Microsoft

Exam Questions SC-401

Administering Information Security in Microsoft 365

NEW QUESTION 1
DRAG DROP - (Topic 1)
You need to meet the technical requirements for the Site1 documents.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The goal is to automatically label documents in Site1 that contain credit card numbers. To achieve this, we need a sensitivity label with an auto-labeling policy based on a sensitive
info type that detects credit card numbers.
Step 1: Create a Sensitive Info Type
A sensitive info type is needed to detect credit card numbers in documents.
Microsoft Purview includes built-in sensitive info types for credit card numbers, but we can also create a custom one if necessary.
Step 2: Create a Sensitivity Label
A sensitivity label is required to classify and protect documents containing sensitive information.
This label can apply encryption, watermarking, or access controls to credit card data.
Step 3: Create an Auto-Labeling Policy
An auto-labeling policy ensures that the sensitivity label is applied automatically when credit card numbers are detected in Site1.
This policy is configured to scan files and automatically apply the correct sensitivity label.

NEW QUESTION 2
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.

Answer Area

Number of files that User1 can access:

- 1
- 2
- 3
- 4

Number of files that User2 can access:

- 1
- 2
- 3
- 4

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

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

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

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

Answer: B

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

NEW QUESTION 4
- (Topic 2)
You have a Microsoft 365 tenant.
You have a database that stores customer details. Each customer has a unique 13-digit identifier that consists of a fixed pattern of numbers and letters.
You need to implement a data loss prevention (DLP) solution that meets the following
requirements:
Email messages that contain a single customer identifier can be sent outside your company.
Email messages that contain two or more customer identifiers must be approved by the company's data privacy team.
Which two components should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: BC

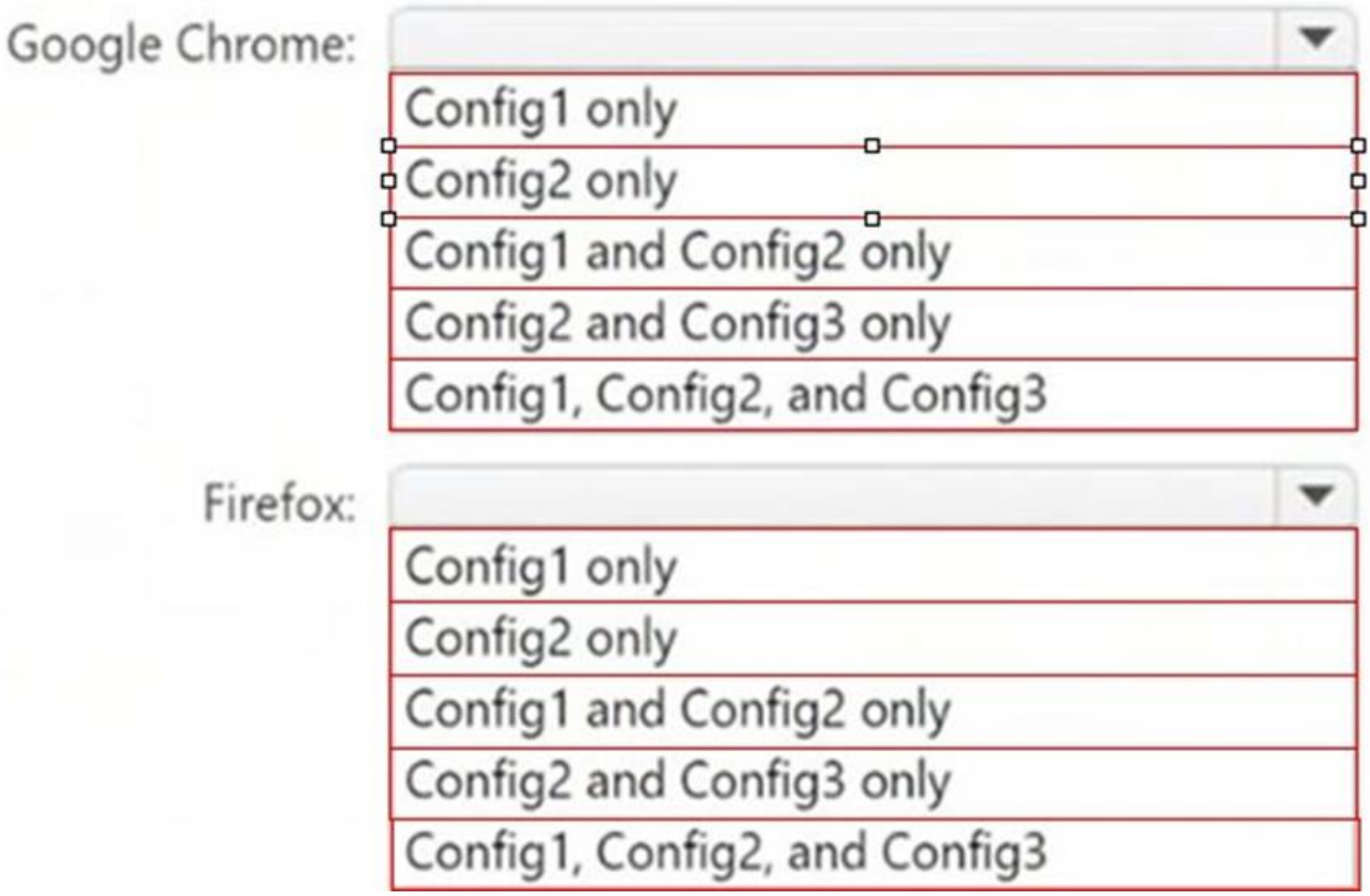
Explanation:
You need to define a custom sensitive information type that recognizes the unique 13-digit identifier format for customer records. Microsoft Purview DLP policies use these types to identify and protect sensitive data.
A Data Loss Prevention (DLP) policy is required to enforce the rules. It will allow emails with a single identifier but trigger an approval workflow when two or more identifiers are detected.

NEW QUESTION 5
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription that contains the device configurations shown in the following table.

Name	Platform
Config1	Windows 11
Config2	macOS
Config3	Android

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

Answer Area



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 6
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription that contains three DOCX files named File1, File2, and File3.
You create the sensitivity labels shown in the following table.

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

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

File	Label
File1	*None*
File2	Label1
File3	Label2

You ask Microsoft 365 Copilot to summarize the files, and you receive the results shown in the following table.

Name	Based on content of
Summary1	File1, File3
Summary2	File2
Summary3	File1, File2, File3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	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 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.

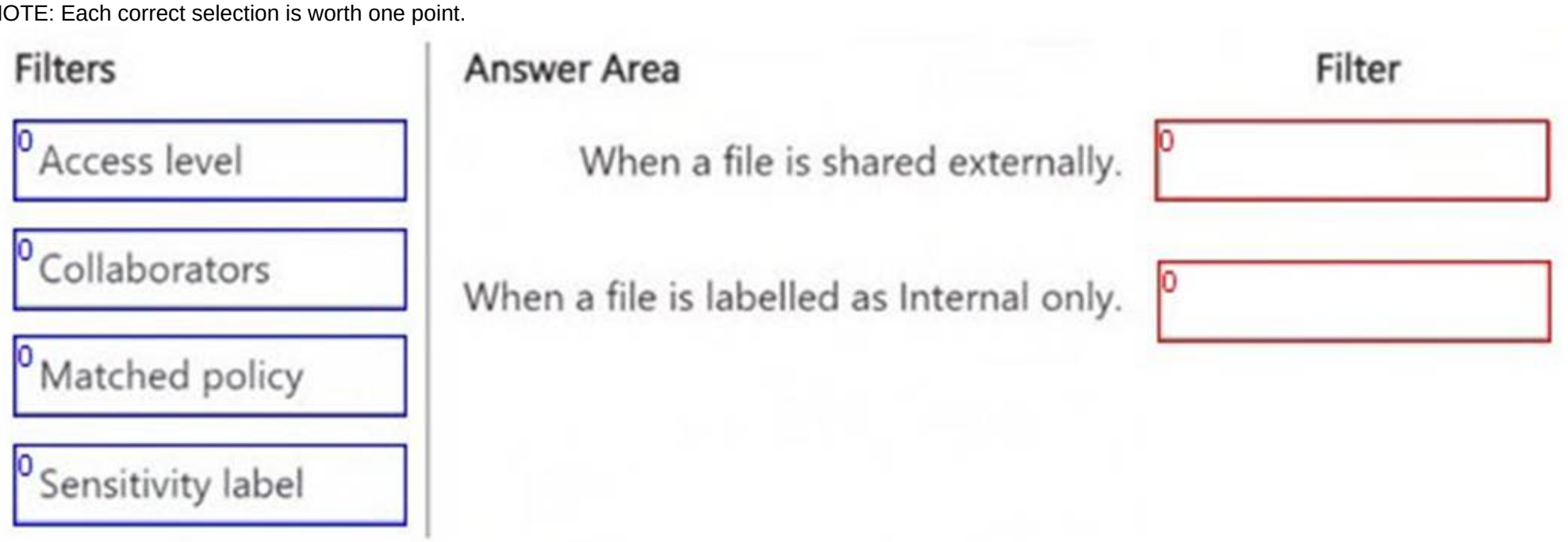
NEW QUESTION 8
- (Topic 2)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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.

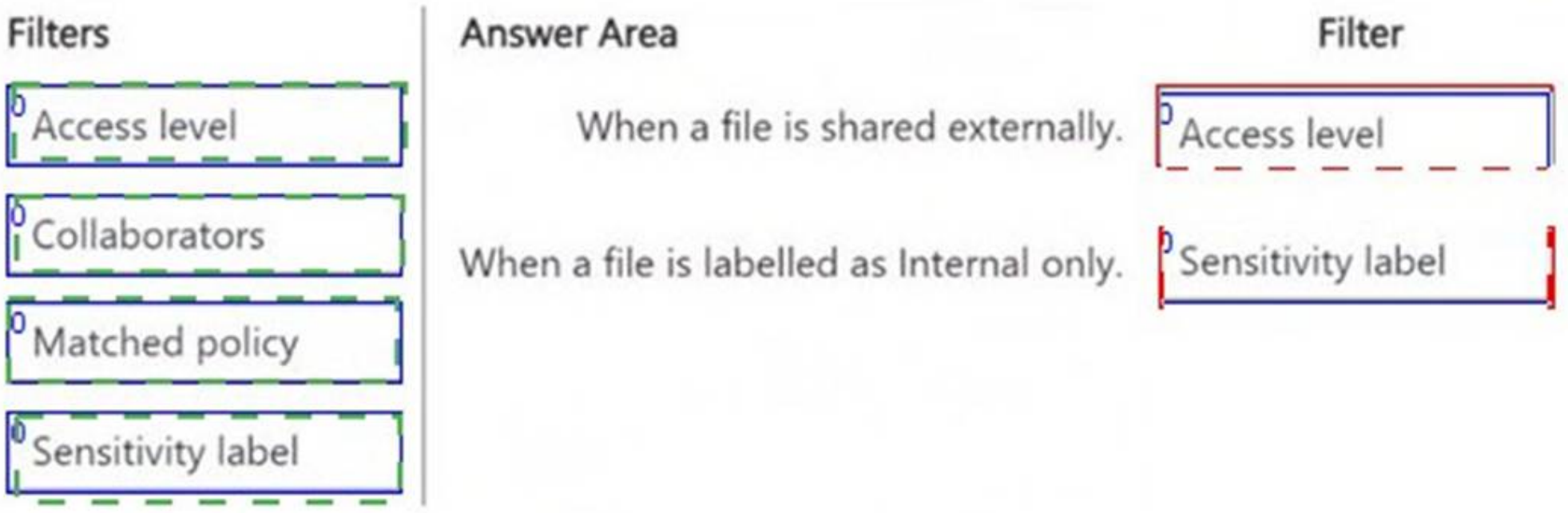
NEW QUESTION 9
DRAG DROP - (Topic 2)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You plan to deploy a Defender for Cloud Apps file policy that will be triggered when the following conditions are met:
A file is shared externally.
A file is labeled as internal 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
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription that uses Microsoft Purview and just-in-time (JIT) protection. The subscription contains the users shown in the following table.

Name	JIT protection scope
User1	Included
User2	Not configured
User3	Included

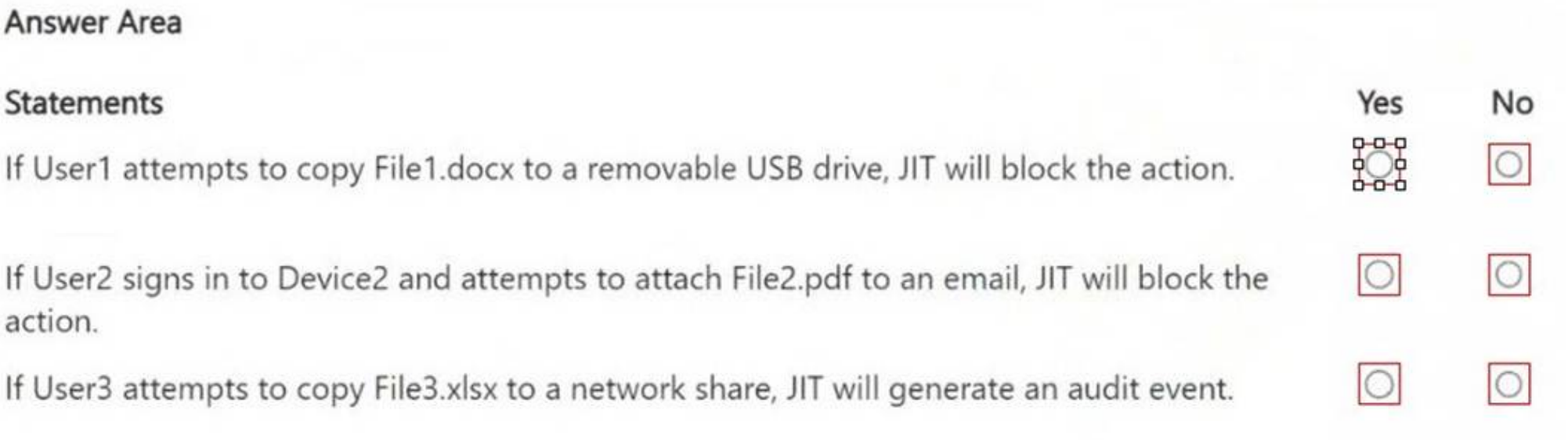
The subscription contains the devices shown in the following table.

Name	Microsoft Defender
Device1	Onboarded
Device2	Onboarded
Device3	Not onboarded

The devices contain the files shown in the following table.

Name	File classification evaluation status	Location
File1.docx	Not evaluated	Device1
File2.pdf	Evaluated	Device2
File3.xlsx	Not evaluated	Device3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



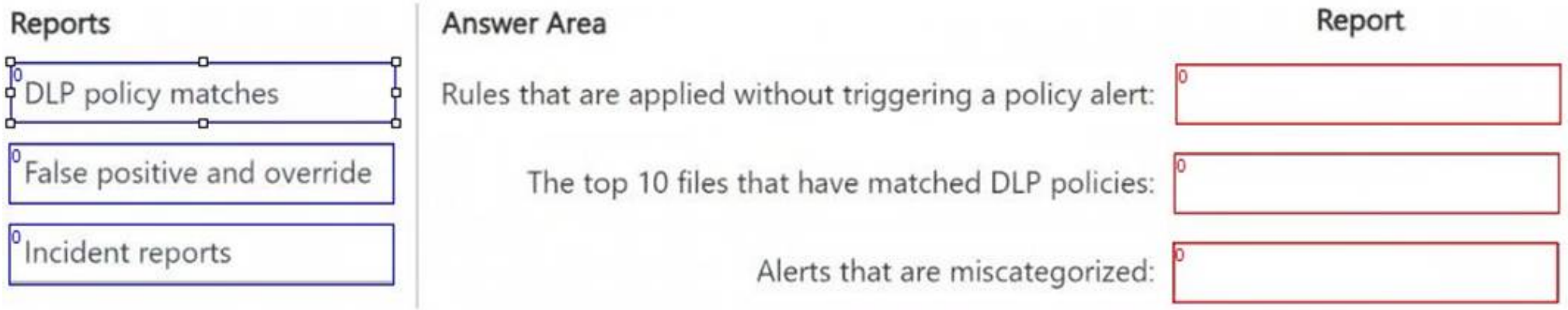
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Statement 1 - No. User1 is included in JIT protection. File1.docx is on Device1, which is onboarded to Microsoft Defender. However, File1.docx has not been evaluated for file classification, meaning JIT cannot enforce protection on it. If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.
Statement 2 - No. User2 is not configured for JIT protection (JIT does not apply to them). File2.pdf has been evaluated for classification, but since User2 is not

included in JIT protection, no blocking occurs. If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.
Statement 3 - No. User3 is included in JIT protection. However, Device3 is not onboarded to Microsoft Defender, meaning JIT protection cannot enforce actions on it. File3.xlsx has not been evaluated, so even if the device were onboarded, JIT would not have classification data to act upon.

NEW QUESTION 10
DRAG DROP - (Topic 2)
You have a Microsoft 365 subscription that contains 20 data loss prevention (DLP) policies. You need to identify the following:
Rules that are applied without triggering a policy alert The top 10 files that have matched DLP policies Alerts that are miscategorized
Which report should you use for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report 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:
The False positive and override report helps identify rules that were applied but did not generate an actual policy alert, which means they were overridden or deemed false positives.
The DLP policy matches report provides details on files that matched DLP policies, including the top 10 files.
The Incident reports report helps analyze and review alerts, including those that may have been miscategorized.

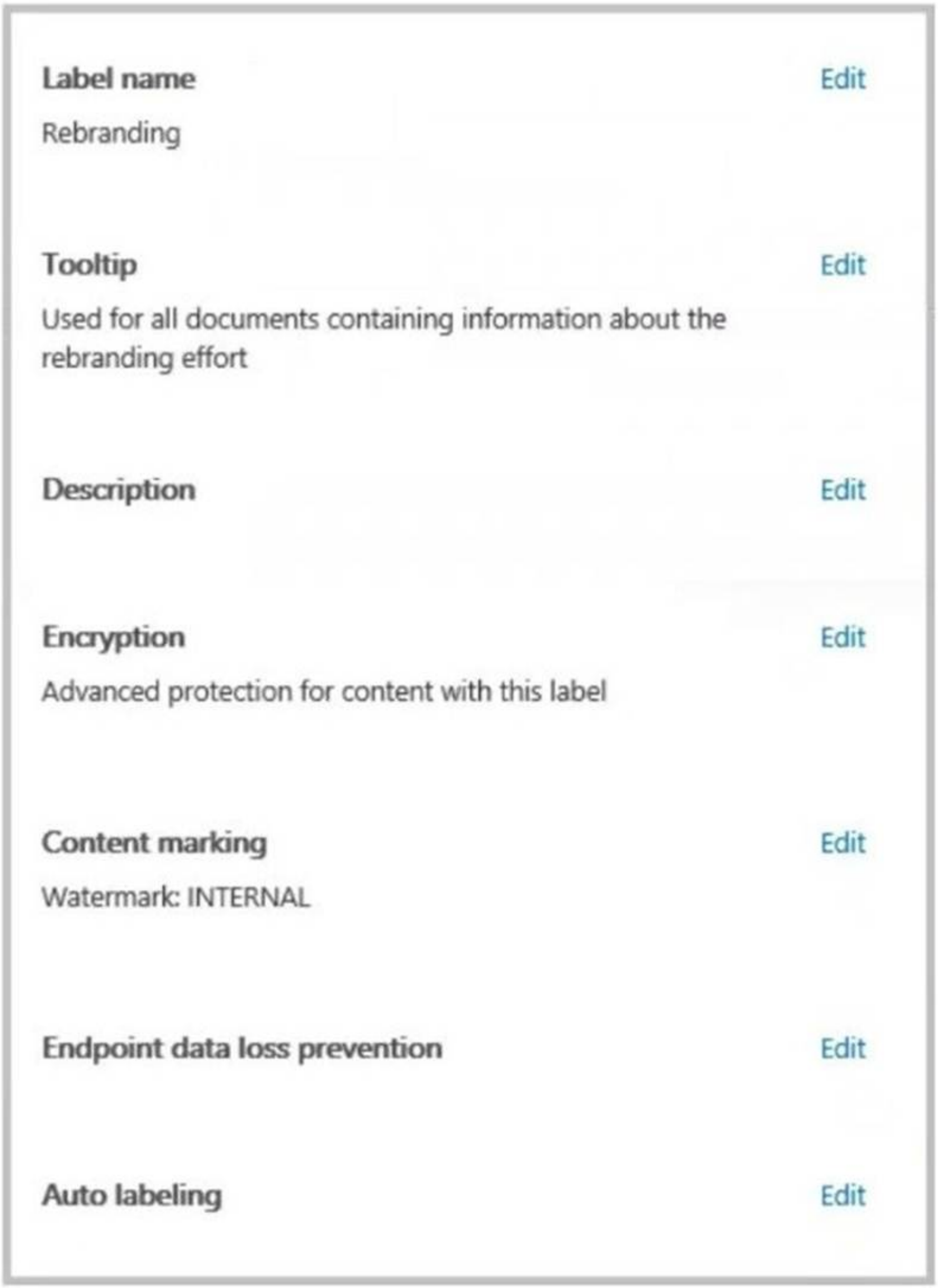
NEW QUESTION 12
- (Topic 2)
You are creating a data loss prevention (DLP) policy that will apply to all available locations except Fabric and Power BI workspaces.
You configure an advanced DLP rule in the policy. Which type of condition can you use in the rule?

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 13
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 15
- (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 18
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription.
You need to identify documents that contain patent application numbers containing the letters PA followed by eight digits, for example, PA 12345678. The solution must minimize administrative effort.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To identify the documents, use a data classification of: [▼]
- Exact data match (EDM)
- Sensitive info type
- Trainable classifier

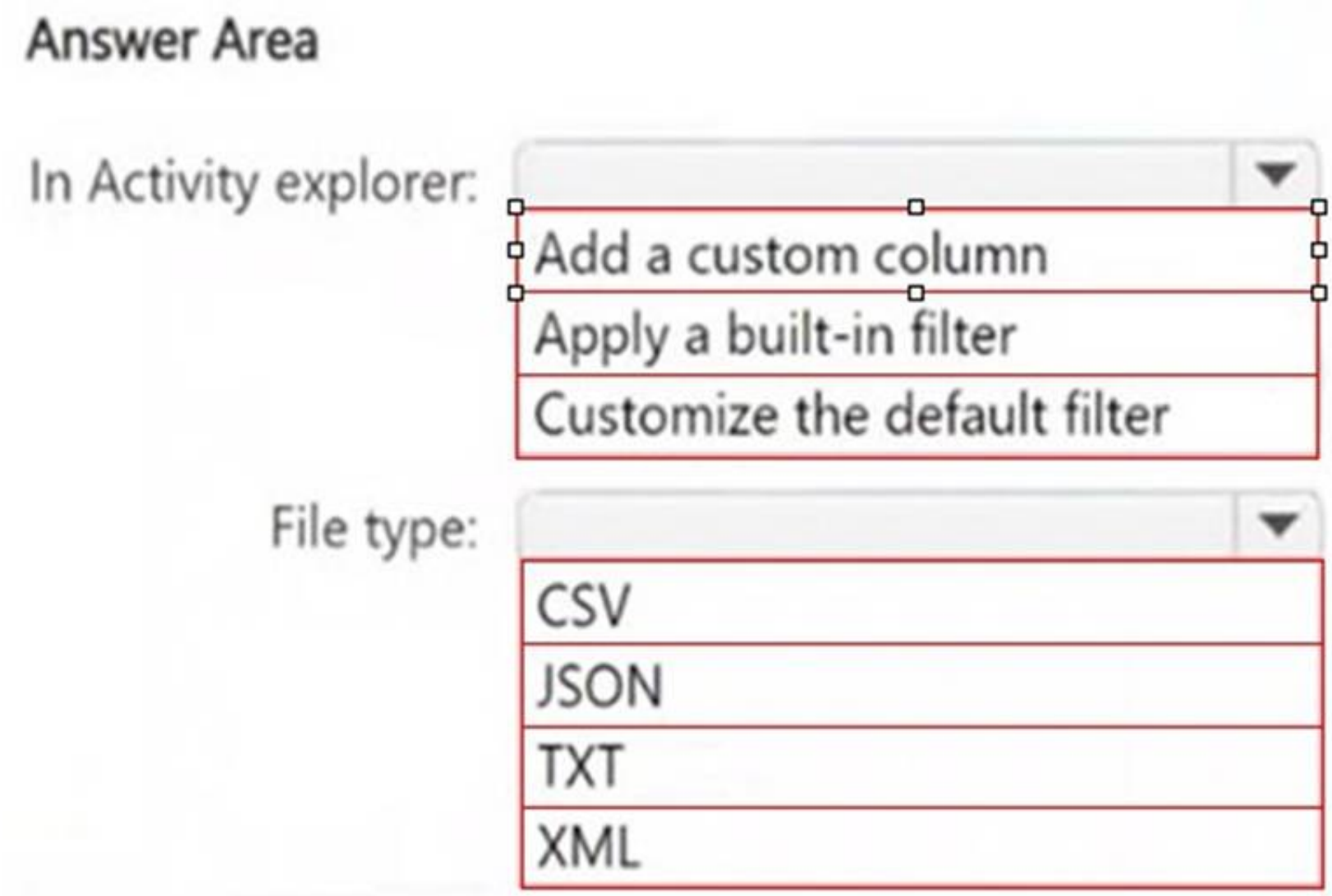
Configure data classifications by using a: [▼]
- Keyword dictionary
- Regular expression
- Function

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Since you are looking for a specific pattern (PA followed by eight digits, e.g., PA 12345678), the best classification method is Sensitive Info Type. Sensitive Info Types allow pattern-based matching to identify structured data. Exact Data Match (EDM) is not needed because you're not comparing against a fixed dataset. Trainable classifier is not appropriate because this is a structured pattern, not an unstructured document classification.
Box 2: Since PA 12345678 follows a structured pattern, the most effective method is Regular Expression (Regex). A Regular Expression (Regex) can be written to match "PA" followed by exactly eight digits (e.g., PA\s\d{8}). Keyword dictionary is not ideal because it works for predefined words, not number patterns. Function is unnecessary because there is no need for checksum validation or predefined validation rules.

NEW QUESTION 19
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.



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 21
- (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 22
- (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 25
- (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.

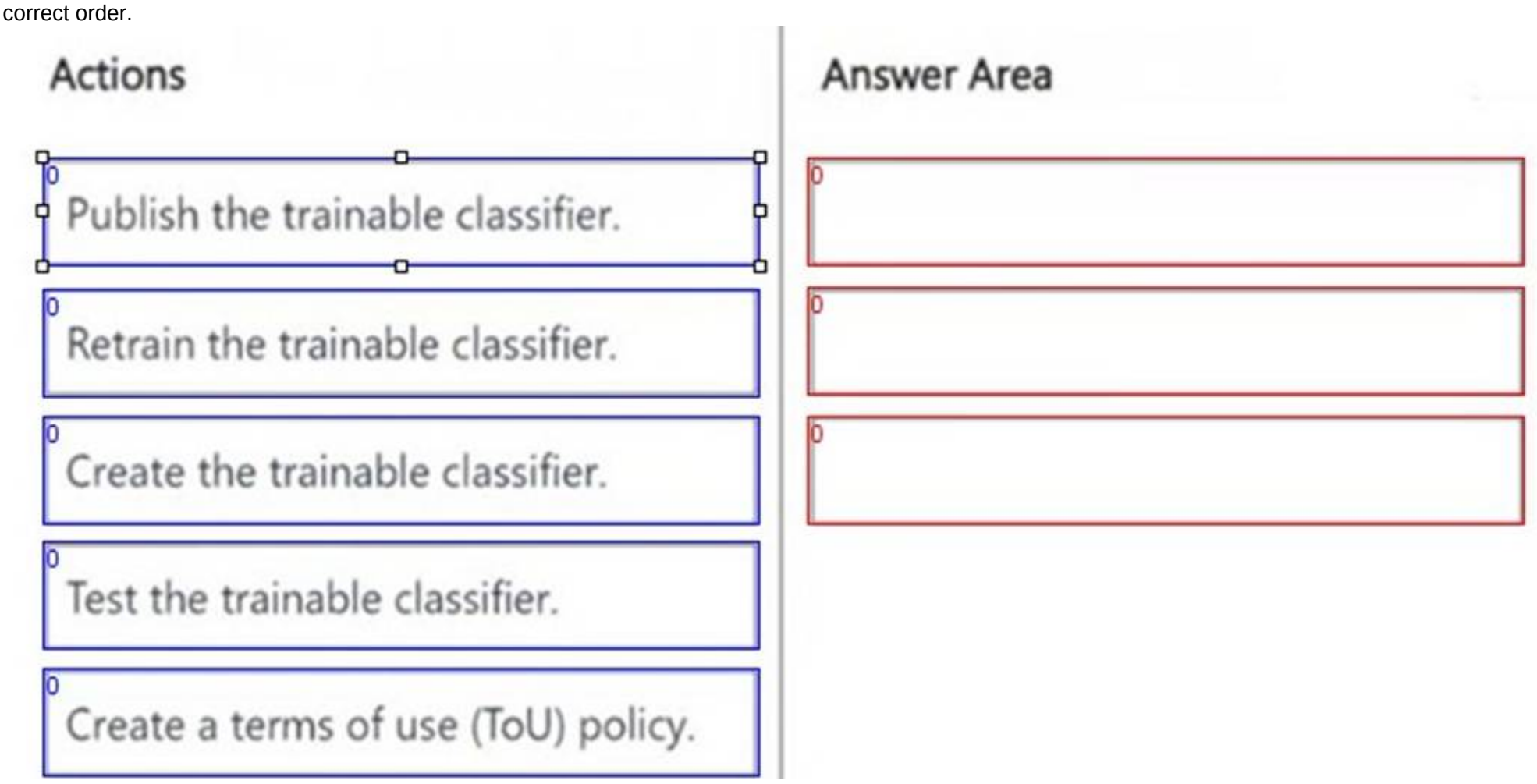
NEW QUESTION 30
- (Topic 2)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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 31
DRAG DROP - (Topic 2)
You need to create a trainable classifier that can be used as a condition in an auto-apply retention label policy.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
To create a trainable classifier that can be used in an auto-apply retention label policy, you need to follow these key steps:
* 1. Create the trainable classifier
This is the first step where you define the classifier, specifying the types of content it should identify.
* 2. Test the trainable classifier
Before using the classifier in production, you need to validate its accuracy by testing it against sample documents to ensure it correctly classifies the intended data.
* 3. Publish the trainable classifier
Once testing is successful, you must publish the classifier so that it can be used in policies like auto-apply retention labels in Microsoft Purview.

NEW QUESTION 34
- (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 the text patterns. 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.
Text patterns in mail flow rules are not as reliable as sensitive information types in DLP. Mail flow rules lack advanced content detection and machine learning-based classification, making them less effective than DLP.

NEW QUESTION 37

- (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 38
- (Topic 2)
You have a Microsoft 365 E5 subscription.
You need to enable support for sensitivity labels in Microsoft SharePoint Online. What should you use?

A. the Microsoft Purview portal
B. the Microsoft Entra admin center
C. the SharePoint admin center
D. the Microsoft 365 admin center

Answer: C

Explanation:
To enable support for sensitivity labels in Microsoft SharePoint Online, you must configure the setting in the SharePoint admin center.
Sensitivity labels in SharePoint Online allow labeling and protection of files stored in SharePoint and OneDrive. This feature must be enabled in the SharePoint admin center Settings Information protection to allow sensitivity labels to apply encryption and protection to stored documents.

NEW QUESTION 40
- (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 45
- (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 49
- (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 50
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

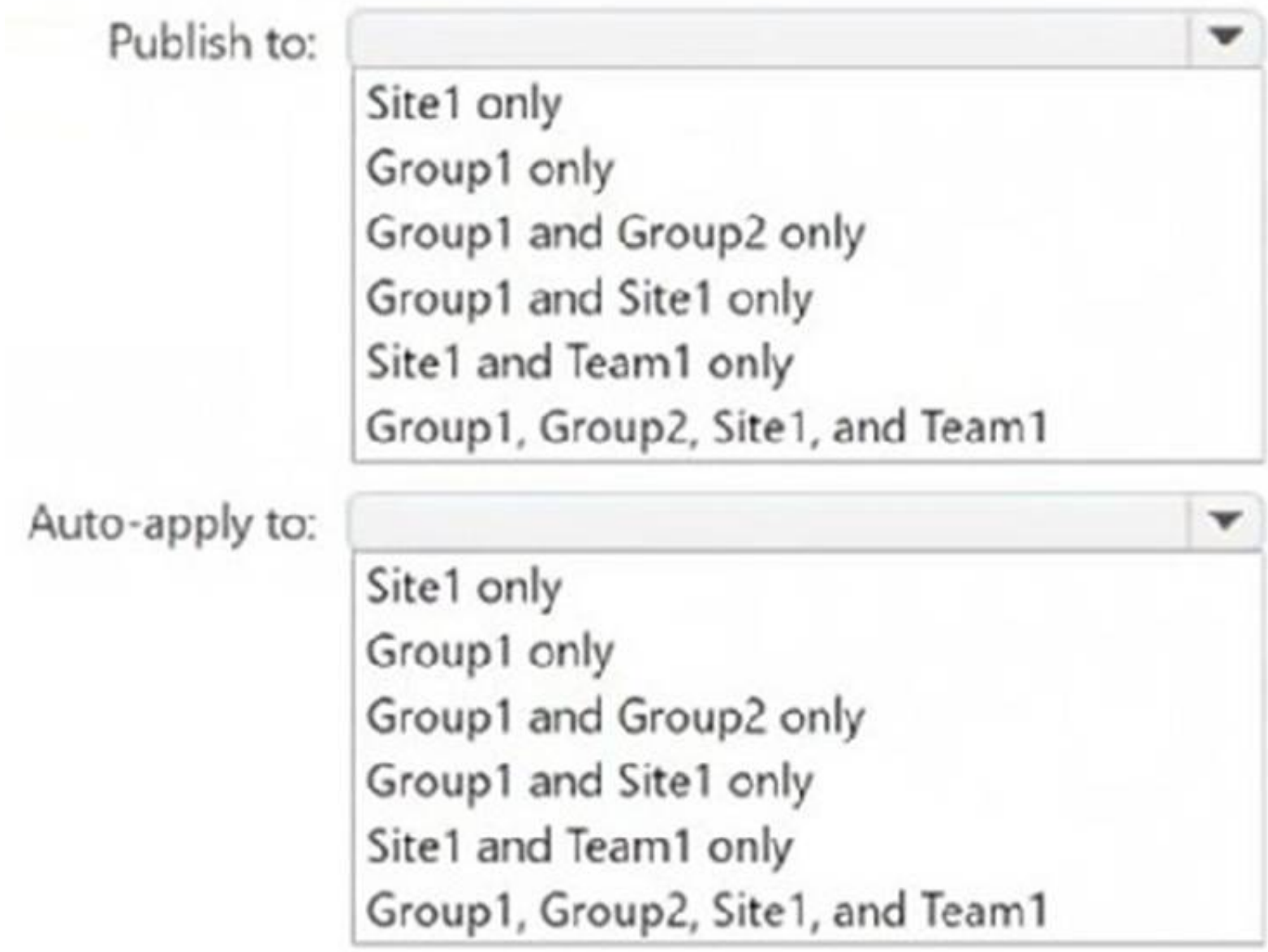
Name	Type
Group1	Microsoft 365
Group2	Security

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



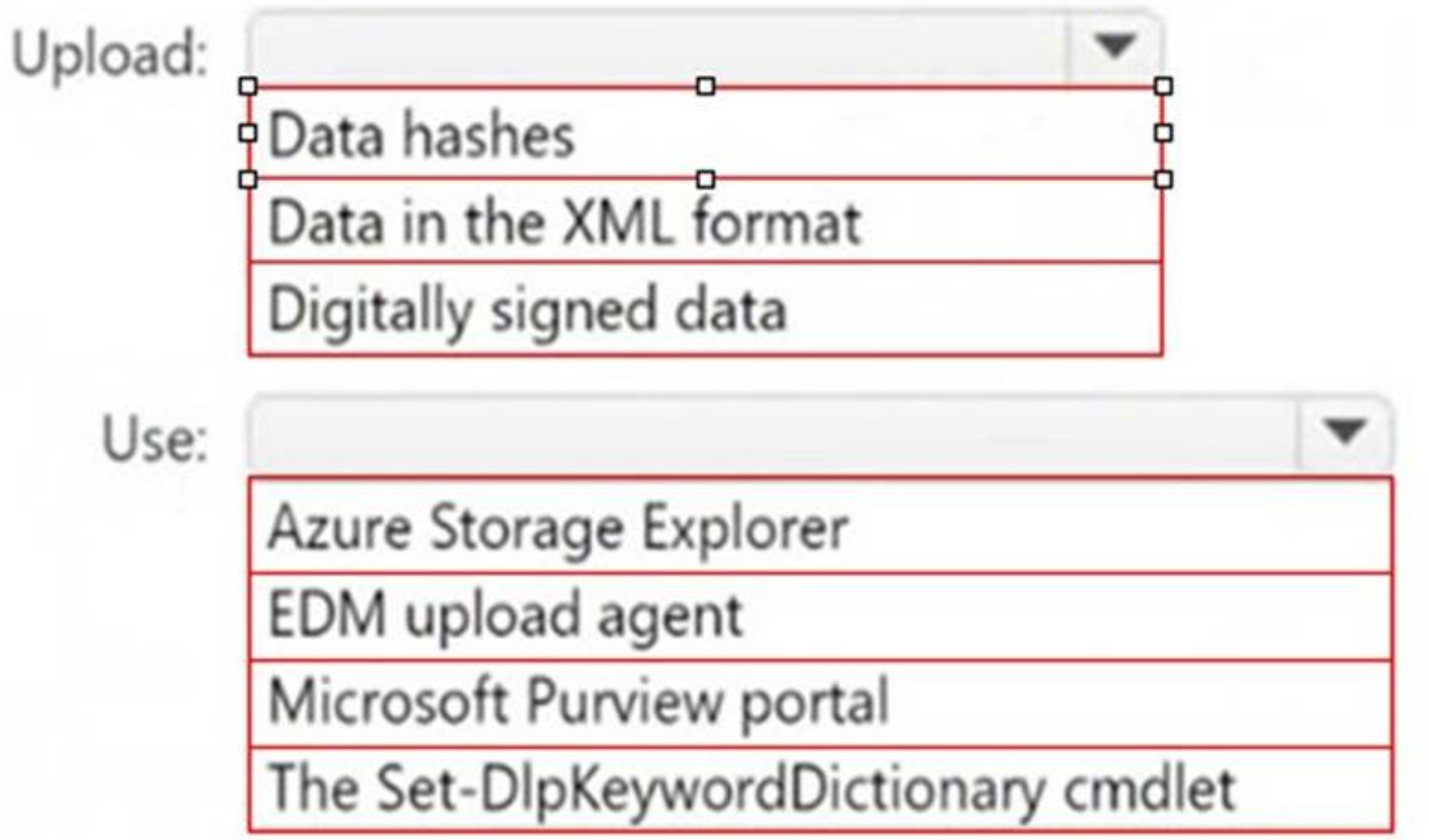
A. Mastered
B. Not Mastered

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 52
HOTSPOT - (Topic 2)
You plan to create a custom sensitive information type that will use Exact Data Match (EDM).
You need to identify what to upload to Microsoft 365, and which tool to use for the upload. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 54
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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