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.

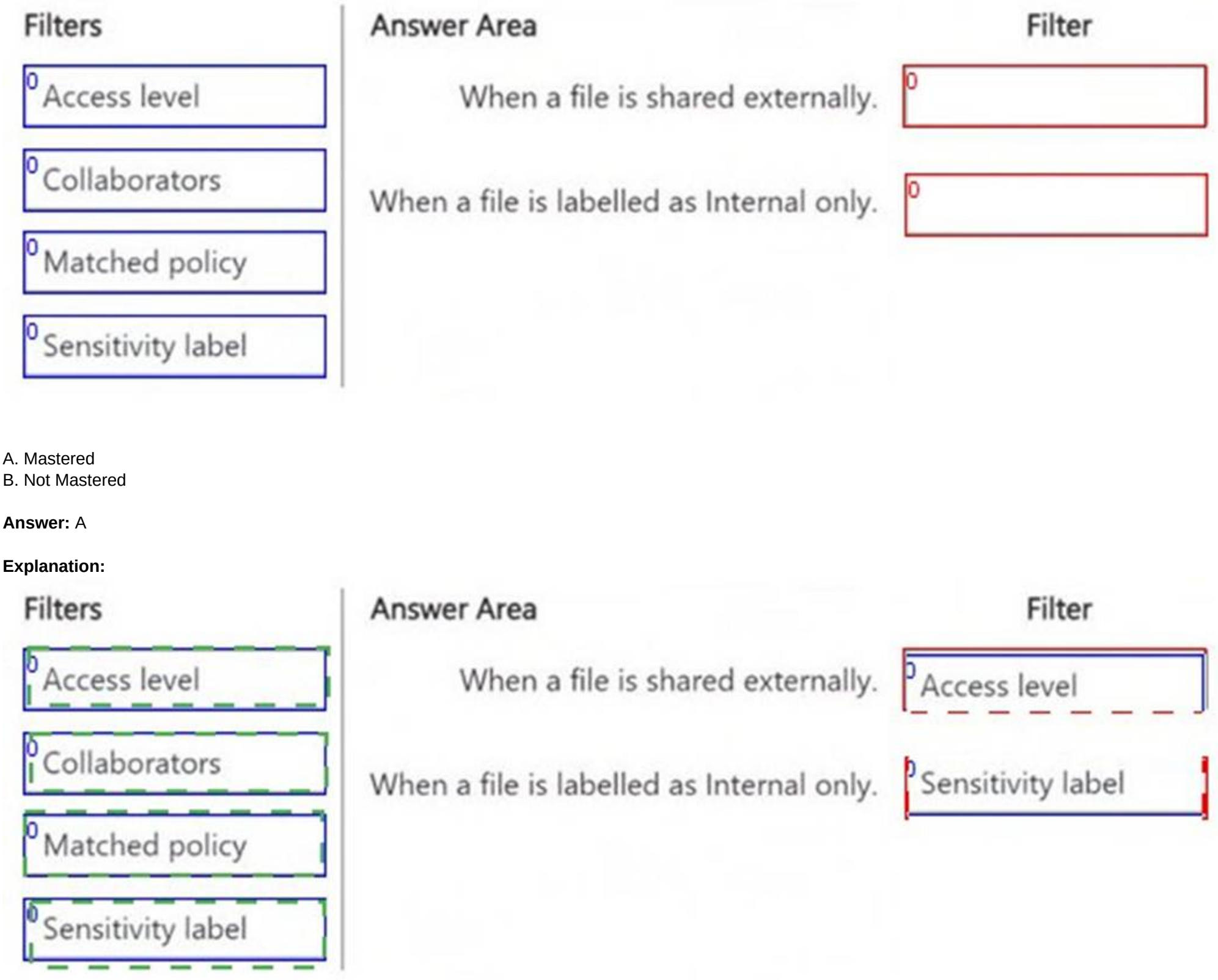
NEW QUESTION 2
HOTSPOT - (Topic 1)
You are reviewing policies for the SharePoint Online environment.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

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
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 4
- (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 5
- (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?

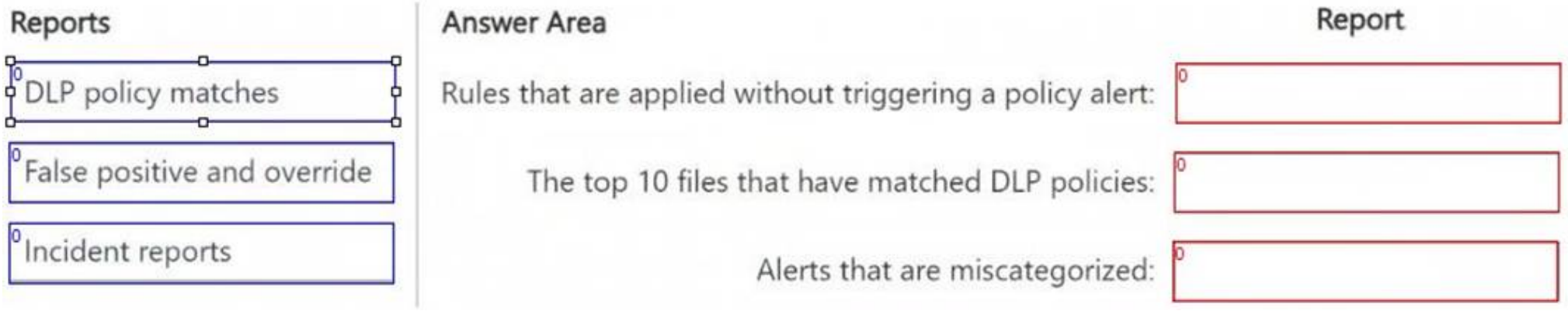
A. Information Protection in the Microsoft Purview portal
B. the Microsoft 365 admin center
C. DSPM for AI in the Microsoft Purview portal
D. the Microsoft Defender portal

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 6
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.

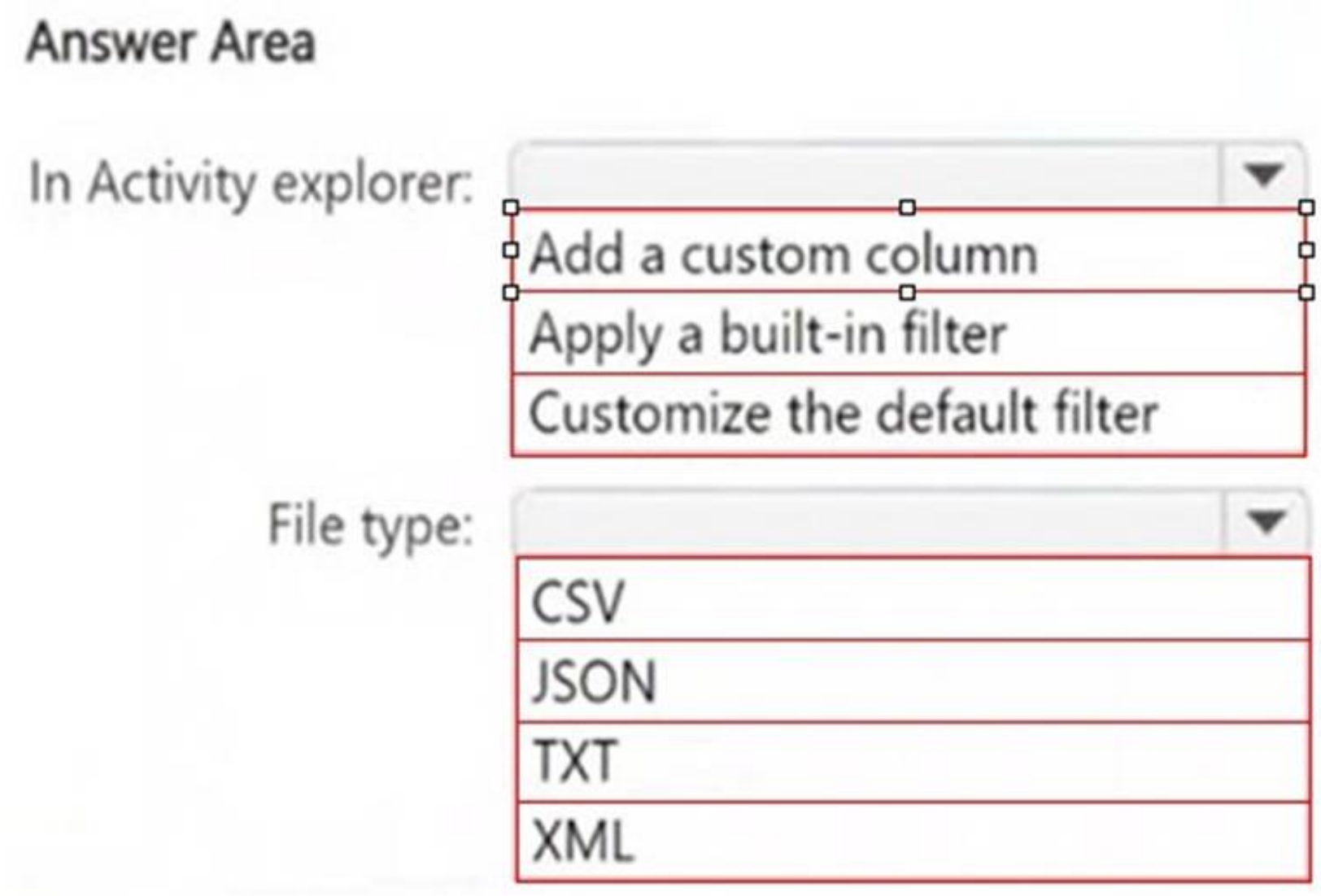


A. Mastered
B. Not Mastered

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 7
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 8
- (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

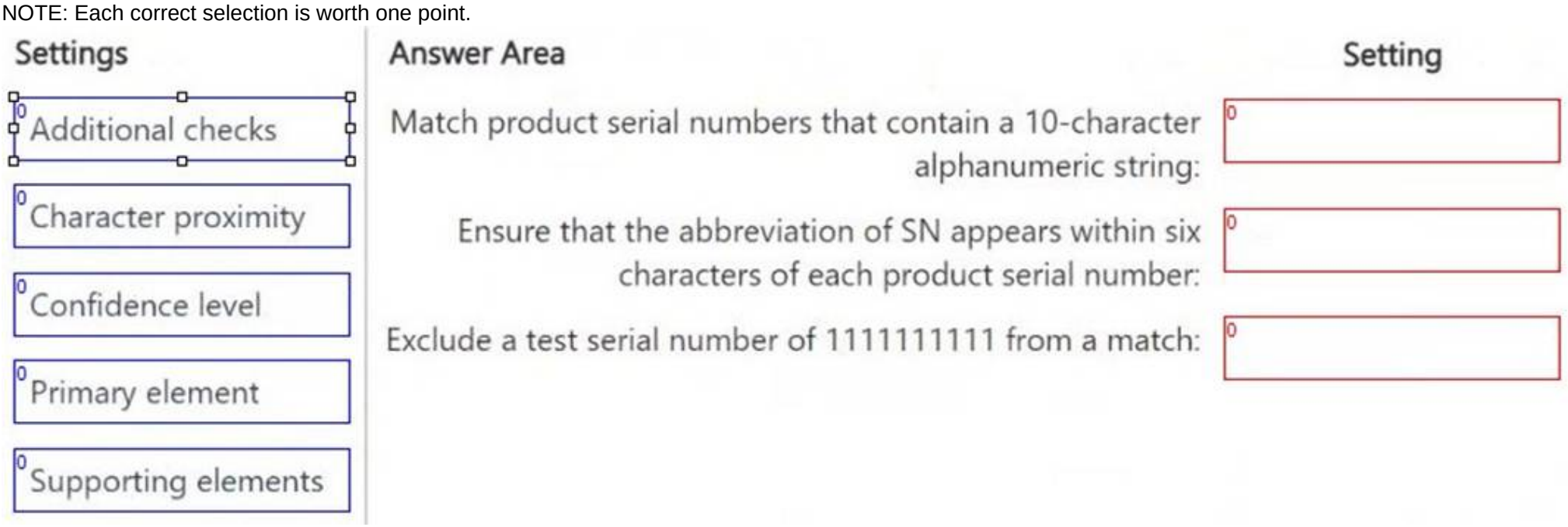
What is the maximum number of primary elements that EDM1 can have?

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.

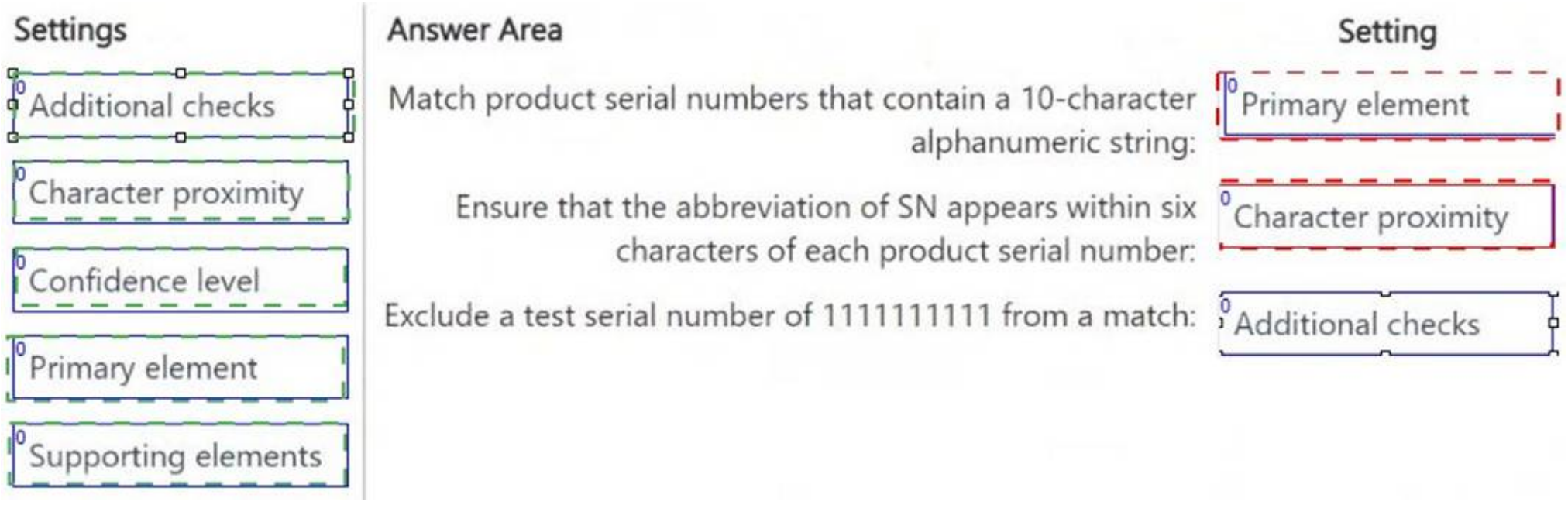
NEW QUESTION 9
DRAG DROP - (Topic 2)
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.
You need to create a custom sensitive info type. The solution must meet the following requirements:
Match product serial numbers that contain a 10-character alphanumeric string.
Ensure that the abbreviation of SN appears within six characters of each product serial number.
Exclude a test serial number of 1111111111 from a match.
Which pattern settings should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting 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 a Microsoft Teams channel named Channel1. Channel1 contains research and development documents.
You plan to implement Microsoft 365 Copilot for the subscription.
You need to prevent the contents of files stored in Channel1 from being included in answers generated by Copilot and shown to unauthorized users.
What should you use?

A. data loss prevention (DLP)
B. Microsoft Purview insider risk management
C. Microsoft Purview Information Barriers
D. sensitivity labels

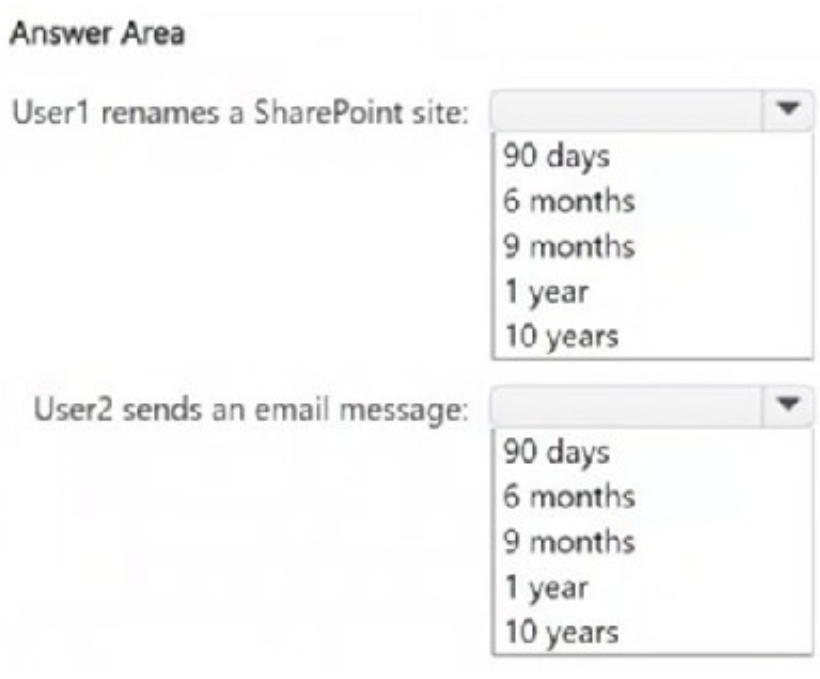
Answer: D

Explanation:
To prevent the contents of files stored in Channel1 from being included in Microsoft 365 Copilot responses and ensure unauthorized users cannot access them, you should use Microsoft Purview Sensitivity Labels.
Sensitivity labels allow you to classify, protect, and restrict access to sensitive files. You can configure label-based encryption and access control policies to ensure that only authorized users can access or interact with the files in Channel1. Microsoft 365 Copilot respects sensitivity labels, meaning if a file is labeled with restricted permissions, Copilot will not use it in generated responses for unauthorized users.

NEW QUESTION 10
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.

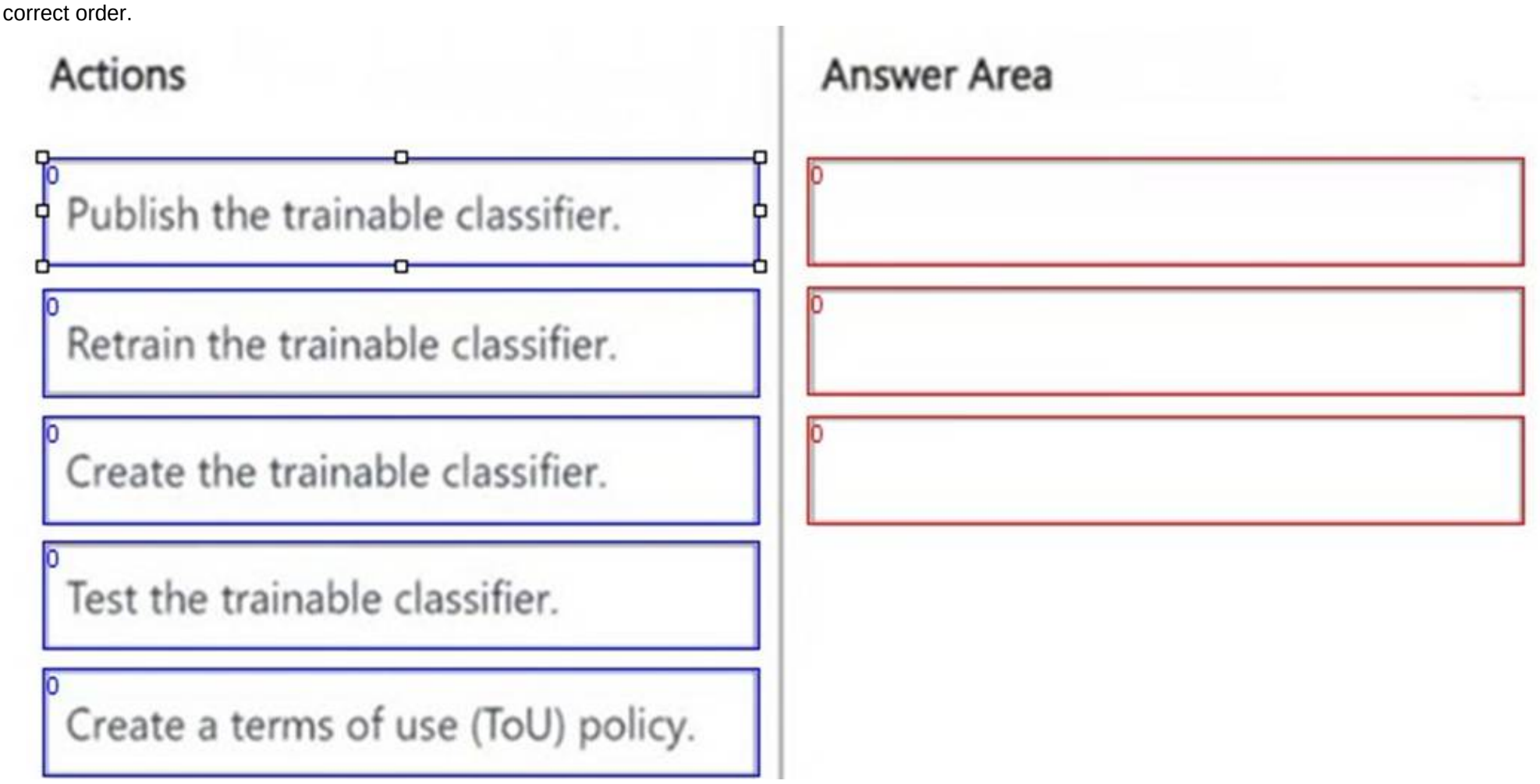


A. Mastered
B. Not Mastered

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 13
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 17

- (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 20
- (Topic 2)
You are planning a data loss prevention (DLP) solution that will apply to Windows Client computers.
You need to ensure that when users attempt to copy a file that contains sensitive information to a USB storage device, the following requirements are met:
If the users are members of a group named Group1, the users must be allowed to copy the file, and an event must be recorded in the audit log.
All other users must be blocked from copying the file. What should you create?

A. one DLP policy that contains one DLP rule
B. one DLP policy that contains two DLP rules
C. two DLP policies that each contains one DLP rule

Answer: B

Explanation:
To meet the requirements, you need one DLP policy with two separate DLP rules to handle the different conditions:
* 1. First DLP Rule (For Group1 Members): If the user is a member of Group1 and attempts to copy a file with sensitive data to a USB storage device. Allow the file copy but log the event in the audit log.

* 2. Second DLP Rule (For All Other Users): If any user who is NOT in Group1 attempts to copy a file with sensitive data to a USB storage device. Block the file transfer.

NEW QUESTION 21
- (Topic 2)
You have a Microsoft 365 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 22
- (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 27
.....

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