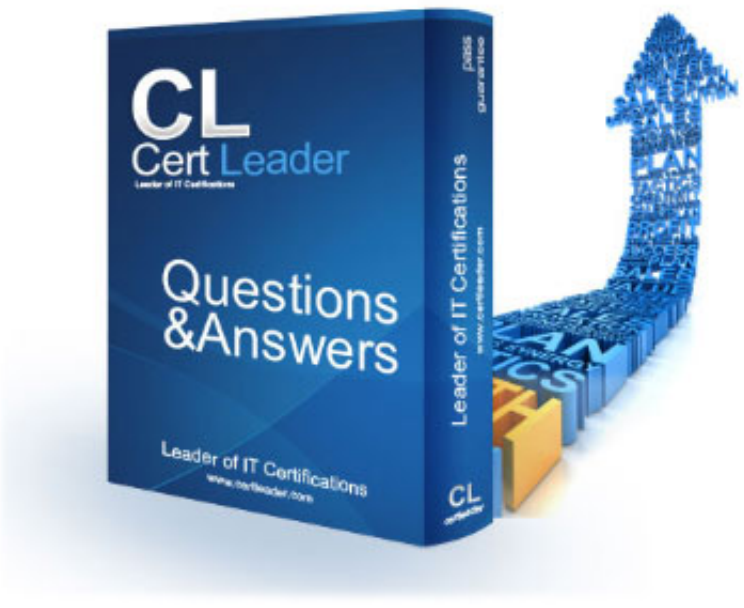
SC-401 Dumps

Administering Information Security in Microsoft 365

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



NEW QUESTION 1
- (Topic 1)
You need to meet the technical requirements for the creation of the sensitivity labels. To which user or users must you assign the Sensitivity Label Administrator role?

A. Admin1 only
B. Admin1 and Admin4 only
C. Admin1 and Admin5 only
D. Admin1, Admin2, and Admin3 only
E. Admin1, Admin2, Admin4, and Admin5 only

Answer: D

Explanation:
To meet the requirement that all administrative users must be able to create Microsoft 365 sensitivity labels, we need to assign the Sensitivity Label Administrator role to the correct users.
Sensitivity Label Administrator Role Responsibilities
This role allows users to:
Create and manage sensitivity labels in Microsoft Purview. Publish and configure auto-labeling policies.
Modify label encryption and content marking settings.
Review of Admin Roles from the Table:

Admin	Role Assigned	Can Create Sensitivity Labels?
Admin1	Global Reader	□ No, read-only permissions.
Admin2	Compliance Data Administrator	□ Yes, can manage compliance data, including labels.
Admin3	Compliance Administrator	□ Yes, has full compliance management, including labels.
Admin4	Security Operator	□ No, this role is focused on security alerts and response.
Admin5	Security Administrator	□ No, primarily focused on security policies and threat management.

Users that must be assigned the Sensitivity Label Administrator role: Admin2 (Compliance Data Administrator)
Admin3 (Compliance Administrator)
Admin1 (Global Reader) (should be assigned this role to fulfill the requirement that all admins can create labels).

NEW QUESTION 2
HOTSPOT - (Topic 1)
You are reviewing policies for the SharePoint Online environment.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	○	○
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2023.	○	○
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2026.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
AI-generated content may be incorrect. Understanding Site4's Retention Policies:
Site4RetentionPolicy1 deletes items older than 2 years from creation. If a file was created on January 1, 2021, it would be deleted after January 1, 2023.
Site4RetentionPolicy2 retains files for 4 years from creation. If a file was created on January 1, 2021, it will be kept until January 1, 2025, but not deleted after that (policy states "Do nothing").
Statement 1 - Yes, because Site4RetentionPolicy2 ensures files are retained for 4 years. Statement 2 - Yes, because Site4RetentionPolicy2 retains the file for 4 years (until January 1, 2025).
Statement 3 - No, because retention is only for 4 years (until January 1, 2025). After that, the policy does "nothing," meaning the file is no longer recoverable after that period.

NEW QUESTION 3
- (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

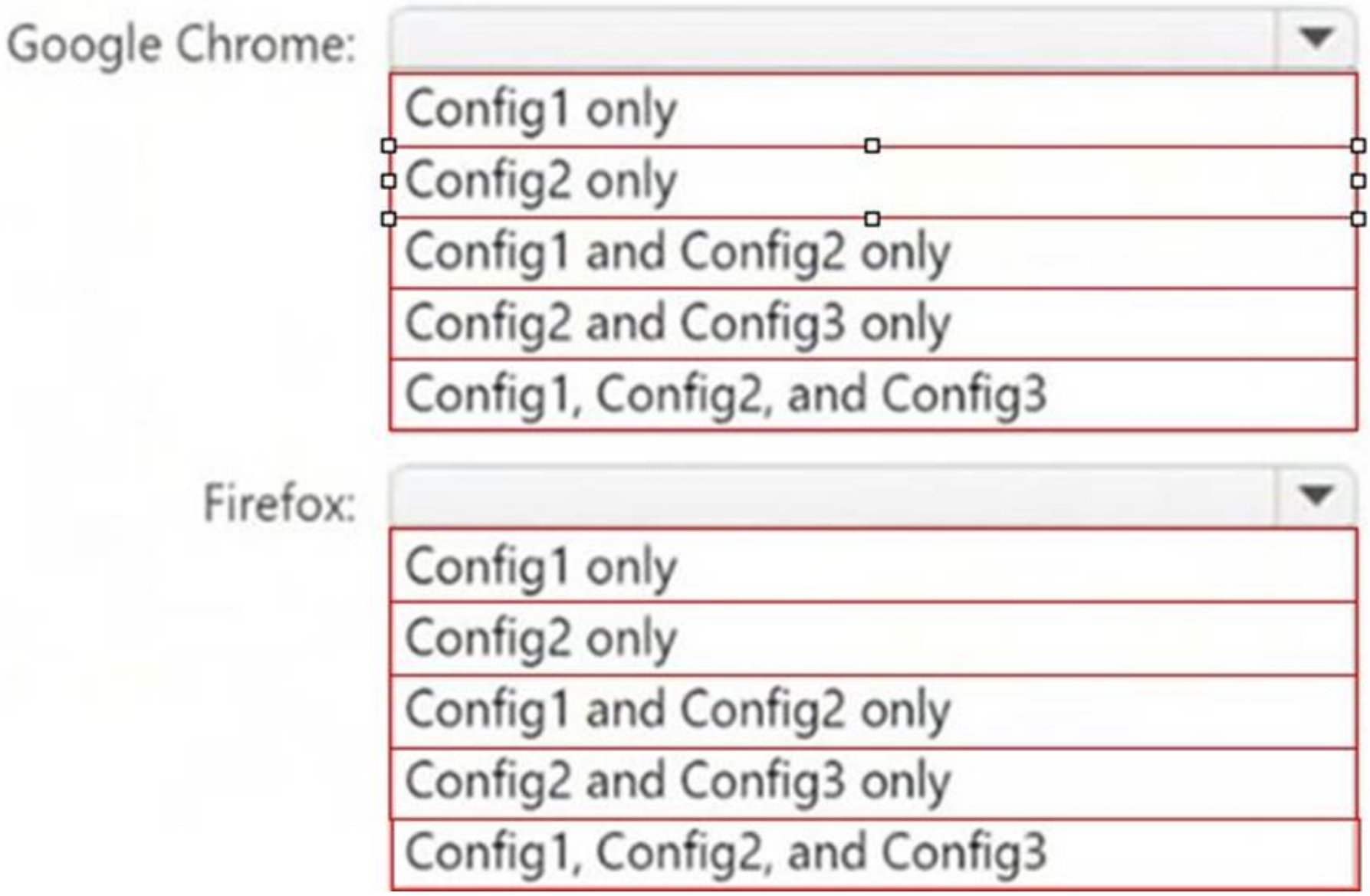
Explanation:
You need to define a custom sensitive information type that recognizes the unique 13-digit identifier format for customer records. Microsoft Purview DLP policies use these types to identify and protect sensitive data.
A Data Loss Prevention (DLP) policy is required to enforce the rules.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

NEW QUESTION 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

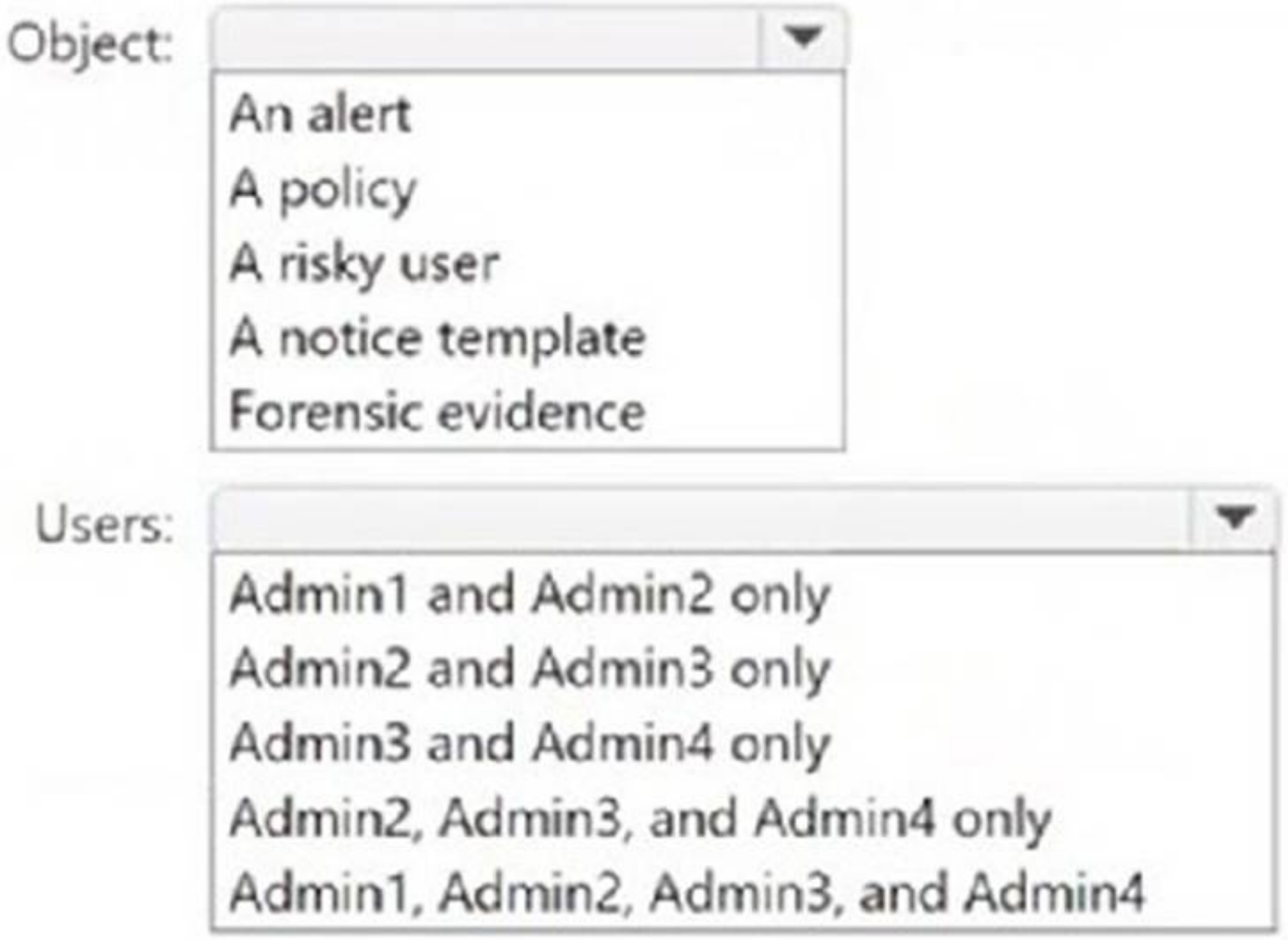
Explanation:
Microsoft Purview browser extensions for Endpoint DLP are supported on: Windows 10/11 (Config1)
macOS (Config2)
Not supported on Android (Config3)
Since Microsoft Purview does not support browser extensions on Android, Config3 is excluded from both Google Chrome and Firefox.

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

Name	Role group
Admin1	Insider Risk Management Admins
Admin2	Insider Risk Management Analysts
Admin3	Risk Management Investigators
Admin4	Insider Risk Management Auditors

You plan to create a Microsoft Purview insider risk management case named Case1. Which insider risk management object should you select first, and which users will be
added as contributors for Case1 by default?
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: When creating a Microsoft Purview Insider Risk Management case, you must first select a risky user to investigate. The case will be built around this specific user??s activities, linking alerts and risk signals to the investigation.
Box 2: The Insider Risk Management role groups determine who can access and contribute to cases:
Admin1 (Insider Risk Management Admins) Full admin access.
Admin2 (Insider Risk Management Analysts) Analysts who review cases. Admin3 (Risk Management Investigators) Investigators who work on cases. Admin4 (Insider Risk Management Auditors) Auditors who oversee cases.
All these roles have default access to insider risk cases in Microsoft Purview, so all four admins are added as contributors.

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
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 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 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 9
- (Topic 2)
Your company has offices in multiple countries.
The company has a Microsoft 365 E5 subscription that uses Microsoft Purview insider risk management.
You plan to perform the following actions:
In a new country, open an office named Office1. Create a new user named User1.
Deploy insider risk management to Office1.
Add User1 to the Insider Risk Management Admins role group.
You need to ensure that User1 can perform insider risk management tasks for only the users and the devices in Office1.
What should you create first?

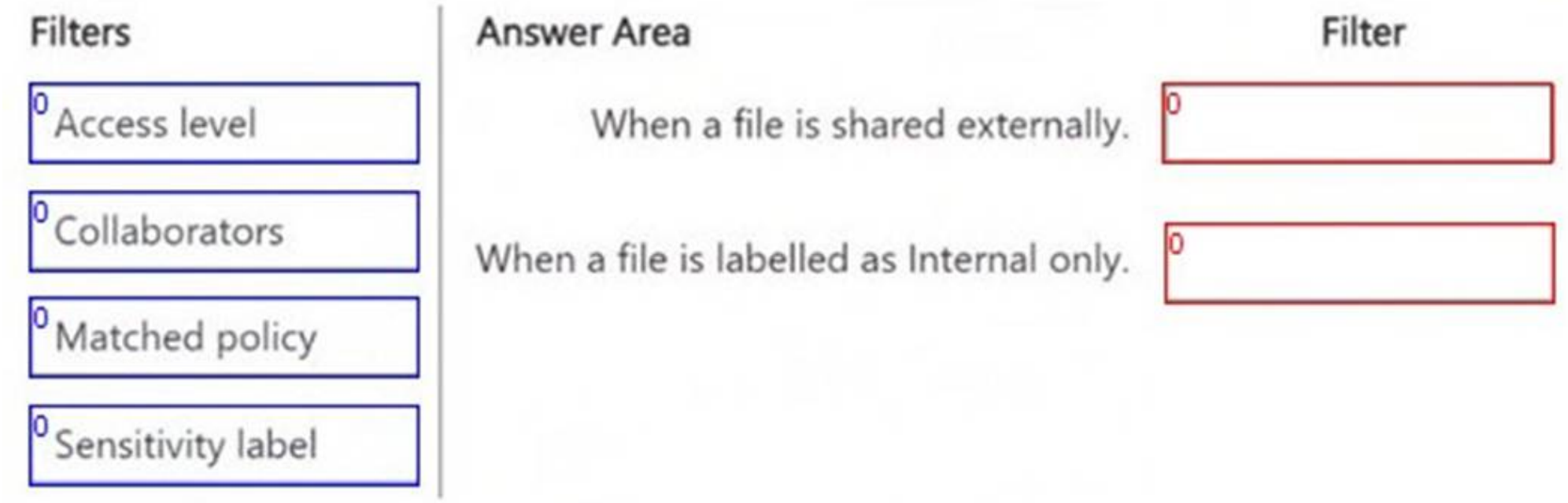
A. a dynamic device group
B. a dynamic user group
C. an administrative unit
D. a management group

Answer: C

Explanation:
To ensure User1 can perform insider risk management tasks only for the users and devices in Office1, the first step is to create an administrative unit in Microsoft Entra ID (formerly Azure AD).
Administrative units allow you to scope permissions to specific users, devices, and locations. By creating an administrative unit for Office1 and assigning User1 to

the Insider Risk Management Admins role group within that unit, User1 will only have access to users and devices in Office1.

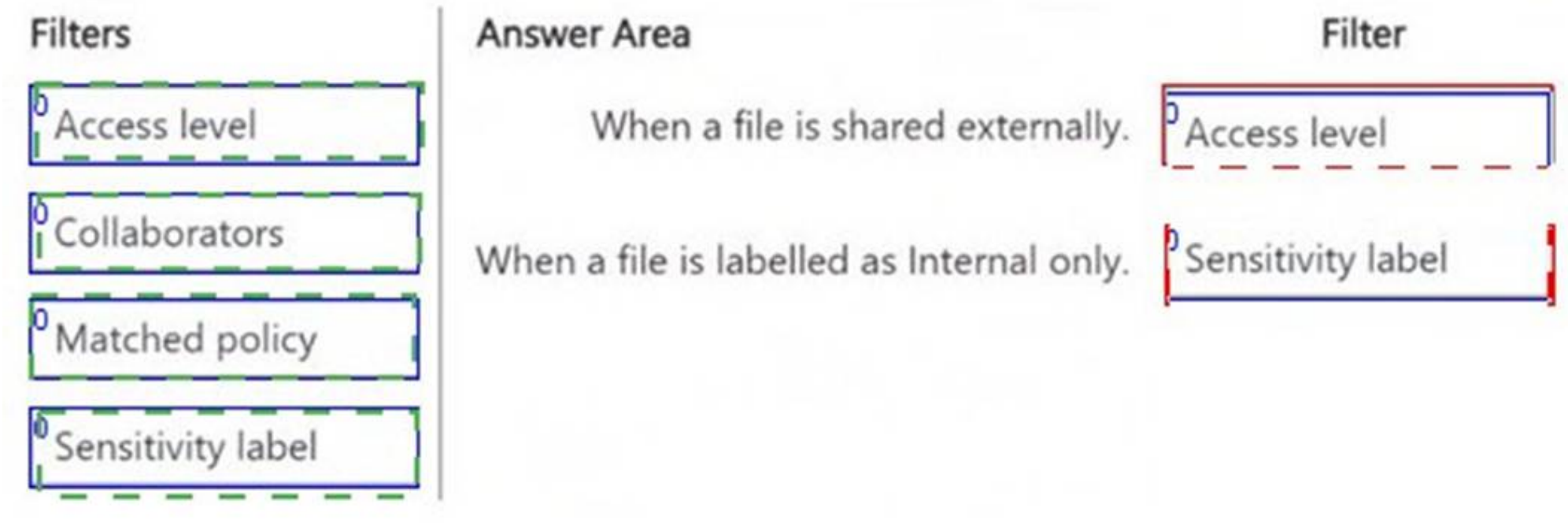
NEW QUESTION 10
DRAG DROP - (Topic 2)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You plan to deploy a Defender for Cloud Apps file policy that will be triggered when the following conditions are met:
A file is shared externally.
A file is labeled as internal 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 13
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.

Answer Area

Statements	Yes	No
If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.	○	○
If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.	○	○
If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.	○	○

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 18
- (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 21
- (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 24
- (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

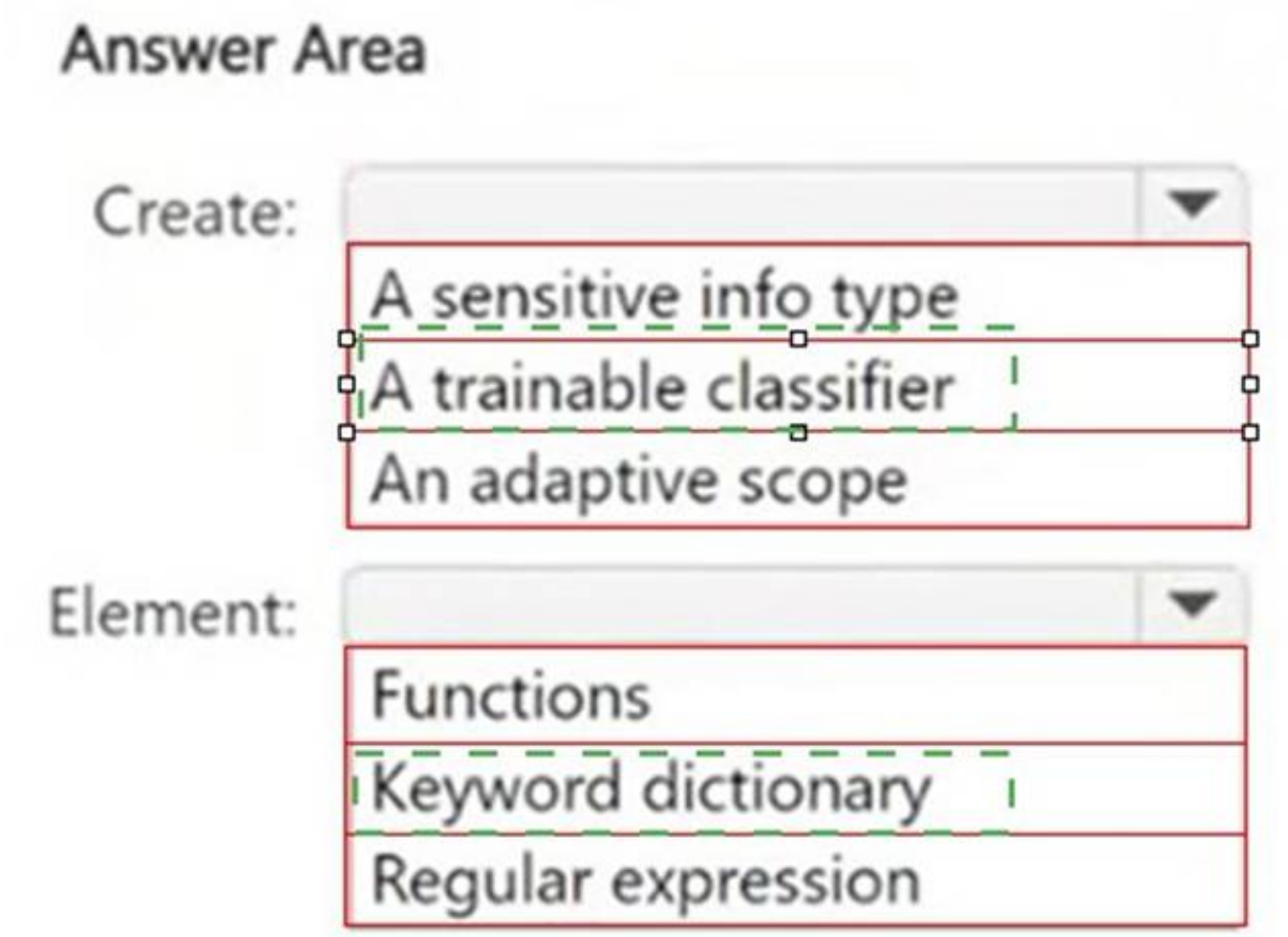
Explanation:
A Preservation Lock in Microsoft Purview Retention Policies enforces strict compliance and prevents certain modifications to ensure data is retained according to compliance requirements.
When a Preservation Lock is applied:
* 1. You cannot disable or delete the policy.
* 2. You cannot remove 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 27
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:



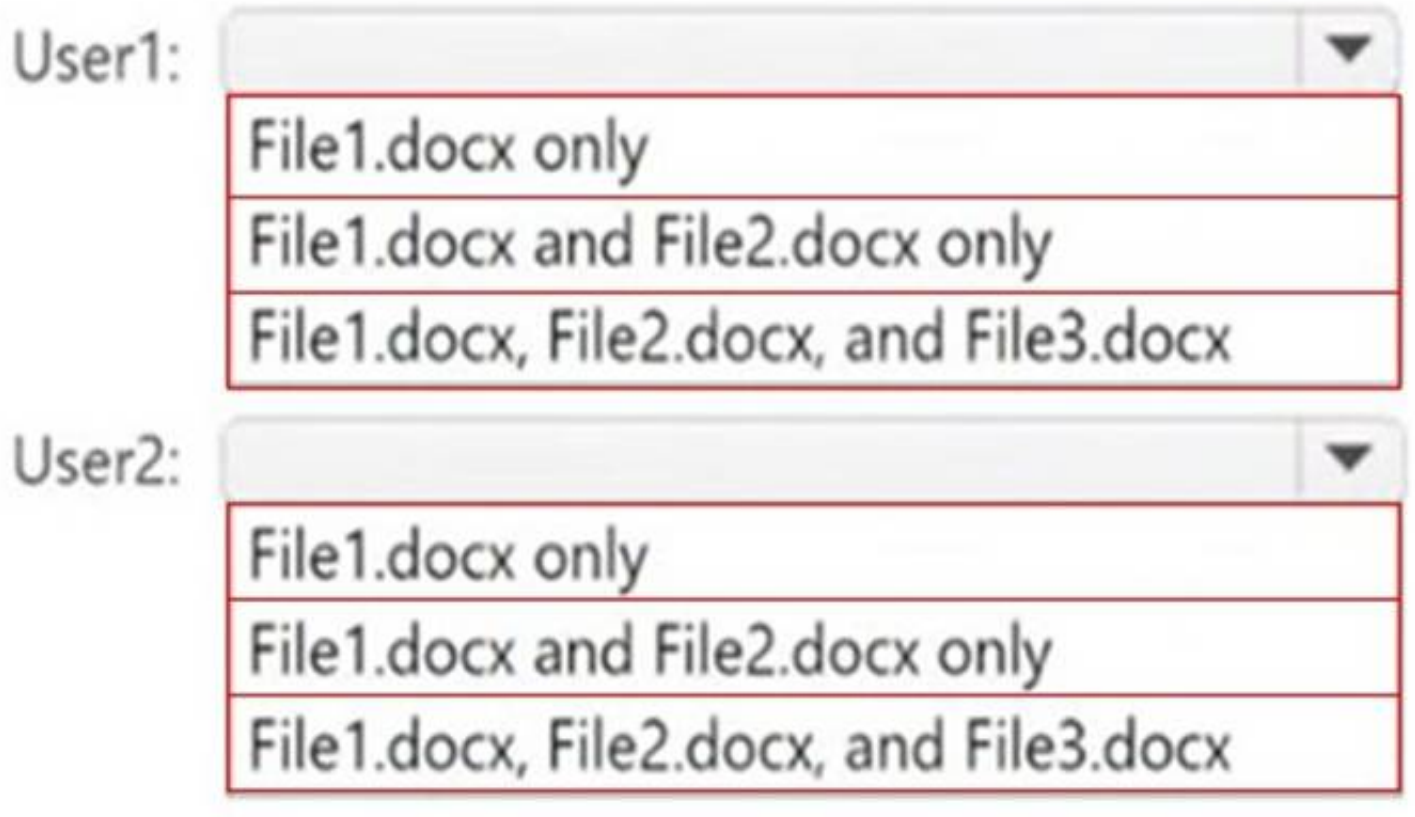
NEW QUESTION 30
HOTSPOT - (Topic 2)
You have a Microsoft SharePoint Online site that contains the following files.

Name	Modified by	Data loss prevention (DLP) action
File1.docx	Manager1	*None*
File2.docx	Manager1	Matched by DLP
File3.docx	Manager1	Blocked by DLP

Users are assigned roles for the site as shown in the following table.

Name	Role
User1	Site owner
User2	Site member

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

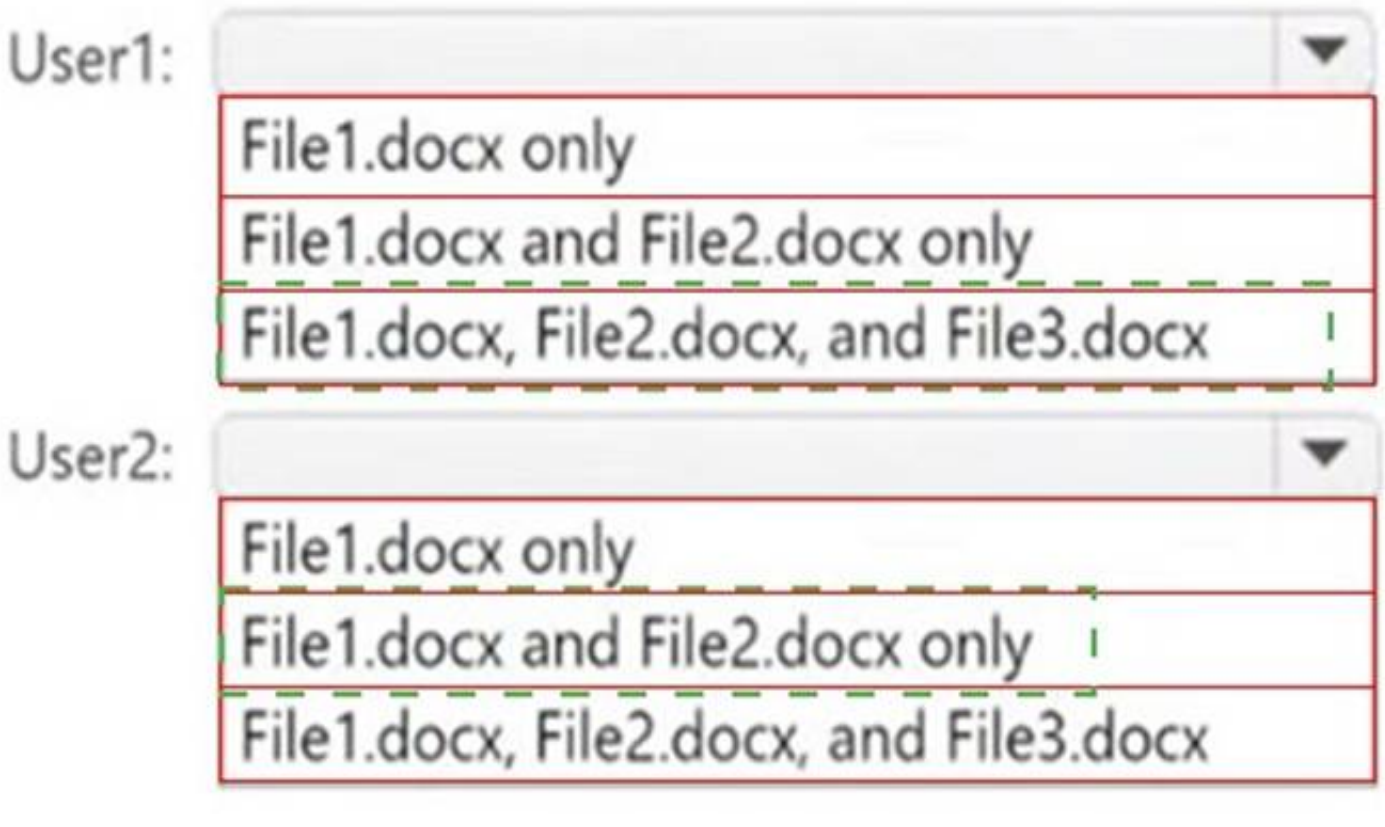


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 33
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

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.

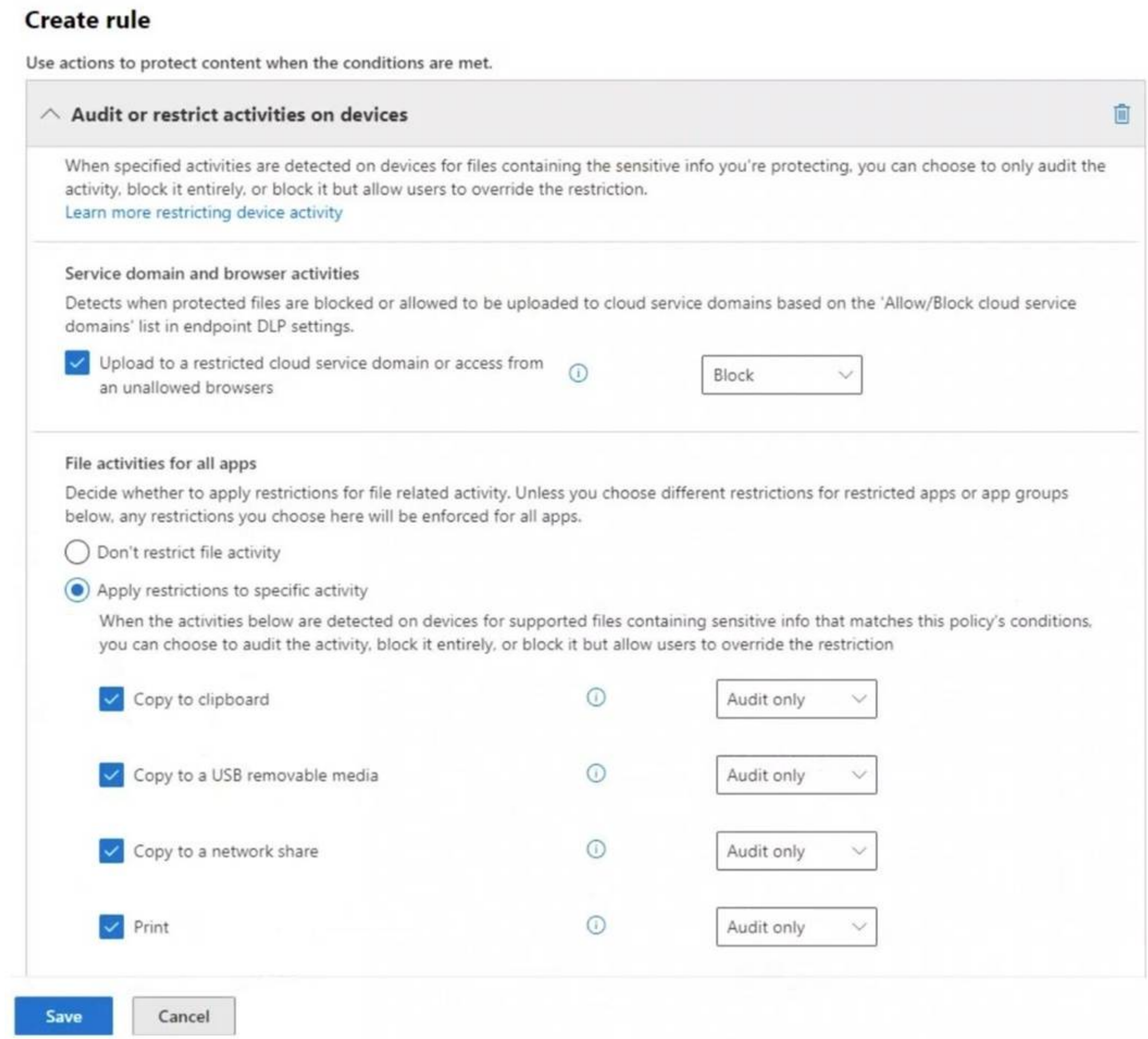
NEW QUESTION 37
- (Topic 2)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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 38
- (Topic 2)
You have a data loss prevention (DLP) policy configured for endpoints as shown in the following exhibit.



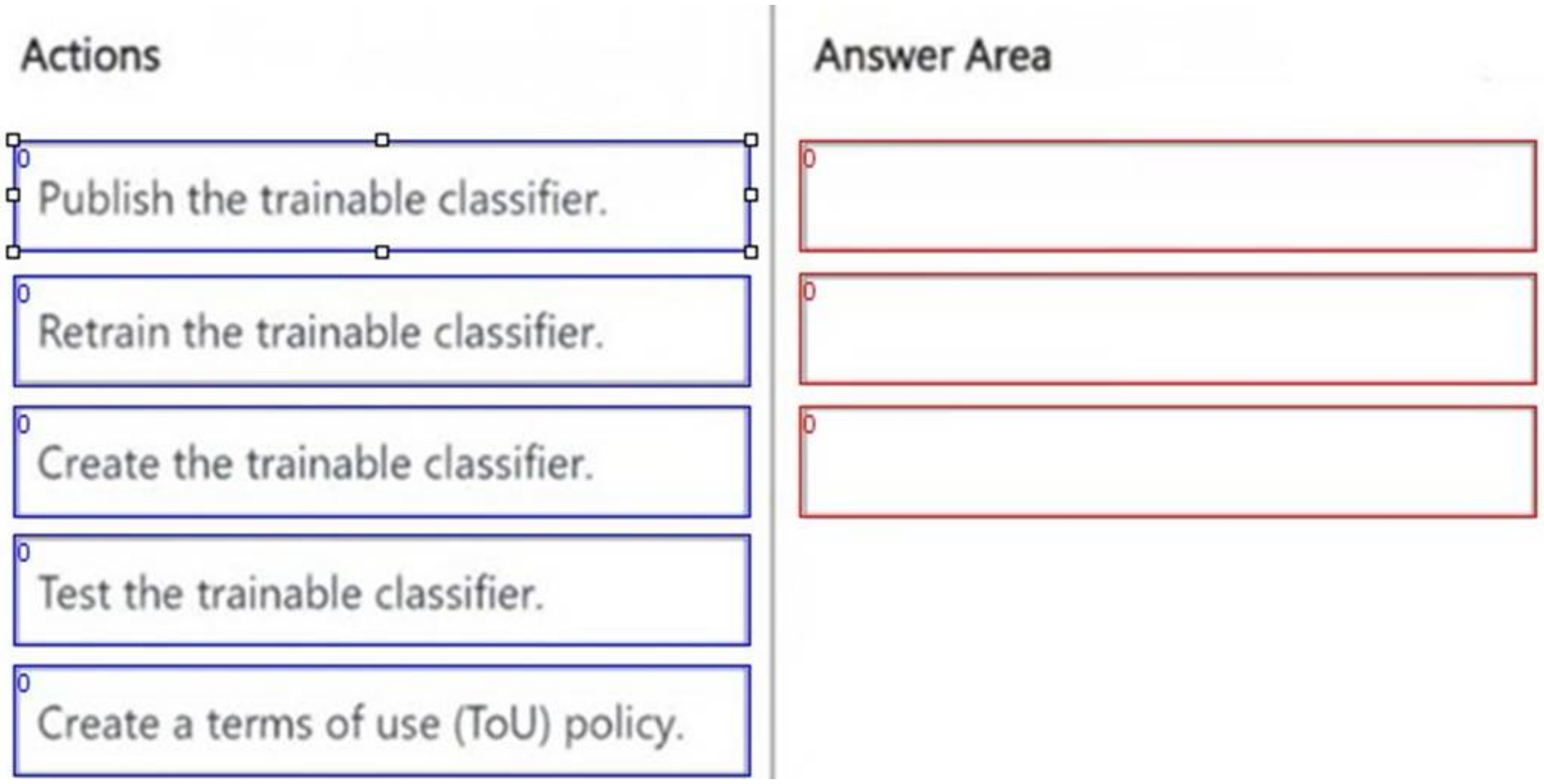
From a computer named Computer1, a user can sometimes upload files to cloud services and sometimes cannot. Other users experience the same issue.
What are two possible causes of the issue? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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 43
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 48
- (Topic 2)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.
You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.
Solution: You create a data loss prevention (DLP) policy that has only the Exchange email location selected.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.
A DLP policy with Exchange email as the only location meets this requirement because it identifies sensitive data in email messages and it applies protection actions, such as encryption, blocking, or alerts.

NEW QUESTION 50
- (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

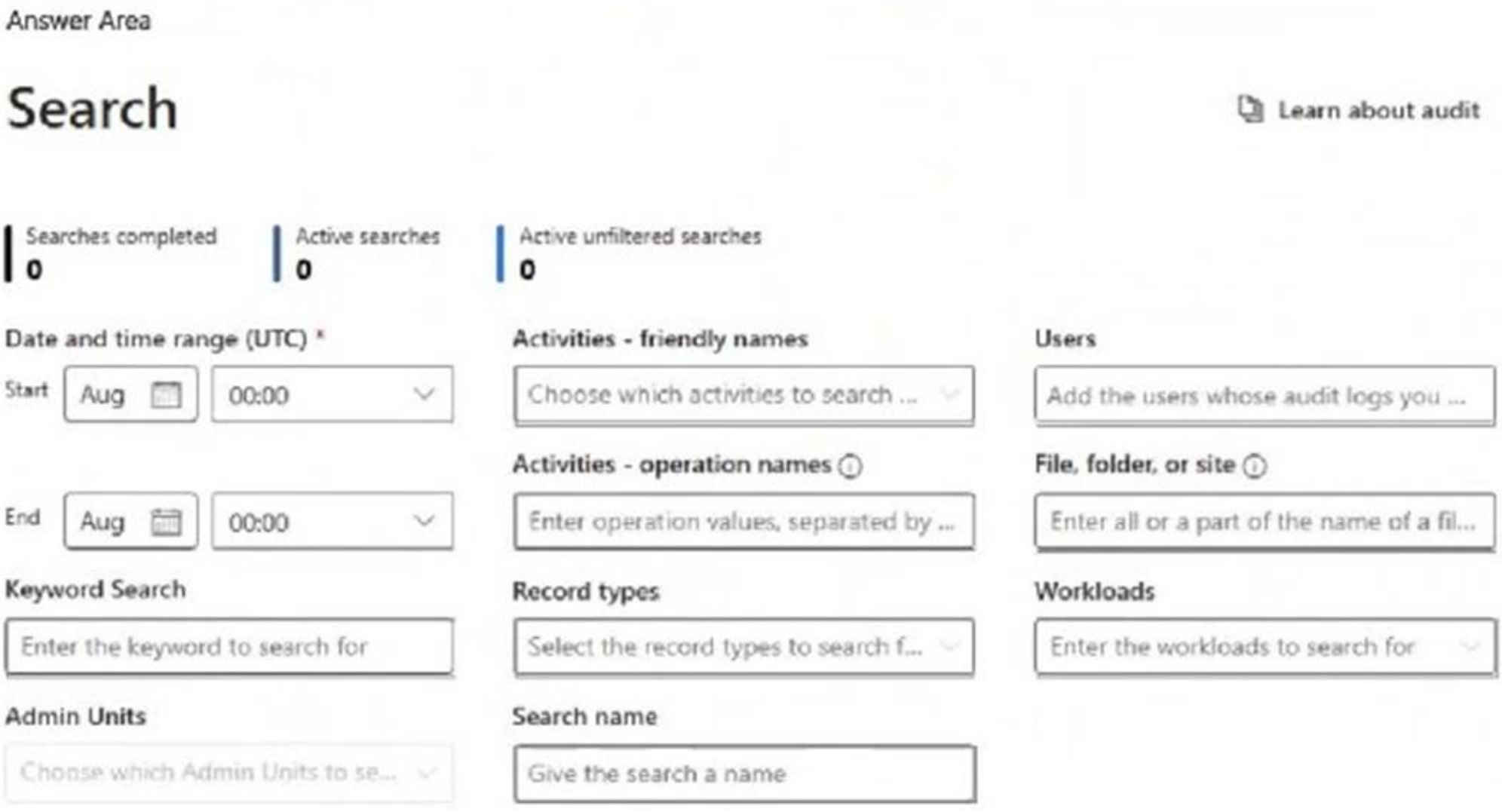
Answer: B

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 55
HOTSPOT - (Topic 2)
You have a Microsoft 365 subscription.
You plan to deploy an audit log retention policy.
You need to perform a search to validate whether the policy will be applied to the intended entries.
Which two fields should you configure for the search? To answer, select the appropriate fields in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
To validate whether an audit log retention policy will apply to the intended entries, you should configure the following fields:
Date and time range (UTC) ensures that you are searching for audit logs within the time period when the policy should be applied. Audit logs are time-sensitive, and policies affect logs based on their timestamp.
Record types allows you to filter and search for specific audit log categories (e.g., Exchange, SharePoint, Teams, etc.) that are affected by the retention policy. Selecting the correct record type ensures that the policy is evaluated against the relevant data.

NEW QUESTION 59
- (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 60
- (Topic 2)
You have a Microsoft 365 E5 subscription.
You need to ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days.
What should you configure first?

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

Answer: C

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

NEW QUESTION 65
- (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 69

- (Topic 2)
You have Microsoft 365 E5 subscription that uses data loss prevention (DLP) to protect sensitive information.
You have a document named Form.docx.
You plan to use PowerShell to create a document fingerprint based on Form.docx. You need to first connect to the subscription.
Which cmdlet should you run?

A. Connect-IPPSSession
B. Connect-SPOService
C. Connect-ExchangeOnline
D. Connect-MgGraph

Answer: A

Explanation:
To create a document fingerprint in Microsoft 365 Data Loss Prevention (DLP), you need to use PowerShell for Microsoft Purview. The correct cmdlet to connect to the Microsoft 365 Security & Compliance Center (where DLP policies are managed) is Connect- IPPSSession. This cmdlet establishes a PowerShell session to manage DLP policies, compliance settings, and document fingerprinting.

NEW QUESTION 74
- (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 76
- (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 79
- (Topic 2)
You have a Microsoft 365 E5 subscription that uses Microsoft Purview.
You create a communication compliance policy named Policy1 and select Detect Microsoft Copilot interactions.
Which two trainable classifiers will be added to Policy1 automatically? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Unauthorized disclosure
B. Prompt Shields
C. Threat
D. Corporate Sabotage
E. Protected Materials

Answer: AE

Explanation:
When you create a communication compliance policy in Microsoft Purview and select "Detect Microsoft Copilot interactions," certain trainable classifiers are automatically added to help detect sensitive or inappropriate AI usage.
The "Unauthorized disclosure" classifier helps detect cases where users might share confidential or sensitive information via Copilot interactions, preventing unintended data leaks. The "Protected Materials" classifier is used to identify sensitive or restricted content that should not be shared through Copilot, ensuring

compliance with organizational policies.

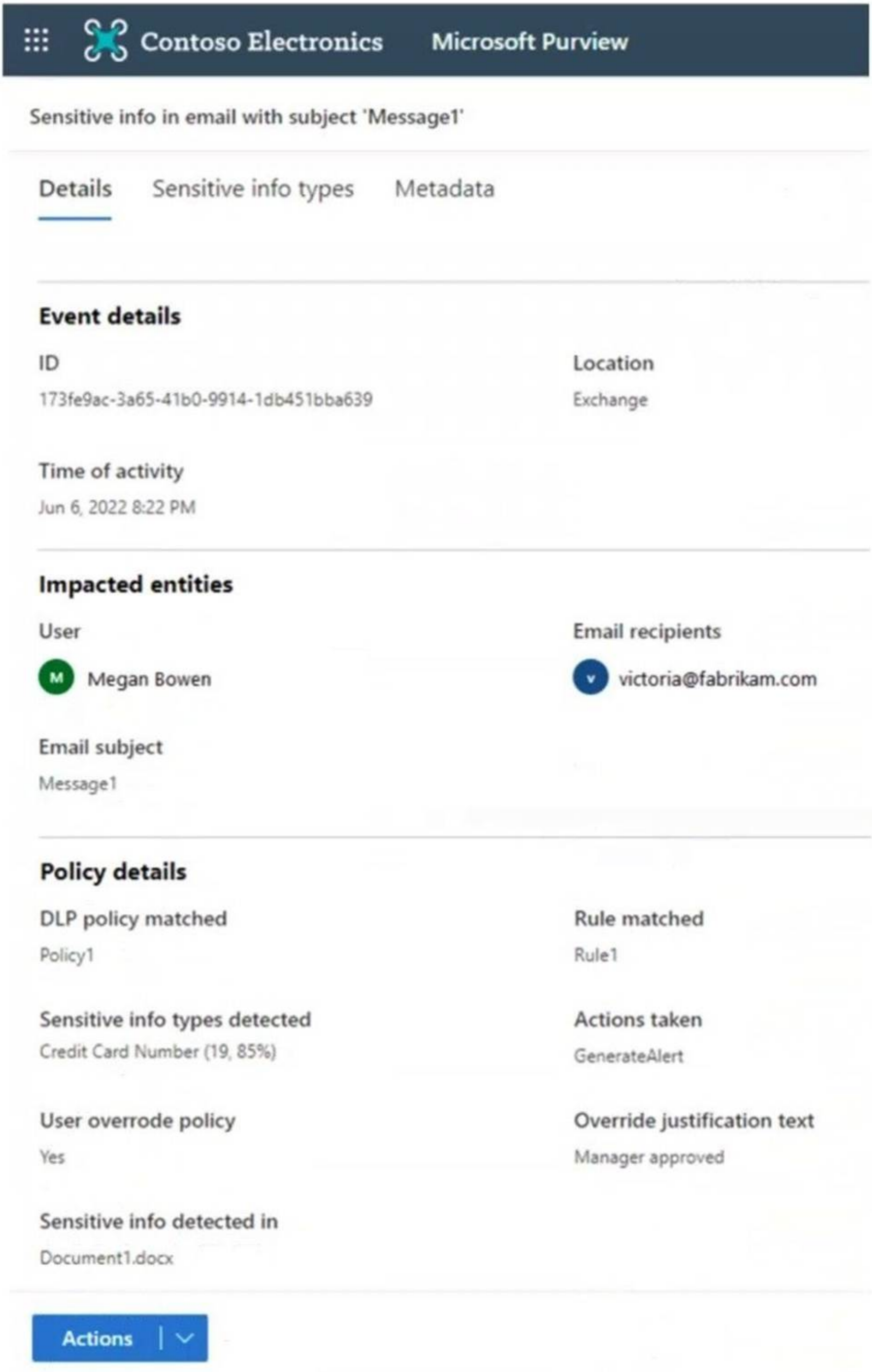
NEW QUESTION 84
- (Topic 2)
You have a Microsoft 365 subscription.
You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection 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.

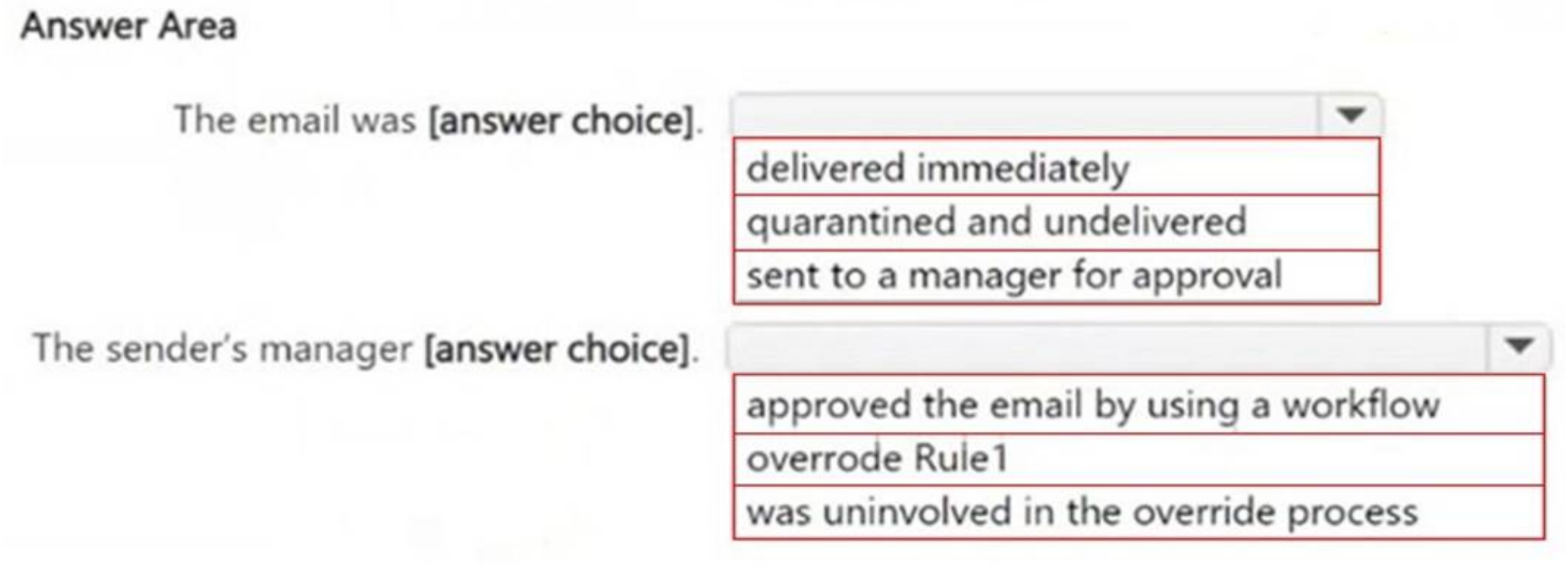
Answer: DE

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 89
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

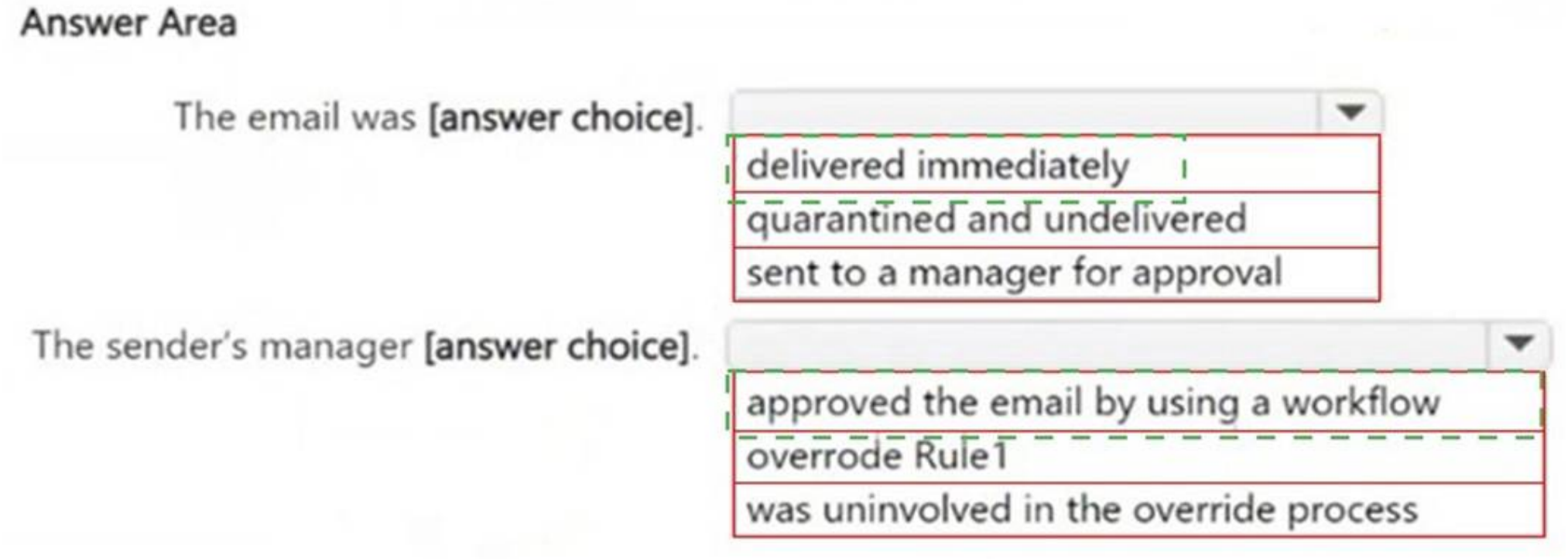
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 90
- (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 91
- (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?

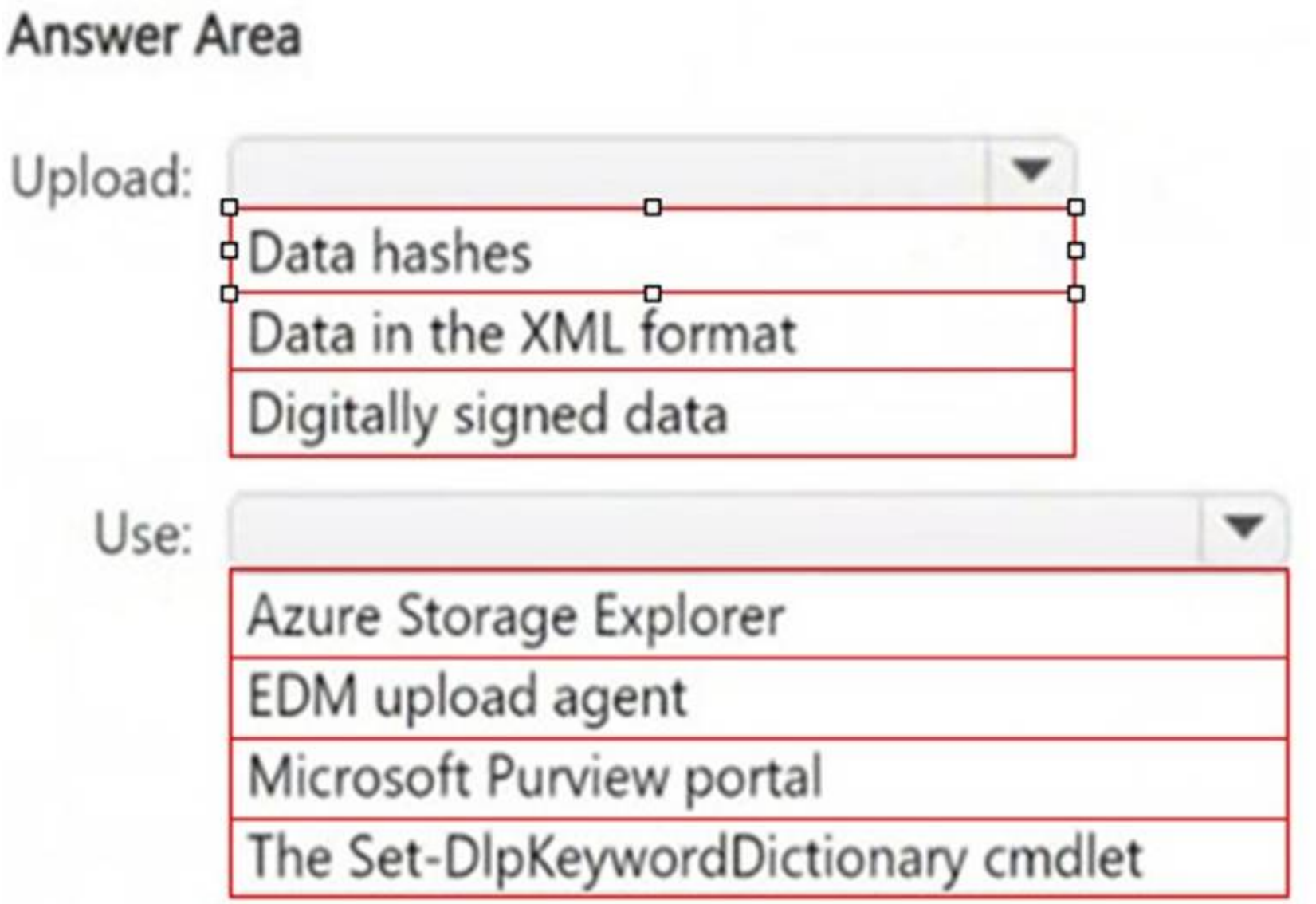
A. From the Microsoft Purview portal create an insider risk policy
B. From the Microsoft Defender portal create a file policy

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 96
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.



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 100
.....

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