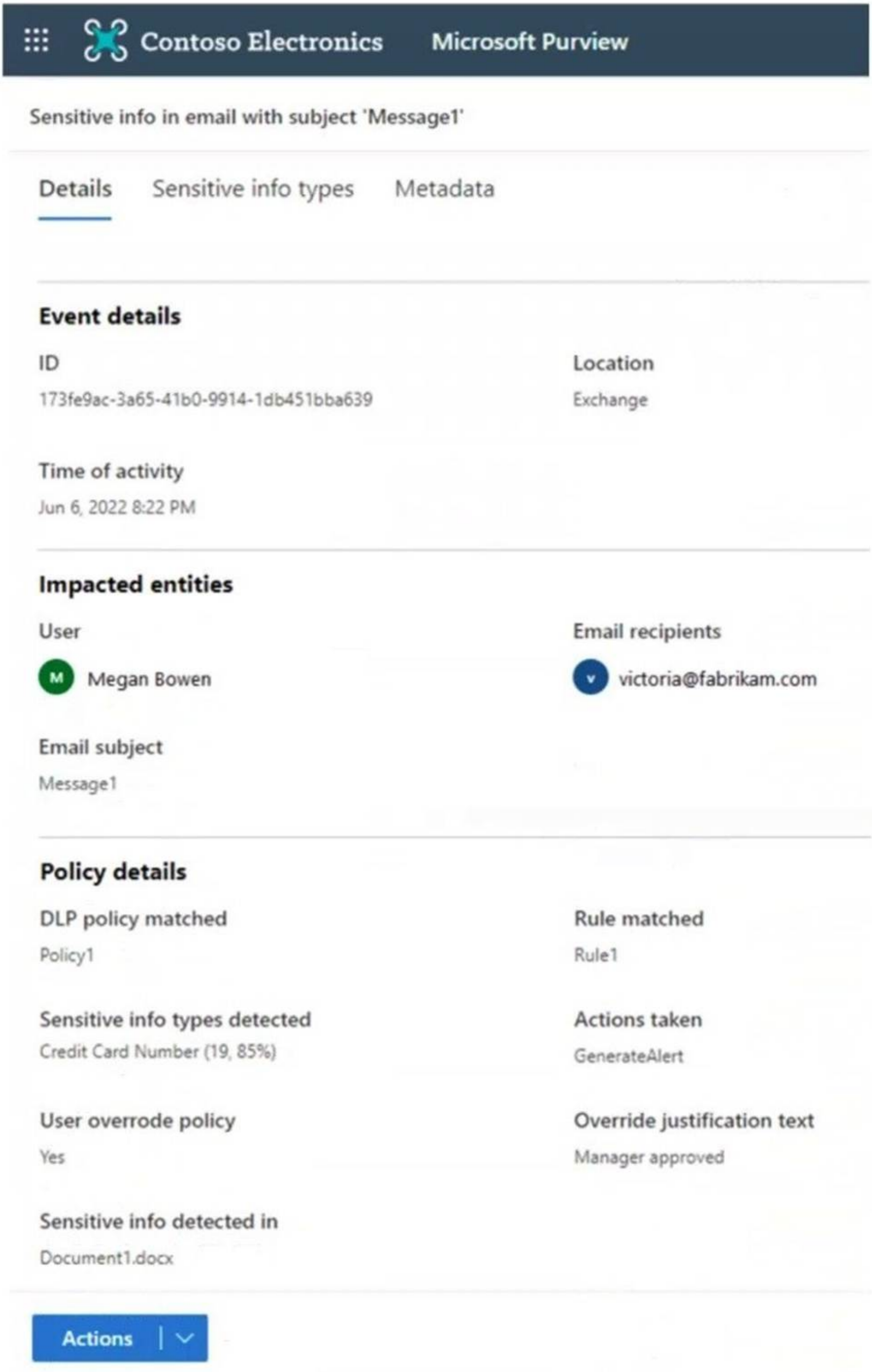
A. From Microsoft Defender for Cloud Apps, create a file policy.
B. From the SharePoint admin center, modify the Site Settings.
C. From the SharePoint ad min center, modify the records management settings.
D. From the Microsoft Purview portal, publish a label.

E. From the Microsoft Purview portal, create a label.

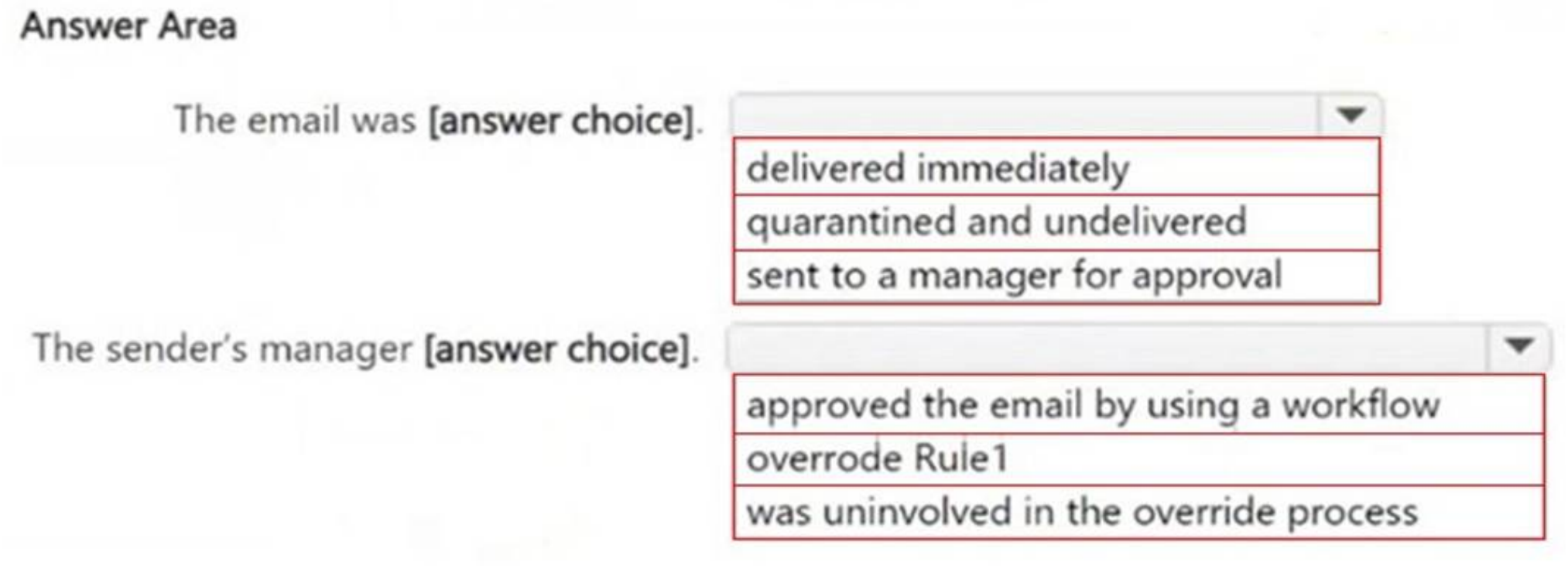
Answer: DE

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 66
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription.
You receive the data loss prevention (DLP) alert shown in the following exhibit.


Contoso Electronics
Microsoft Purview
Sensitive info in email with subject 'Message1'
Details
Sensitive info types
Metadata
Event details
ID
173fe9ac-3a65-41b0-9914-1db451bba639
Location
Exchange
Time of activity
Jun 6, 2022 8:22 PM
Impacted entities
User
Megan Bowen
Email recipients
victoria@fabrikam.com
Email subject
Message1
Policy details
DLP policy matched
Policy1
Rule matched
Rule1
Sensitive info types detected
Credit Card Number (19, 85%)
Actions taken
GenerateAlert
User overrode policy
Yes
Override justification text
Manager approved
Sensitive info detected in
Document1.docx
Actions

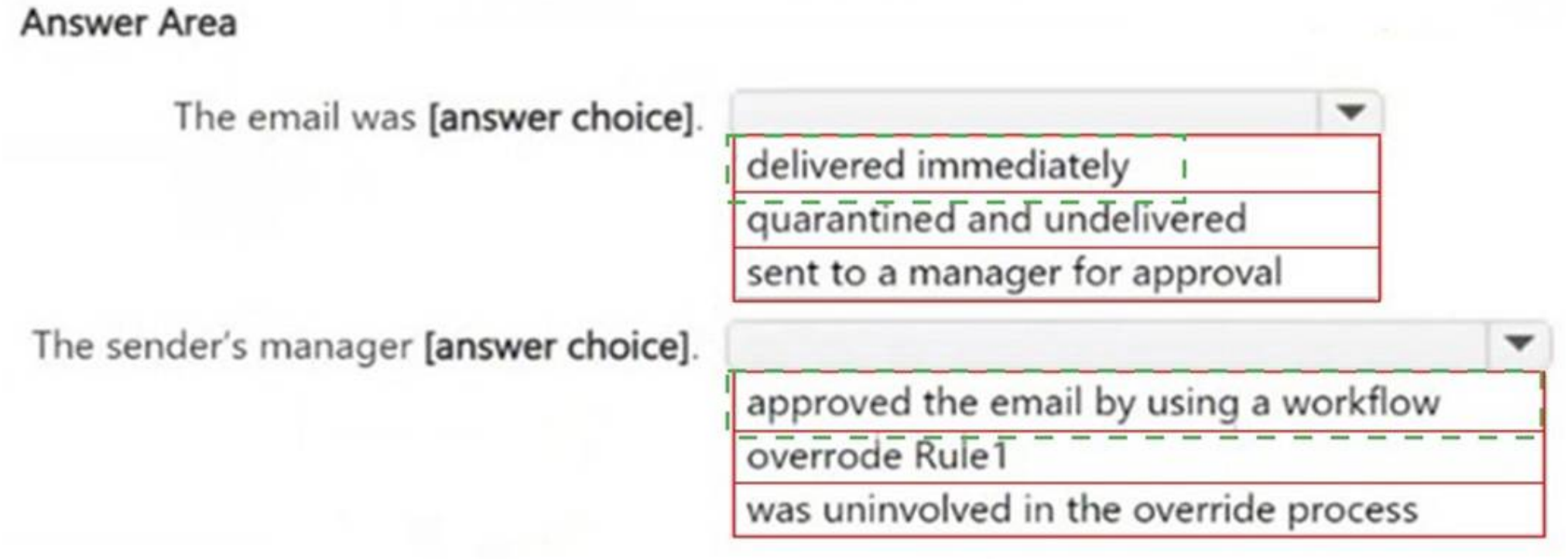
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 70
- (Topic 2)
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft Purview insider risk management. You implement the HR data connector.
You need to prepare the data that will be imported by the data connector. In which format should you prepare the data?

A. JSON
B. CSV
C. TSV
D. XML
E. PRN

Answer: B

Explanation:
When implementing Microsoft Purview Insider Risk Management and using the HR data connector, you must prepare HR data in CSV (Comma-Separated Values) format. This format is required because Microsoft Purview supports CSV files for importing user employment details, termination dates, role changes, and other HR-related attributes.

NEW QUESTION 75
- (Topic 2)
You need to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company.
What should you do?

A. From the Microsoft Purview portal create an insider risk policy
B. From the Microsoft Defender portal create a file policy

C. From the Microsoft Defender portal, create an activity policy.
D. From the Microsoft Purview portal, start a data investigation.

Answer: B

Explanation:
An activity policy in Microsoft Defender for Cloud Apps (Microsoft Defender portal) allows you to track and alert on specific user actions, such as sharing sensitive documents externally from OneDrive. This policy can detect file-sharing activities and send alerts when files are shared with external users, which meets the requirement.

NEW QUESTION 77
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type
Group1	Microsoft 365
Group2	Security

The subscription contains the resources shown in the following table.

Name	Type
Site1	Microsoft SharePoint Online site
Team1	Microsoft Teams team

You create a sensitivity label named Label1.
You need to publish Label1 and have the label apply automatically.
To what can you publish Label1, and to what can Label1 be auto-applied? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Publish to:
- Site1 only
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- Group1, Group2, Site1, and Team1

Auto-apply to:
- Site1 only
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- Group1, Group2, Site1, and Team1

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: Publishing a Sensitivity Label
Sensitivity labels can be published to Microsoft 365 groups, security groups, SharePoint
Online sites, and Microsoft Teams. Since we have: Group1 (Microsoft 365 group) - Supported Group2 (Security group) - Supported
Site1 (SharePoint Online site) - Supported Team1 (Microsoft Teams team) - Supported
This means we can publish Label1 to Group1, Group2, Site1, and Team1. Box 2: Auto-Applying a Sensitivity Label
Auto-apply policies for sensitivity labels work on: SharePoint Online sites (documents)
OneDrive (documents) Exchange email (messages)
However, labels cannot be auto-applied to Microsoft 365 groups or Teams directly because labels are applied to files and emails, not to groups or Teams as entities. Since Site1 (a SharePoint Online site) supports auto-apply, it is the correct option.

NEW QUESTION 81
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SC-401 Exam with Our Prep Materials Via below:

https://www.certleader.com/SC-401-dumps.html