# Microsoft

## Exam Questions SC-401

Administering Information Security in Microsoft 365

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

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

**Answer:** B

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

**NEW QUESTION 2**
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 3**
- (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 4**
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 5**
- (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

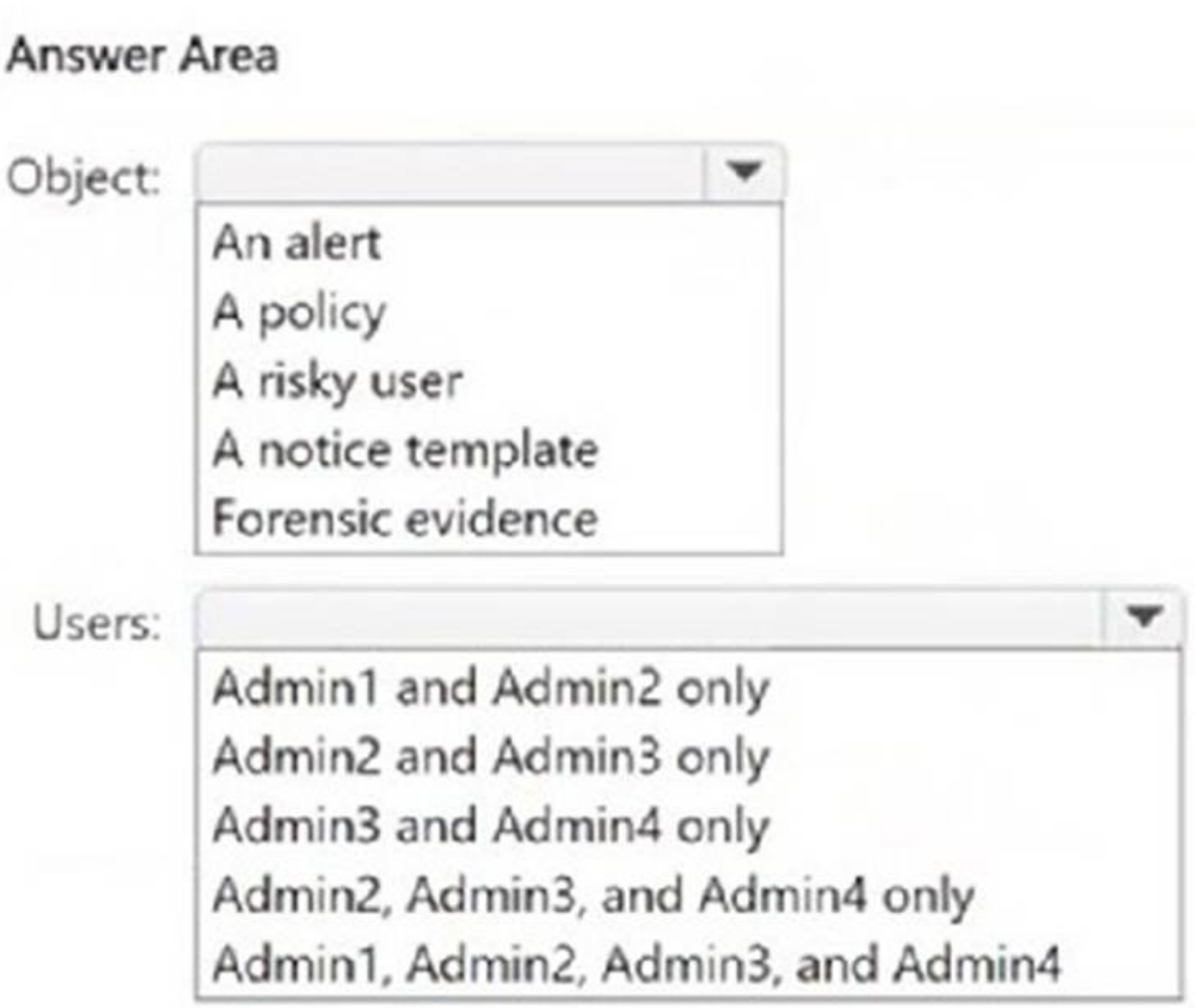
**Answer:** B

**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 6**
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.




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 7**
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 8**
- (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 9**
- (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.<br>• User1 is assigned the Reader role.<br>• Three department managers report to User1. |
| User2 | • User2 is the human resources (HR) department manager.<br>• User2 has no Microsoft Entra roles assigned.<br>• Five HR department users report to User2. |
| User3 | • User3 is a developer.<br>• User3 reports to User2.<br>• User3 is the only user in the compliance department.<br>• User3 is assigned the Compliance Administrator role. |
| User4 | • User4 is the assistant of User1.<br>• User4 has no Microsoft Entra roles assigned.<br>• 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.
You need to review a Microsoft 365 Copilot usage report. From where should you review the report?

A. Information Protection in the Microsoft Purview portal
B. the Microsoft 365 admin center
C. DSPM for AI in the Microsoft Purview portal
D. the Microsoft Defender portal

**Answer:** C

**Explanation:**
To review a Microsoft 365 Copilot usage report, you need to use Data Security Posture Management for AI (DSPM for AI) in the Microsoft Purview portal. DSPM for AI provides insights into AI-related activities, including Copilot usage, risk assessments, and data security posture related to AI interactions within Microsoft 365.

**NEW QUESTION 10**
- (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

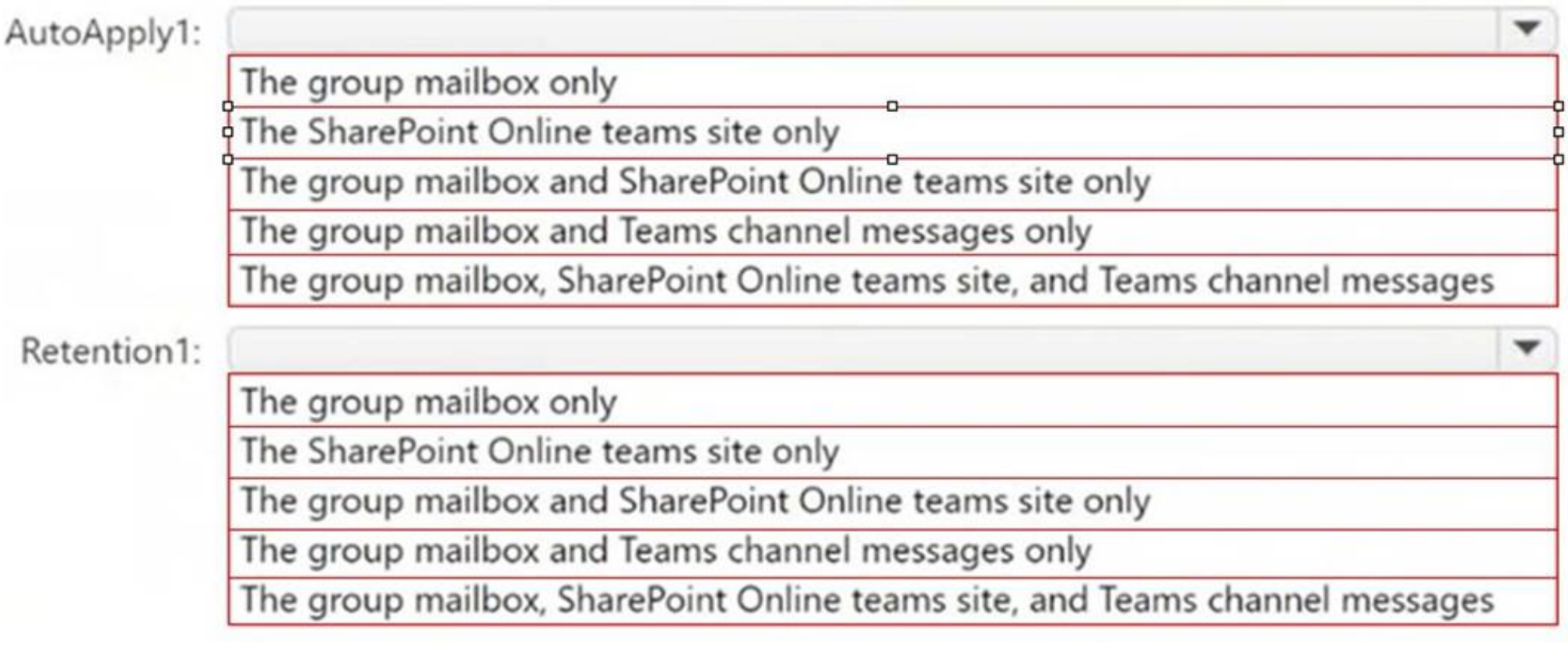
**Explanation:**
When configuring an advanced DLP rule in Microsoft Purview Data Loss Prevention (DLP), you can use a Sensitive Information Type (SIT) condition to detect and classify specific types of sensitive data, such as credit card numbers, Social Security numbers, or custom sensitive data patterns. 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 E5 subscription that contains two Microsoft 365 groups named Group1 and Group2. Both groups use the following resources:
A group mailbox
Microsoft Teams channel messages
A Microsoft SharePoint Online teams site
You create the objects shown in the following table.

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

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

Answer Area



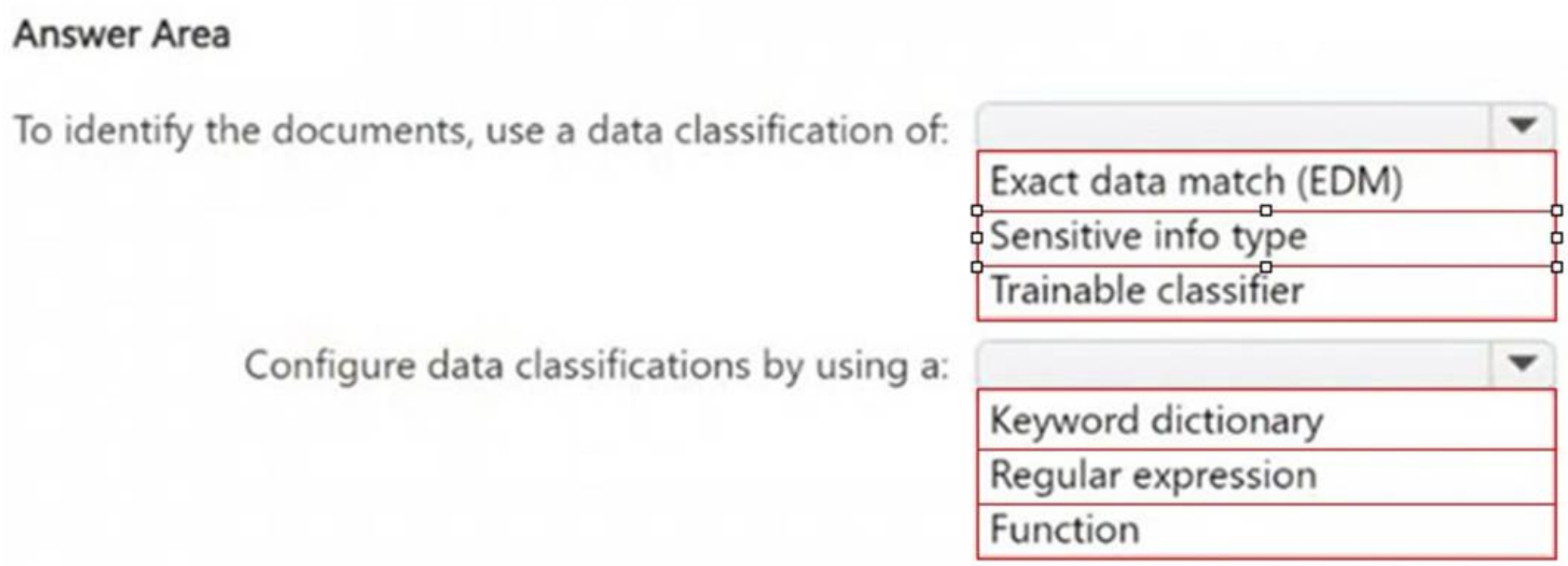

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 14**
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




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 17**
- (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)<br>• 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 19**
- (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 23**
- (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 27**
- (Topic 2)
You have a Microsoft 365 E5 subscription that uses Microsoft Purview. You are creating an exact data match (EDM) classifier named EDM1.
For EDM1, you upload a schema file that contains the fields shown in the following table.

| Column name | Match mode |
|---|---|
| PP | EU Passport Number |
| Name | All Full Names |
| DateOfBirth | Single-token |
| AccountNumber | Multi-token |

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

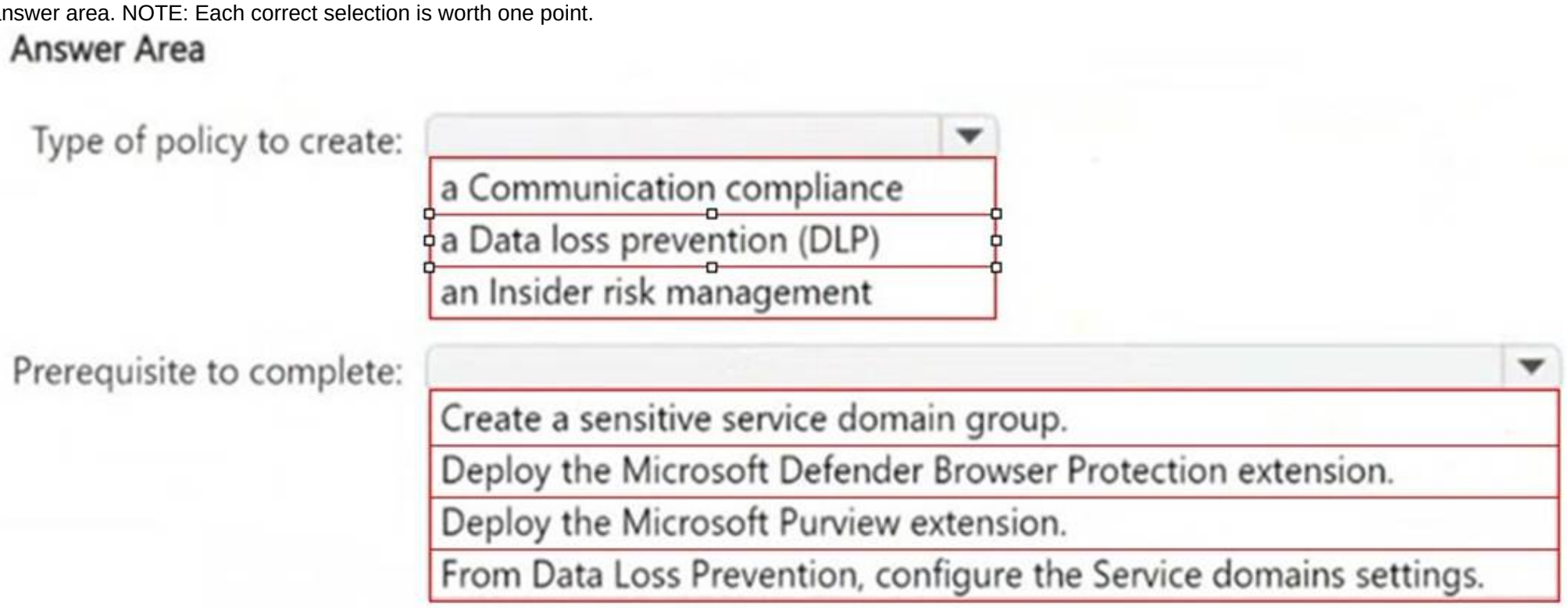
A. 1
B. 2
C. 3
D. 4

**Answer:** B

**Explanation:**
In Microsoft Purview Exact Data Match (EDM) classifiers, a primary element is a unique, identifying field used for data matching. EDM allows up to two primary elements per schema.
From the provided table, the Match mode indicates how data is analyzed: PP (EU Passport Number) Likely a primary element because it's unique.
Name (All Full Names) Typically not a primary element as names are common.
DateOfBirth (Single-token) Usually a secondary element, not unique. AccountNumber (Multi-token) Can be a primary element, as it's a unique identifier.
Since EDM supports a maximum of two primary elements, the correct answer is 2.

**NEW QUESTION 29**
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription that uses Microsoft Purview.
You need ensure that an incident will be generated when a user visits a phishing website. What should you do? 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: Insider Risk Management policies in Microsoft Purview can be configured to detect risky behavior, such as accessing phishing websites. These policies monitor user activity, generate alerts, and help organizations investigate potential security threats.
Box 2: Microsoft Defender Browser Protection extension helps in detecting unsafe or phishing websites and integrating this detection with Insider Risk Management policies. This extension works with Microsoft Edge and Google Chrome to identify risky browsing activity and trigger alerts.

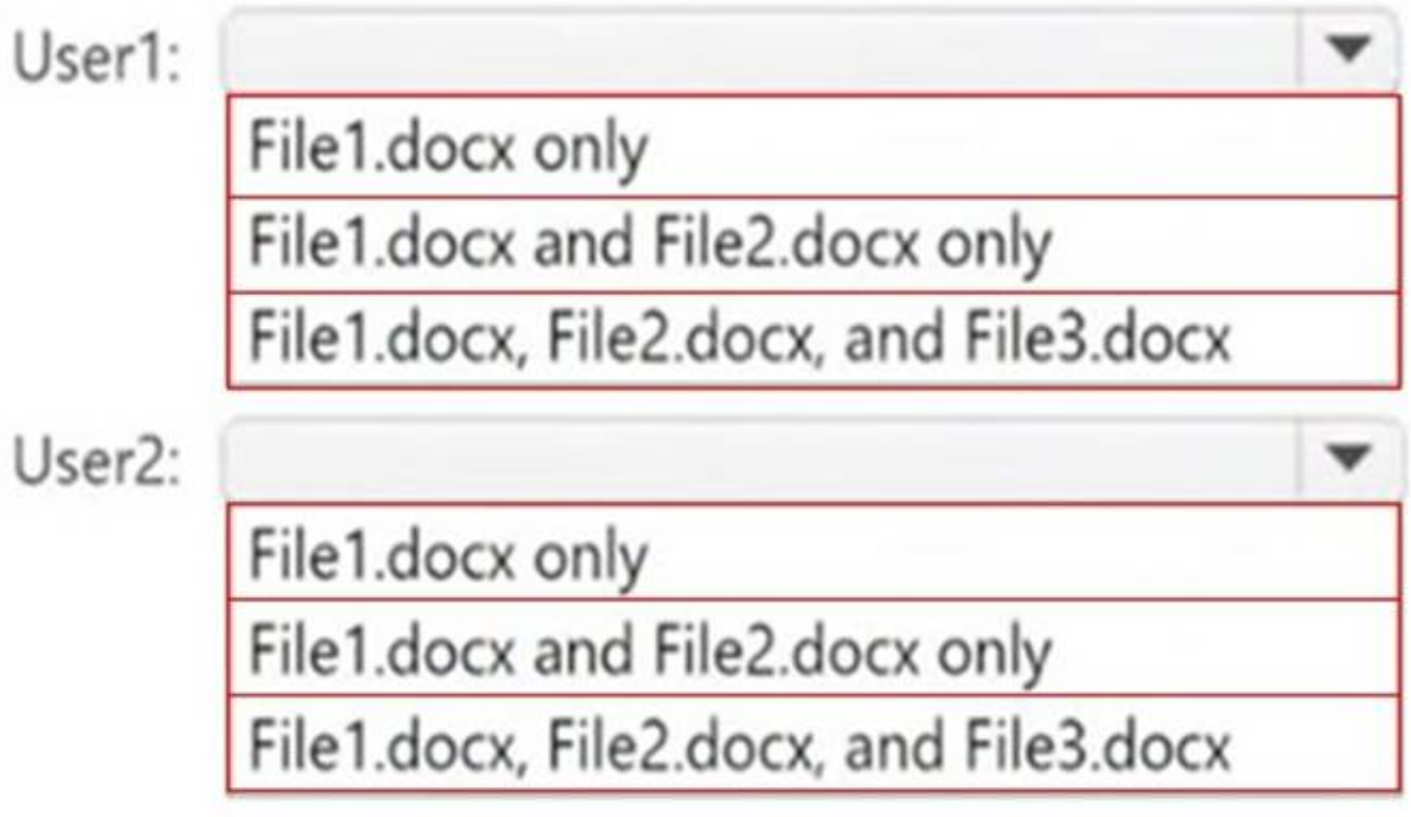
**NEW QUESTION 34**
HOTSPOT - (Topic 2)
You have a Microsoft SharePoint Online site that contains the following files.

| 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.

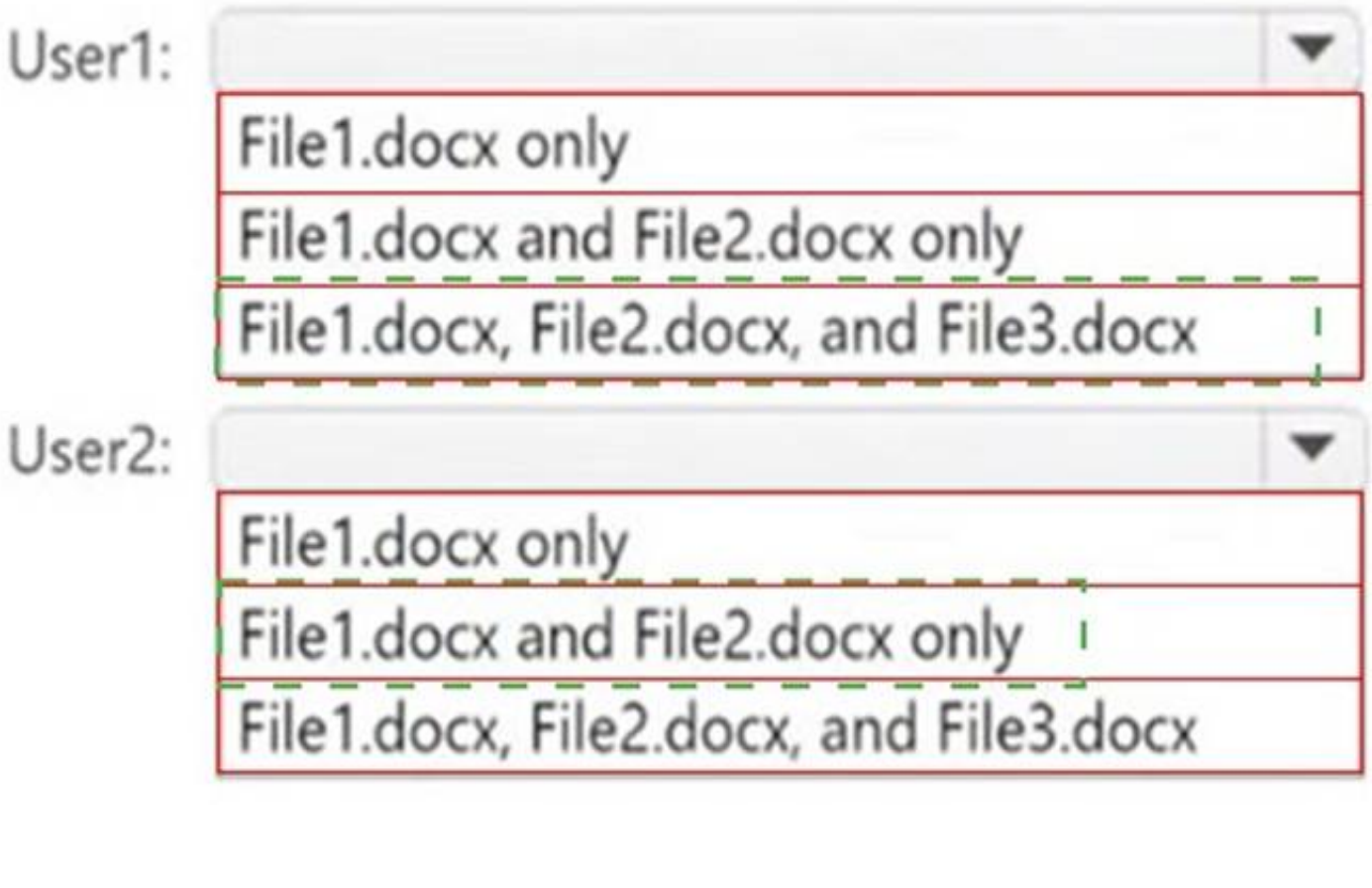



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

## Answer Area




**NEW QUESTION 37**
- (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 |

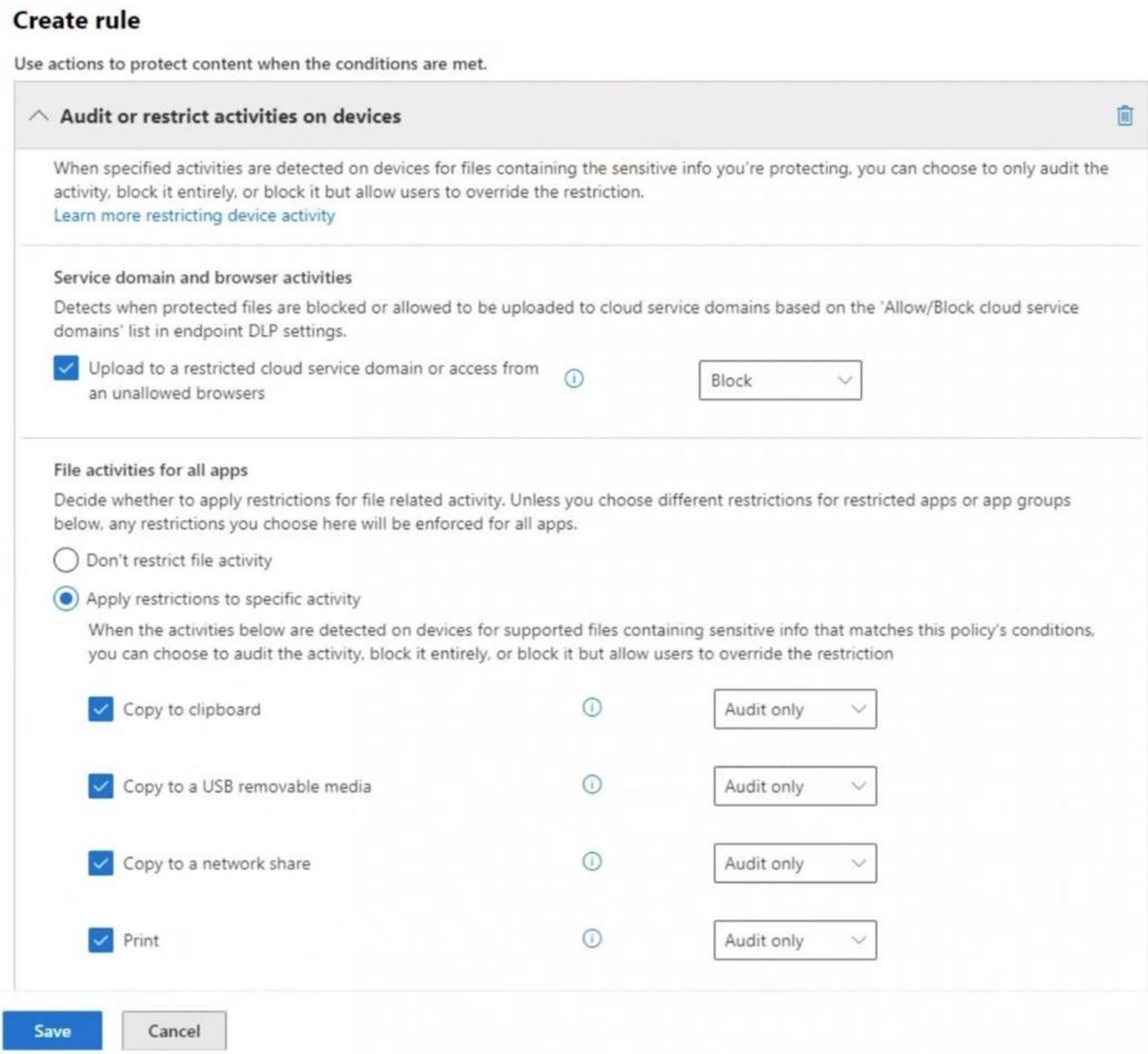
Which items can use Trainable 1?

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 39**
- (Topic 2)
You have a data loss prevention (DLP) policy configured for endpoints as shown in the following exhibit.



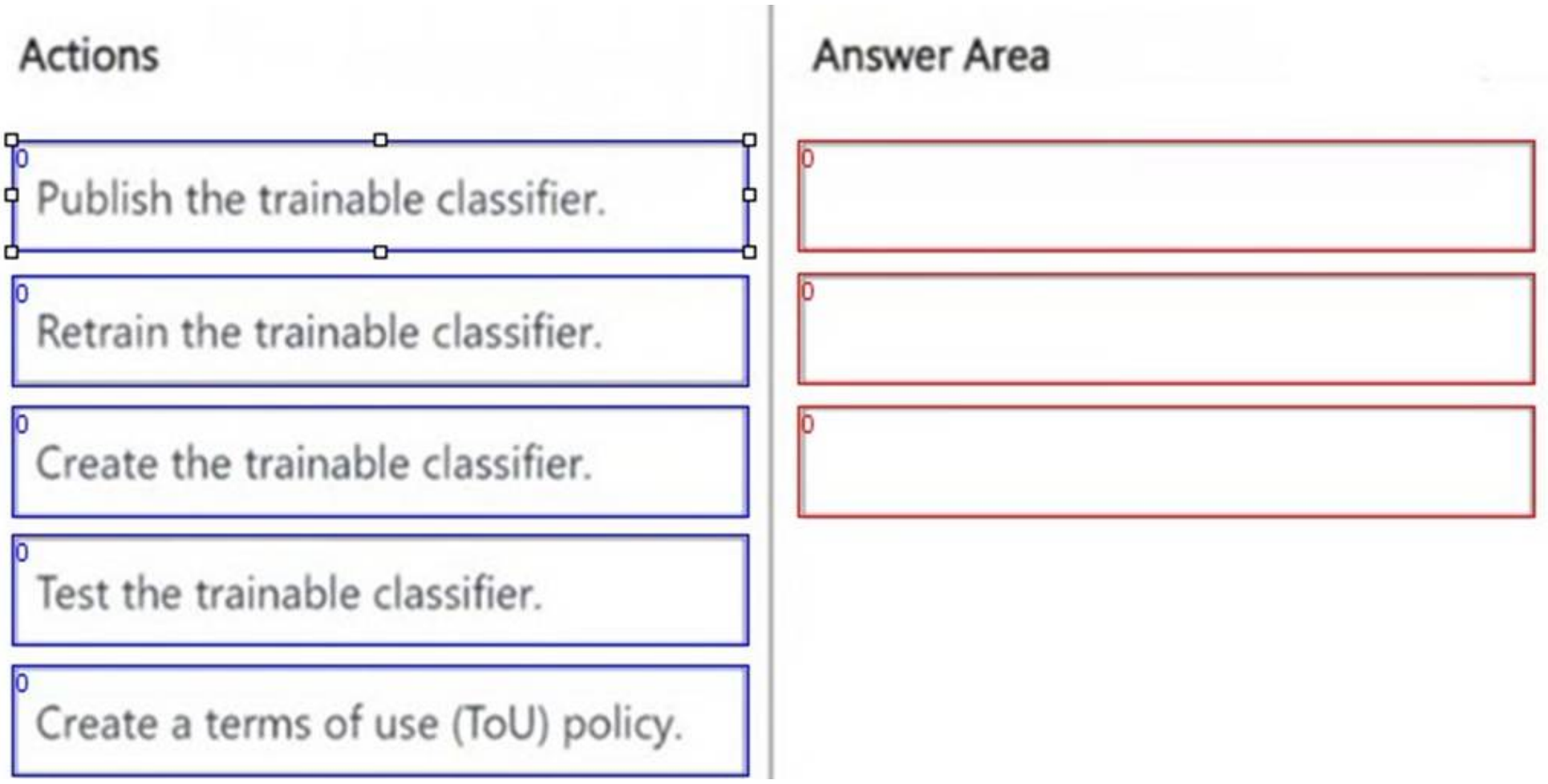

From a computer named Computer1, a user can sometimes upload files to cloud services and sometimes cannot. Other users experience the same issue.
What are two possible causes of the issue? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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 41**
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.

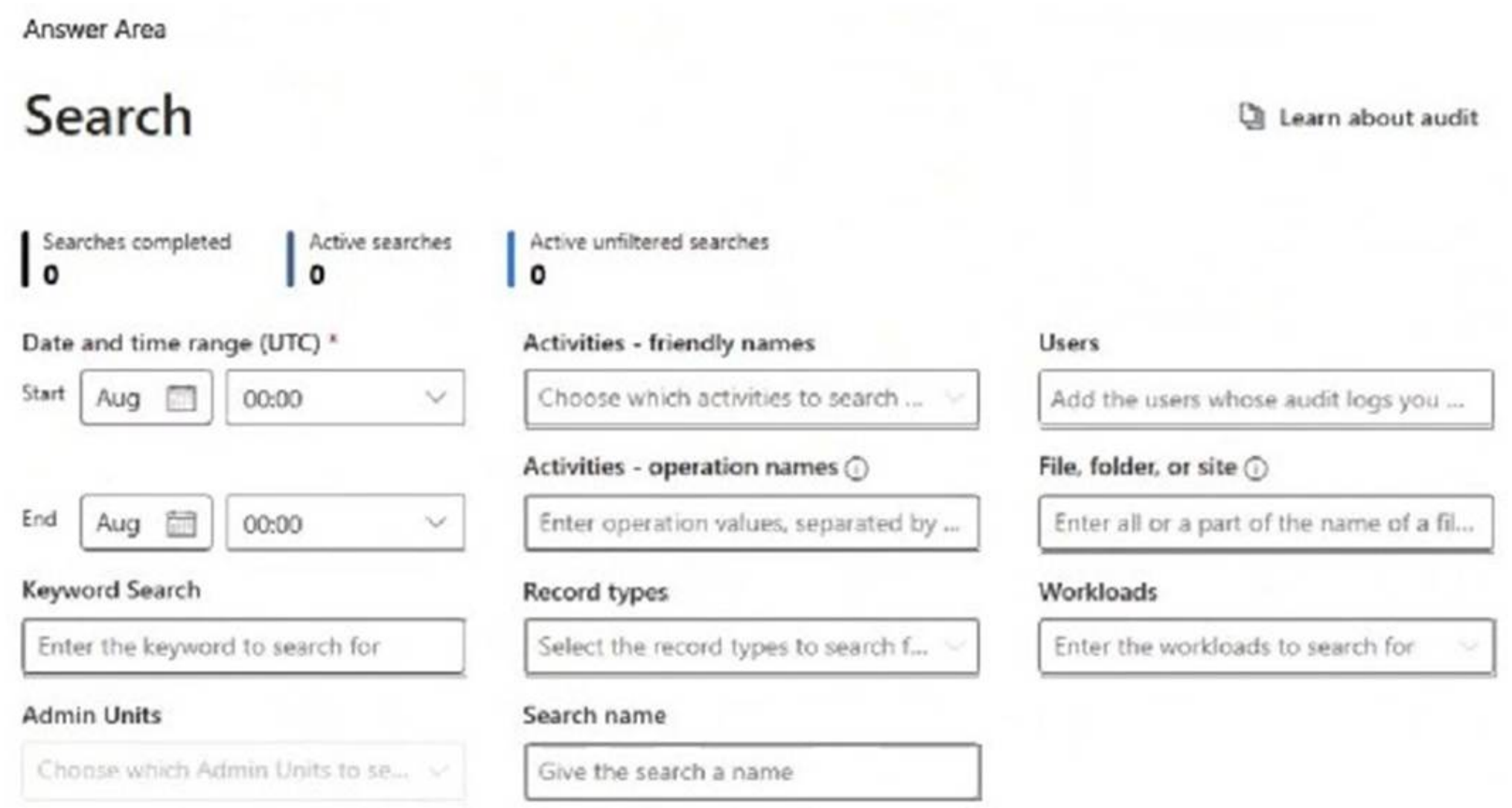
**NEW QUESTION 43**
- (Topic 2)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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 48**
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.




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 51**
- (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 53**
- (Topic 2)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.
You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers. Tailspin_scanner.exe is installed locally on the computers.
You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.
Solution: From the Microsoft Defender for Cloud Apps, you mark the application as Unsanctioned.
Does this meet the goal?

A. Yes
B. No

**Answer:** B

**Explanation:**
Marking Tailspin_scanner.exe as "Unsanctioned" in Microsoft Defender for Cloud Apps only blocks its usage in cloud-based activities (such as accessing SharePoint, OneDrive, or Exchange Online). However, it does not prevent a locally installed application on Windows 11 devices from accessing sensitive files.
To block Tailspin_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin_scanner.exe to the Restricted Apps list.
Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for non-sensitive content.

**NEW QUESTION 54**
- (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 59**
- (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 63**
- (Topic 2)
You have a Microsoft 365 E5 subscription.
You plan to implement insider risk management for users that manage sensitive data associated with a project.
You need to create a protection policy for the users. The solution must meet the following requirements:
Minimize the impact on users who are NOT part of the project. Minimize administrative effort.
What should you do first?

A. From the Microsoft Purview portal, create an insider risk management policy.
B. From the Microsoft Entra admin center, create a security grou
C. C From the Microsoft Entra admin center create a User risk policy D From the Microsoft Purview portal create a priority user group

**Answer:** B

**Explanation:**
To implement insider risk management for users managing sensitive project data while minimizing the impact on other users and reducing administrative effort, you should first create a security group in Microsoft Entra ID (formerly Azure AD).
Security groups allow you to scope insider risk management policies to specific users instead of applying policies to all users, which helps in minimizing unnecessary alerts and reducing administrative overhead. After creating the security group, you can assign this group to a Microsoft Purview Insider Risk Management policy, ensuring that only project- related users are affected.

**NEW QUESTION 66**
.....

# 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