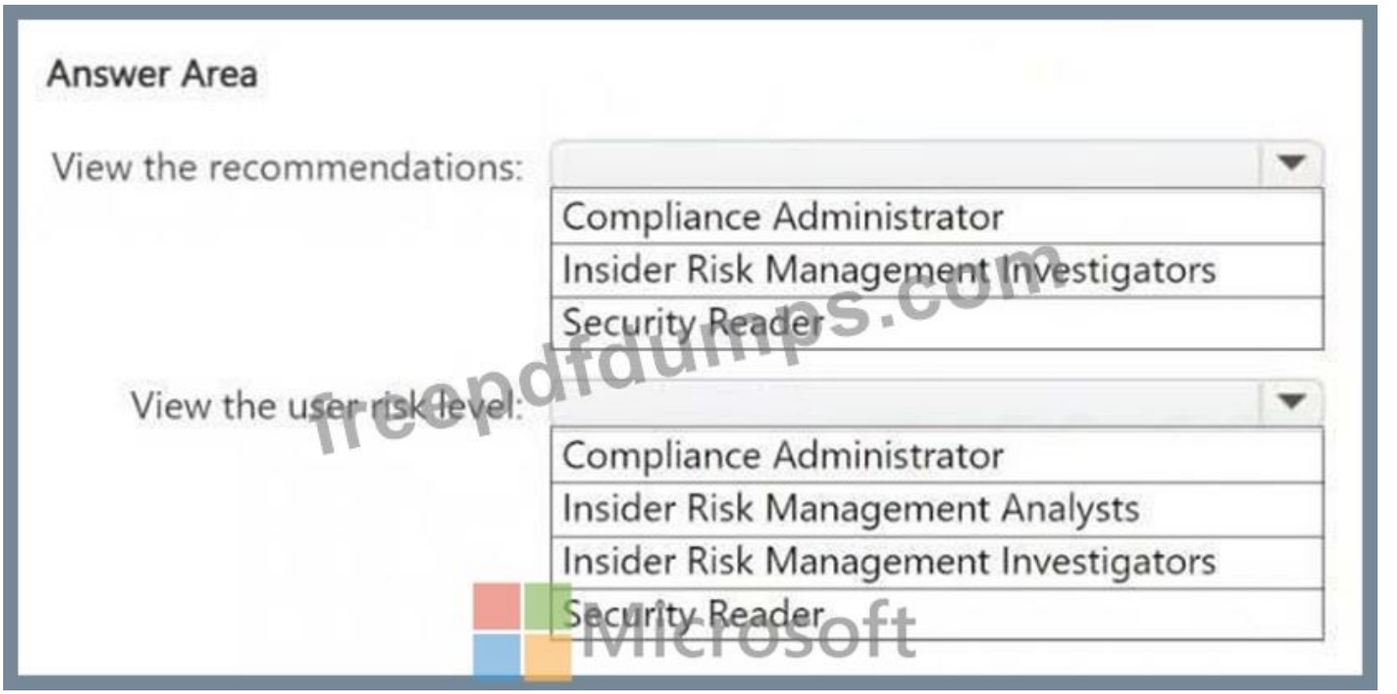
# Microsoft.SC-401.v2026-03-09.q117

| | |
|---|---|
| **Exam Code:** | SC-401 |
| **Exam Name:** | Administering Information Security in Microsoft 365 |
| **Certification Provider:** | Microsoft |
| **Free Question Number:** | 117 |
| **Version:** | v2026-03-09 |
| **# of views:** | 181 |
| **# of Questions views:** | 1170 |
| https://www.freepdfdumps.com/Microsoft.SC-401.v2026-03-09.q117.html | |

**NEW QUESTION: 1**
Hotspot Question
You have a Microsoft 365 E5 subscription that contains a user named User1.
You deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI).
You need to ensure that User1 can perform the following actions:
- View recommendations from the Recommendations page.
- View the user risk level for all events by using Activity explorer.
The solution must follow the principle of least privilege.
To which role group should you add User1 for each action? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.




**Answer:**


Explanation:

Box 1: The Insider Risk Management Investigators role allows users to view recommendations related to insider risk cases and Microsoft Purview DSPM for AI insights. This role is appropriate because it grants access to review AI-related risk recommendations without unnecessary administrative privileges.

Box 2: The Insider Risk Management Analysts role allows users to analyze user risk levels and events using Activity Explorer. This follows the principle of least privilege, ensuring that User1 can only view risk levels and investigate but does not gain full administrative control over insider risk policies.

**NEW QUESTION: 2**

Hotspot Question

You have a Microsoft 365 E5 subscription that contains the device configurations shown in the following table.

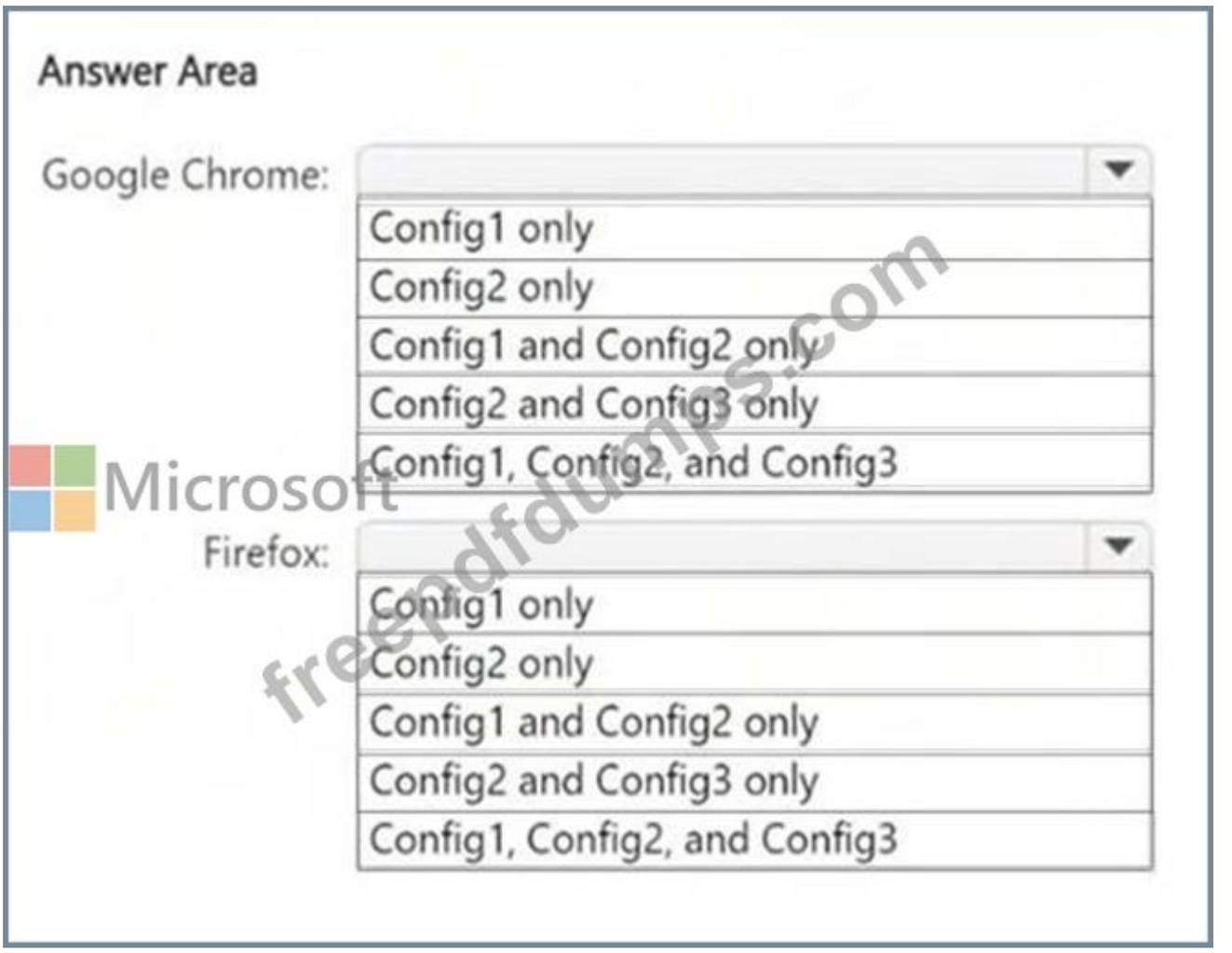
| Name | Platform |
|---|---|
| Config1 | Windows 11 |
| Config2 | macOS |
| Config3 | Android |

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.

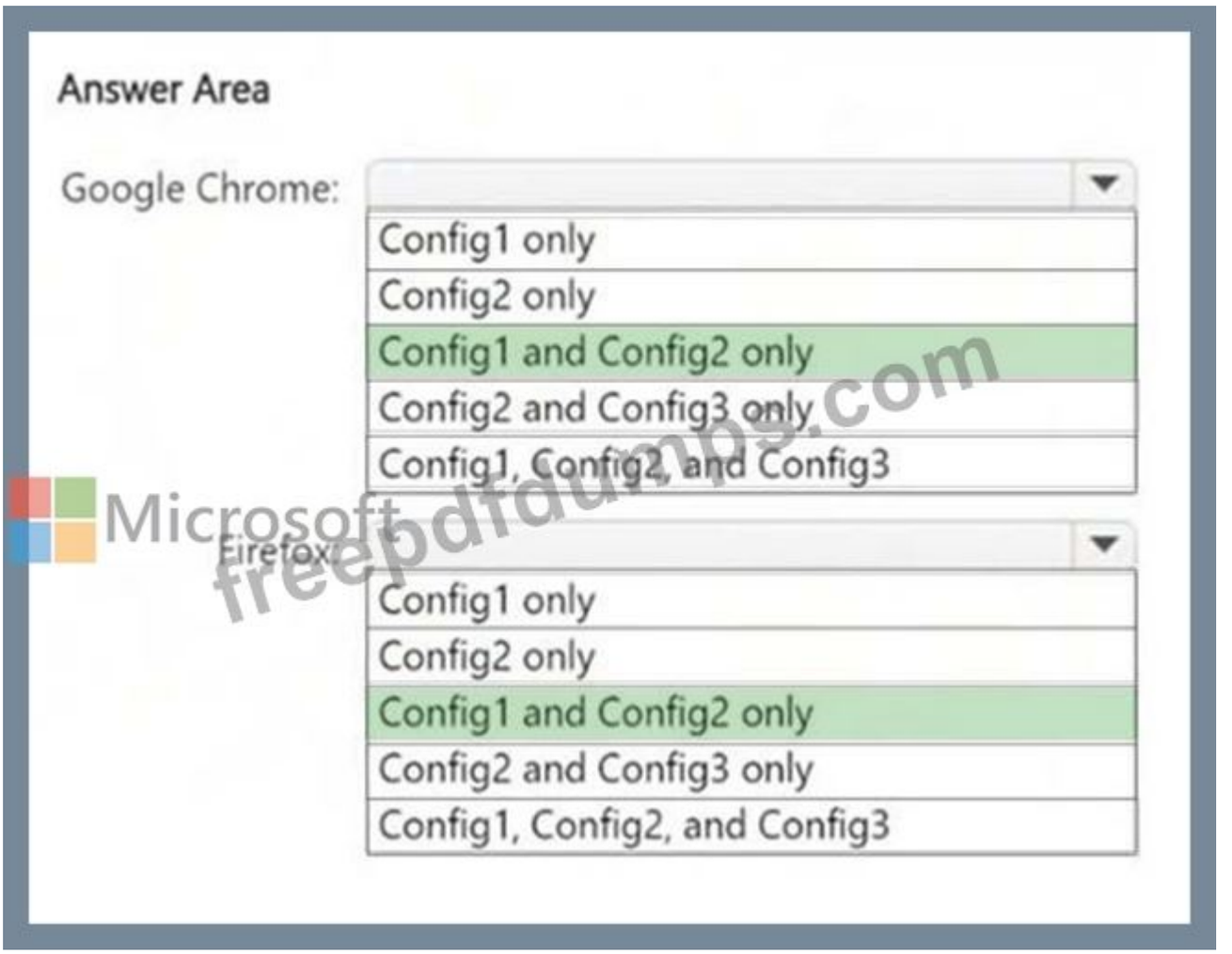
To which configuration can each extension be deployed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.






**Answer:**





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: 3**
You have a Microsoft 365 E5 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2.
You plan to configure a retention label named Label1 and apply Label1 to all the files in Site1.
You need to ensure that two years after a file is created in Site1, the file moves automatically to Site2.
How should you configure the Choose what happens after the retention period setting for Label1?
**A.** Deactivate retention settings
**B.** Run a Power Automate flow
**C.** Start a disposition review
**D.** Change the label

**Answer: B (LEAVE A REPLY)**
Common settings for retention policies and retention label policies
Selecting Run a Power Automate flow enables moving labeled items to be moved to a certain location.
Reference:
https://learn.microsoft.com/en-us/purview/retention-settings

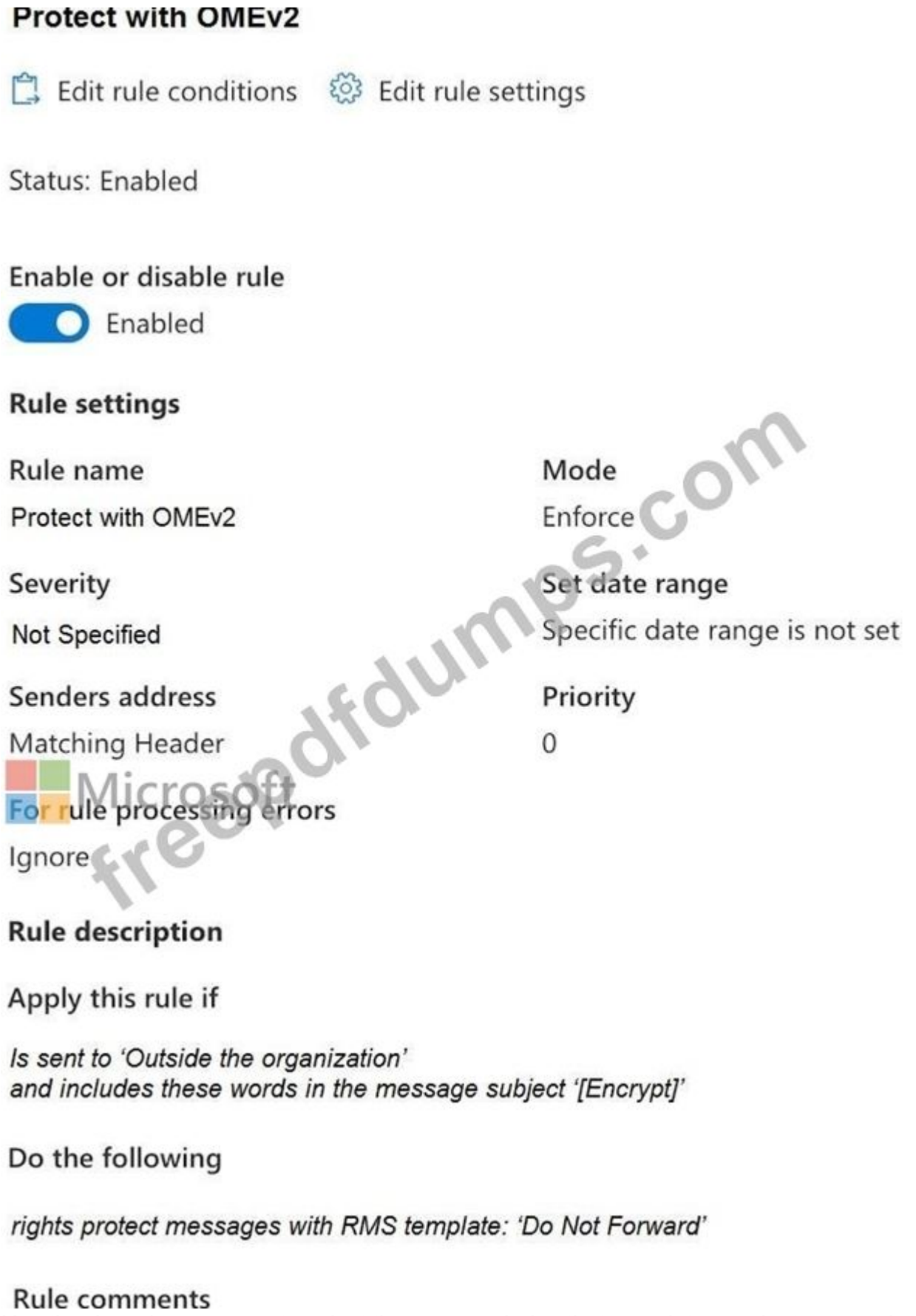
**NEW QUESTION: 4**
SIMULATION
Username and password
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and select the username below.
To enter your password, place your cursor in the Enter password box and select the password below.
Microsoft 365 Username:
admin@WWLx971455.onmicrosoft.com
Microsoft 365 Password: XXXXXXXXX
If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL "https://admin microsoft.com", and press Enter.
The following information is for technical support purposes only:
Lab Instance: XXXXXXXX.
Task 9
You plan to create a data loss prevention (DLP) policy that will apply to content containing the following keywords:
- Tailspin
- Litware
- Falcon
You need to create a keyword list that can be used in the DLP policy.
**Answer:**
To create a sensitive information type that matches all words in a keyword list, you can use the "All" condition instead of the default "Any" condition. Here are the steps to create such a sensitive information type:
Step 1: Go to the Microsoft 365 compliance center and navigate to the "Sensitive information types" page.
Step 2: Click on "Create a sensitive information type".
Step 3: Choose "Keyword dictionary" as the type of sensitive information you want to create.
Step 4: Enter a name and description for the sensitive information type.
Step 5: In the "Keywords" section, enter all the words you want to match separated by com-mas. Here we enter: Tailspin, Litware, Falcon
Step 6: Click on "Add condition" and choose "Any" as the condition type.

Step 7: Click on "Create" to create the sensitive information type.
Step 8: Click on "Create" to create the sensitive information type.
With this configuration, the DLP policy will only detect the sensitive information if any the words in the keyword list are present in the content being scanned.
Reference:
https://learn.microsoft.com/en-us/answers/questions/1419105/how-to-create-sensitive-information-types-to-match

**NEW QUESTION: 5**
You have a Microsoft 365 E5 subscription. Microsoft Priva Privacy Risk Management licenses are assigned to all users.
You need to review and delete all the personal data that relates to a former employee. The solution must minimize administrative effort.
What should you do first?
**A.** Purchase a Microsoft Priva Subject Rights Requests license.
**B.** Create an eDiscovery (Standard) case.
**C.** From Data matching, add a personal data schema for the data profile.
**D.** Create a retention policy.
**Answer: D (LEAVE A REPLY)**

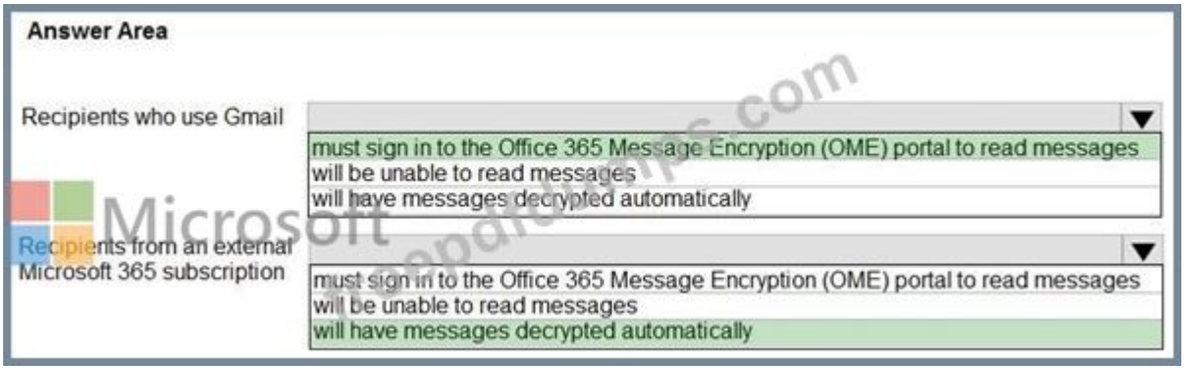
**NEW QUESTION: 6**
You are creating a data loss prevention (DLP) policy that will apply to all available locations except Fabric and Power BI workspaces.
You configure an advanced DLP rule in the policy.
Which type of condition can you use in the rule?
**A.** Sensitive info type
**B.** Content search query
**C.** Sensitive label
**D.** Keywords
**Answer: A (LEAVE A REPLY)**
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: 7**
Hotspot Question
You have a Microsoft 365 E5 subscription.
In Microsoft Exchange Online, you have the mail flow rule shown in the following exhibit.




Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.


**Answer:**




Explanation:

Box 1: must sign in to the Office 365 Message Encryption (OME) portal to read messages.

Recipients using Gmail can read emails protected by Microsoft Exchange Online mail flow rules set to Protect with OMEv2 (Office Message Encryption version 2). They will typically receive a link to view the message in the Microsoft Purview Message Encryption portal.

Box 2: will have messages decrypted automatically

Recipients from an external Microsoft 365 subscription can read emails protected by a Microsoft Exchange Online mail flow rule set to "Protect with OMEv2" (Microsoft Purview Message Encryption). External recipients will receive a wrapper email with instructions on how to access the encrypted message, either by signing in with their Microsoft account, Google account, Yahoo account, or by using a one-time passcode.

Reference:

https://learn.microsoft.com/en-us/purview/email-encryption

https://learn.microsoft.com/en-us/purview/ome

**NEW QUESTION: 8**

You are creating a custom trainable classifier to identify organizational product codes referenced in Microsoft 365 content.

You identify 300 files to use as seed content.

Where should you store the seed content?

**A.** an Azure file share

**B.** a Microsoft OneDrive folder

**C.** a Microsoft SharePoint Online folder

**D.** a Microsoft Exchange Online shared mailbox

**Answer: (SHOW ANSWER)**

Seed content files for a custom trainable classifier should be stored in a SharePoint Online folder (or folders) that is dedicated to holding only that seed content. You'll need to create a separate folder for positive examples and another for negative examples. After placing the files, make note of the full URL of the SharePoint site, library, and folder for each set of content.

Note: How to create a trainable classifier: The following process automates the testing of trainable classifiers and shortens the creation workflow from 12 days to two days. In some cases, the process can take only a few hours.

1. Collect between 50 and 500 seed content items that strongly represent the data you want the classifier to positively identify as being in the category. For a list of supported file types, see Default crawled file name extensions and parsed file types in SharePoint Server.
2. Collect a second set of seed content (from 150 to 1,500 items) that represents data that don't belong in the category.
3. Place the positive and negative seed content in separate SharePoint folders. Each folder must be dedicated to holding only the seed content. Make note of the site, library, and folder URL for each set.
4. Sign in to the Microsoft Purview portal with either Compliance admin or Security admin role access and navigate to Data loss prevention > Data classification > Classifiers.

Reference:

https://learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with

**NEW QUESTION: 9**

You have a Microsoft OneDrive folder that contains the files shown in the following table.

| Type | Number of files |
|---|---|
| .jpg | 50 |
| .docx | 300 |
| .txt | 50 |
| .zip | 20 |



In Microsoft Defender for Cloud Apps, you create a file policy to automatically apply a classification.

What is the effect of applying the policy?

**A.** The policy will apply to only the .docx and .txt files. The policy will classify the files immediately.

**B.** The policy will apply to only the .docx files. The policy will classify only 100 files daily.

**C.** The policy will apply to all the files. The policy will classify only 100 files daily.

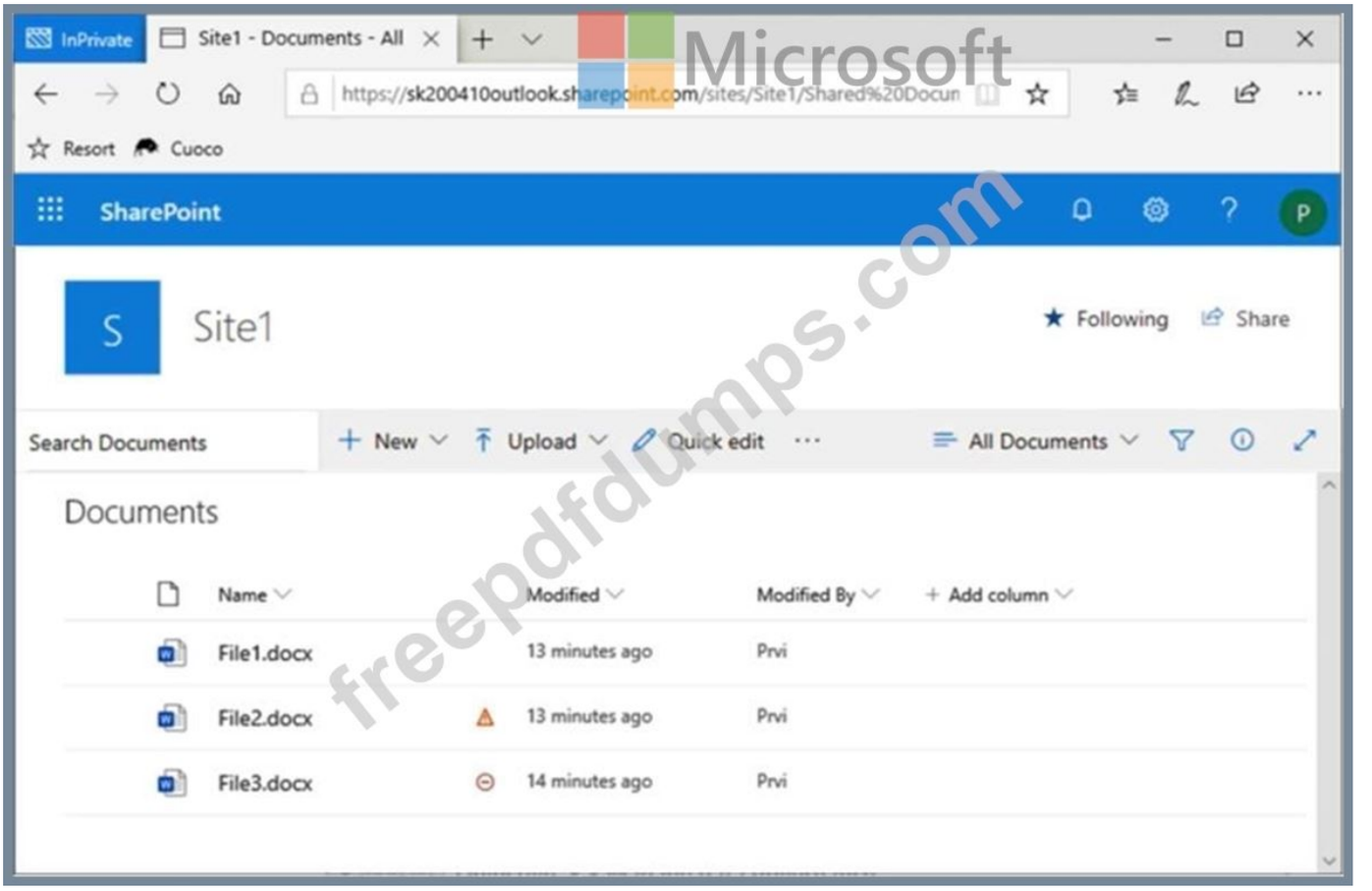
**D.** The policy will apply to only the .docx and .txt files. The policy will classify the files within 24 hours.

**Answer: B (LEAVE A REPLY)**

https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

**NEW QUESTION: 10**
You have a Microsoft 365 E5 subscription. The subscription contains 500 Windows devices that are onboarded to Microsoft Purview.
You need to prevent users from sharing sensitive information with third-party generative AI websites.
Which Microsoft Purview solution should you use?
**A.** Data Loss Prevention
**B.** Insider Risk Management
**C.** Information Protection
**D.** Information Barriers
**Answer: A (LEAVE A REPLY)**
Considerations for DSPM for AI to manage data security and compliance protections for AI interactions To prevent users from sharing sensitive information with third-party generative AI websites when Windows devices are onboarded to Microsoft Purview, you can configure Data Loss Prevention (DLP) policies. These policies allow you to restrict access to specific service domains and block file uploads or sensitive data sharing with those domains.
Reference:
https://learn.microsoft.com/en-us/purview/dspm-for-ai-considerations

**NEW QUESTION: 11**
Hotspot Question
You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and a Microsoft SharePoint Online site named Sitel as shown in the following exhibit.




For Site1, the users are assigned the roles shown in the following table.

| Name | Role |
|---|---|
| User1 | Owner |
| User2 | Member |

You publish a retention label named Retention1 to Site1.

To which files can the users apply Retention1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

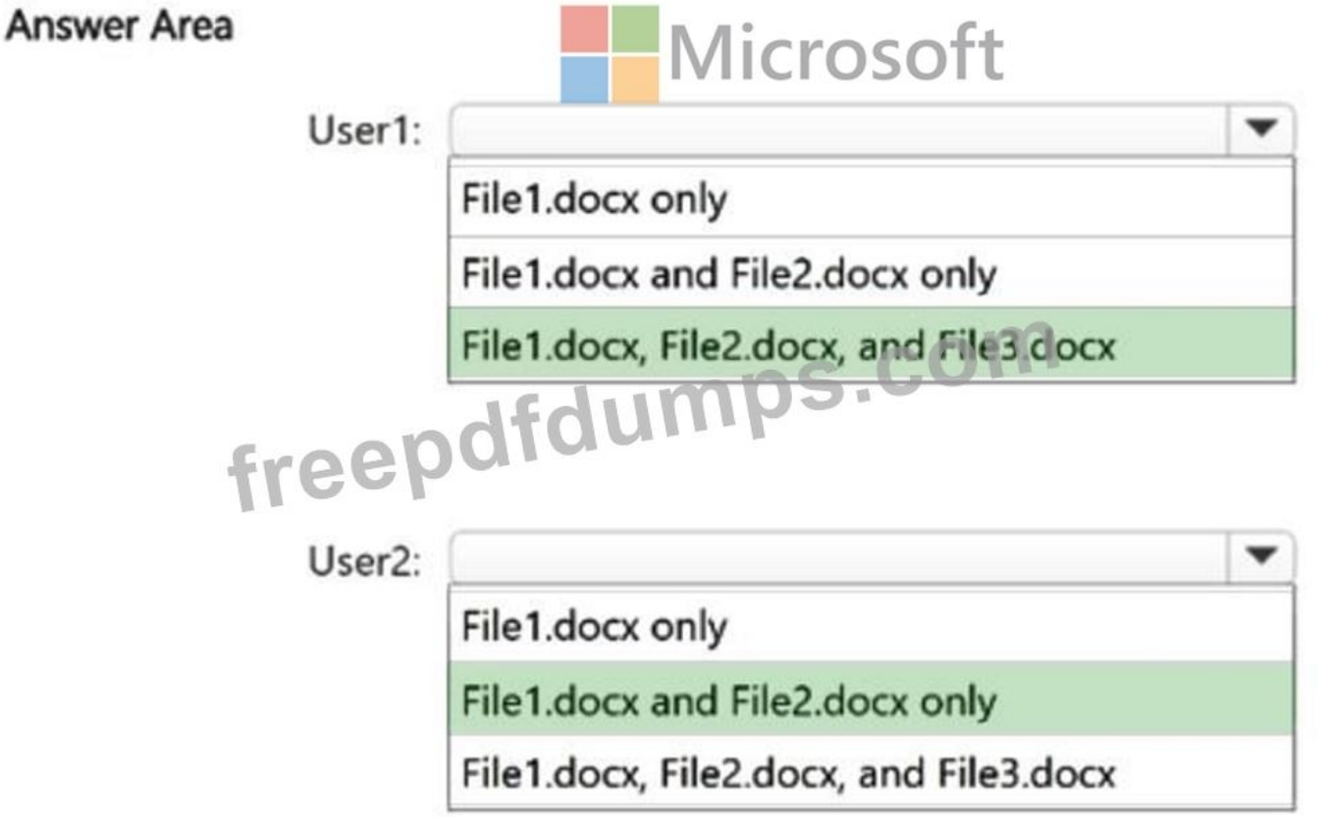
User1:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

**Answer:**





Explanation:
Box 1: File1.docx, File2.docx, and File3.docx
User1 is owner.
Note:
File1 and File2 are normal.
File3 has a red minus-sign (-) denoting the following:
This item is protected by a policy in your organization. It can't be shared with people outside your organization.
Issues
Item contains the following sensitive information: Etc.
Box 2: File1.docx and File2.docx only
User is member and cannot access File3.
Reference:
https://answers.microsoft.com/en-us/msteams/forum/all/a-red-circle-with-a-minus-sign-after-file-name-in/94a98f8e-69e1-46cd-9799-86b4e297ce00

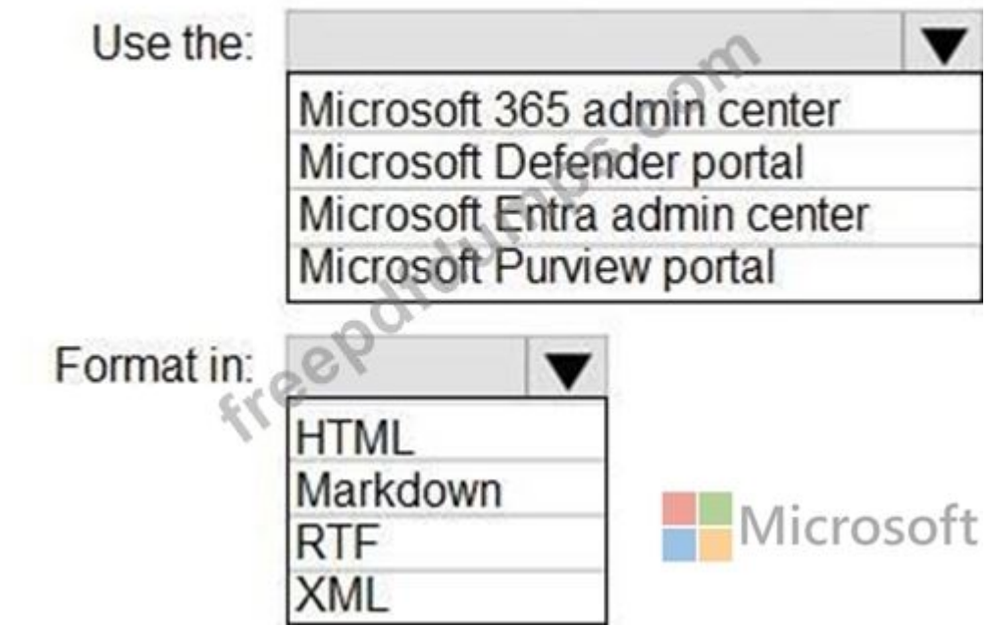
**NEW QUESTION: 12**
You have a Microsoft 365 subscription.
You configure a Microsoft Purview insider risk management policy named Policy1.
You need to ensure that you will receive real-time recommendations on how to configure the indicator thresholds for Policy1. The solution must ensure that the recommendations are based on a user's activity from the past 10 days.

What should you do first?
**A.** Create an Insider Risk Indicators connector.
**B.** Configure the Insider Risk Management Data sharing settings.
**C.** Create a data loss prevention (DLP) policy
**D.** Enable insider risk management analytics.
**Answer: (SHOW ANSWER)**
Prerequisites for using real-time analytics
To use real-time analytics (preview), you must enable insider risk analytics insights. After analytics is enabled, it can take 24 to 48 hours for insights and recommendations to appear.
Note: Adjust threshold settings manually
If you select the Choose your own thresholds option and manually adjust a threshold setting for a specific indicator, the insight below the indicator updates in real time. This helps you configure the appropriate thresholds for each indicator to achieve the highest level of alert effectiveness before activating your policies.
Reference:
https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-policy-indicators

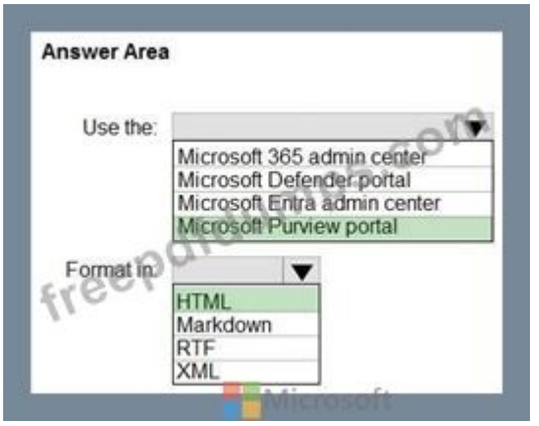
**NEW QUESTION: 13**
You have a Microsoft 365 E5 subscription.
You need to create a sensitivity label named Label1. The solution must ensure that users can use Microsoft 365 Copilot to summarize files that have Label1 applied.
Which permission should you select for Label1?
**A.** Export content(EXPORT)
**B.** Copy and extract content(EXTRACT)
**C.** Edit content(DOCEDIT)
**D.** View rights(VIEW)
**Answer: B (LEAVE A REPLY)**
If content grants a user VIEW usage rights but not EXTRACT:
Copilot won't summarize this content but can reference it with a link so the user can then open and view the content outside Copilot.
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-considerations

**NEW QUESTION: 14**
Hotspot Question
You have a Microsoft 365 E5 subscription.
You are implementing insider risk management.
You need to create an insider risk management notice template and format the message body of the notice template.
How should you configure the template? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

## Answer Area




**Answer:**




Explanation:

Box 1: Microsoft Purview portal

Create insider risk management notice templates

To create a new insider risk management notice template, you'll use the notice creation tool in Insider risk management solution in the Microsoft Purview portal.

Box 2: HTML

HTML for notices

If you'd like to create more than a simple text-based email message for notifications, you can create a more detailed message by using HTML in the message body field of a notice template.

Reference:

https://learn.microsoft.com/en-us/purview/insider-risk-management-notices

**NEW QUESTION: 15**

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.
You need to deploy a Microsoft Purview insider risk management solution that will generate an alert when users share sensitive information on Site1 with external recipients.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct answer is worth one point.
**A.** Turn on analytics.
**B.** Turn on indicators.
**C.** Configure adaptive protection.
**D.** Create an insider risk policy.
**E.** Create a data loss prevention (DLP) policy.
**Answer: B,D (LEAVE A REPLY)**
Turning on indicators is required to enable the monitoring of user activities, such as file sharing and access to sensitive data, which are used by insider risk policies to evaluate risk.
Creating an insider risk policy allows you to define risk scenarios, such as data leaks to external users, and trigger alerts when the policy conditions are met, including sensitive info sharing from SharePoint Online (Site1).
Reference:
https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-policy-indicators

**NEW QUESTION: 16**
You have a Microsoft 365 E5 subscription.
You are implementing insider risk management.
You need to maximize the amount of historical data that is collected when an event is triggered.
What is the maximum number of days that historical data can be collected?
**A.** 60
**B.** 30
**C.** 90
**D.** 180
**Answer: C (LEAVE A REPLY)**



**NEW QUESTION: 17**

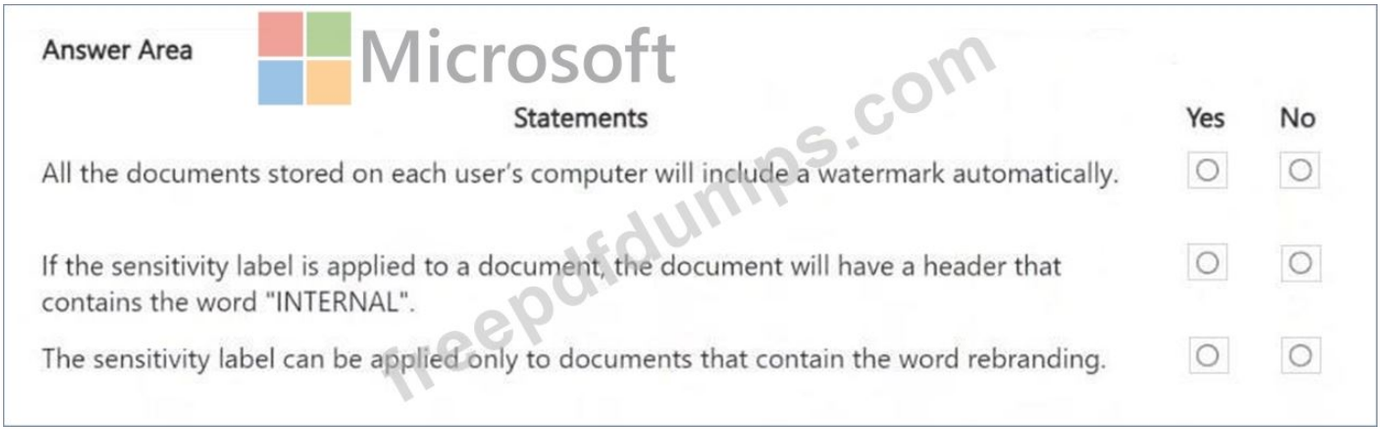
You have a Microsoft 365 E5 subscription.
You have a Microsoft SharePoint Online document library that contains Microsoft Word and Excel documents. The documents contain the following types of information:
- Credit card numbers
- Physical addresses in the UK
- National health service numbers from the UK
- Sensitive projects that contain the following words: Project Tailspin, Project Contoso, and Project Falcon
You have email messages in Microsoft Exchange Online that contain the following information types:
- Credit card numbers
- User sign-in credentials
- National health service numbers from the UK
You plan to use sensitive information types (SITs) for compliance policies.
What is the minimum number of SITs required to classify all the information types?
**A.** 2
**B.** 5
**C.** 7
**D.** 10
**Answer: (SHOW ANSWER)**
* In Documents: Sensitive projects that contain the following words: Project Tailspin, Project Contoso, and Project Falcon - One SIT
* In documents: Physical addresses in the UK - one SIT
* Credit card numbers in documents and emails - one SIT
a single sensitive information type for credit card numbers can be applied to both documents and emails, often as part of a data loss prevention (DLP) or sensitivity labeling system in Microsoft 365 and other platforms. These systems can automatically detect credit card numbers within documents and emails and then apply predefined sensitivity labels that enforce security policies, such as encryption or access restrictions, for both types of content.
* User sign-in credentials in emails - one SIT
* National health service numbers from the UK in documents and emails - one SIT A single sensitive information type classification, such as for UK National Health Service (NHS) numbers, can be applied to both documents and emails, typically by using a data loss prevention (DLP) or sensitivity labelling system within Microsoft 365 or NHSmail. This allows a uniform policy to detect and protect NHS numbers whether they appear in a Word document or an email, ensuring consistent security protocols across different data formats within the NHS environment.
Reference:
https://learn.microsoft.com/en-us/purview/sit-sensitive-information-type-learn-about

**NEW QUESTION: 18**
Hotspot Question

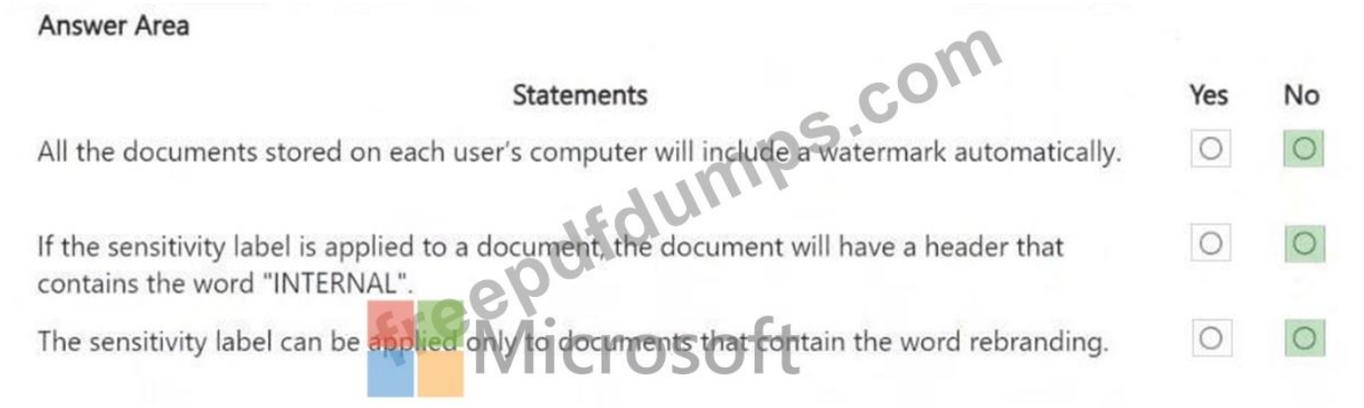
You have a Microsoft 365 sensitivity label that is published to all the users in your Microsoft Entra tenant as shown in the following exhibit.




For each of the following statements, select Yes if the statement is true. Otherwise, select No.




**Answer:**




Explanation:

Statement 1 - No. The sensitivity label includes content marking (watermark: INTERNAL), but it only applies to documents where the label is manually or automatically applied, not to all documents by default.

Statement 2 - No. The sensitivity label only specifies a watermark, not a header. If a header marking was configured, it would explicitly appear in the label settings.

Statement 3 - No. There is no indication that auto-labeling is configured to apply the label only to documents with the word "rebranding". Auto-labeling is an optional setting that needs explicit configuration.

**NEW QUESTION: 19**

Hotspot Question

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. | ○ | ○ |

**Answer:**

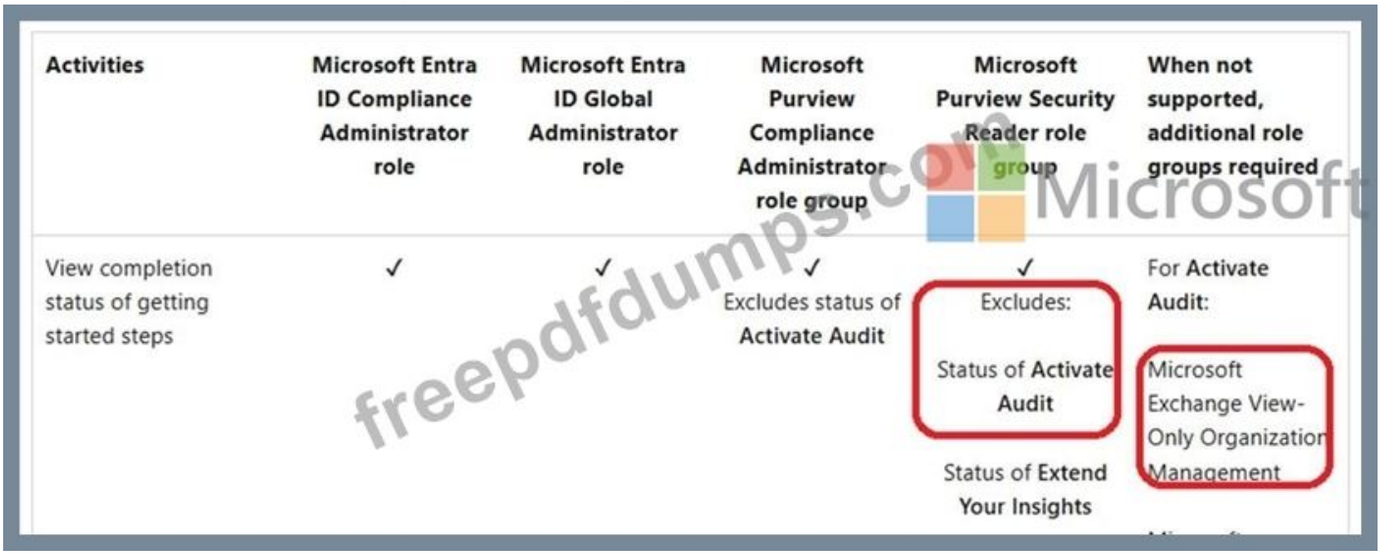
Answer Area

| 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. | ○ | ○ |

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: 20**
You have a Microsoft 365 E5 subscription that contains a user named User1.
You deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI).
You need to ensure that User1 can verify the auditing status of the subscription. The solution must follow the principle of least privilege.
To which role group should you add User1?
**A.** Security Reader
**B.** Insider Risk Management Analysts
**C.** Insider Risk Management Investigators
**D.** View-Only Organization Management for Microsoft Exchange Online
**Answer: (SHOW ANSWER)**
Permissions for Data Security Posture Management for AI



| Activities | Microsoft Entra ID Compliance Administrator role | Microsoft Entra ID Global Administrator role | Microsoft Purview Compliance Administrator role group | Microsoft Purview Security Reader role group | When not supported, additional role groups required |
|---|---|---|---|---|---|
| View completion status of getting started steps | ✓ | ✓ | ✓ Excludes status of Activate Audit | ✓ Excludes: Status of Activate Audit; Status of Extend Your Insights | For Activate Audit: Microsoft Exchange View-Only Organization Management |



Note: Roles and role groups that can view, create, and edit in Data Security Posture Management for AI:
Microsoft Entra ID Compliance Administrator role
Microsoft Entra ID Global Administrator role
Microsoft Purview Compliance Administrator role group
Roles and role groups that can view-only in Data Security Posture Management for AI:
Microsoft Purview Security Reader role group
Reference:
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-permissions

**NEW QUESTION: 21**
You have a Microsoft 365 E5 subscription.

You create a sensitivity label named Label1 and publish Label1 to all users and groups.
You have the following files on a computer:
- File1.doc
- File2.docx
- File3.xlsx
- File4.txt
You need to identify which files can have Label1 applied.
Which files should you identify?
**A.** File2.docx only
**B.** File2.docx and File3.xlsx only
**C.** File1.doc, File2.docx, and File3.xlsx only
**D.** File1.doc, File2.docx, File3.xlsx, and File4.txt
**Answer: B (LEAVE A REPLY)**
https://learn.microsoft.com/en-us/purview/sensitivity-labels-office-apps#office-file-types-supported

**NEW QUESTION: 22**
Hotspot Question
You have two Microsoft 365 subscriptions named Contoso and Fabrikam. The subscriptions contain the users shown in the following table.

| Name | Subscription | Email address |
|---|---|---|
| User1 | Contoso | user1@contoso.com |
| User2 | Contoso | user2@contoso.com |
| User3 | Fabrikam | user3@fabrikam.com |
| User4 | Fabrikam | user4@fabrikam.com |

You have a sensitivity label named Sensitivity1 as shown in the exhibit. (Click the Exhibit tab)

# Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. Learn more about access control settings

- ○ Remove access control settings if already applied to items
- ◉ Configure access control settings

ⓘ Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. Learn more about this setting

Go to co-authoring setting

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

Never

Allow offline access ⓘ

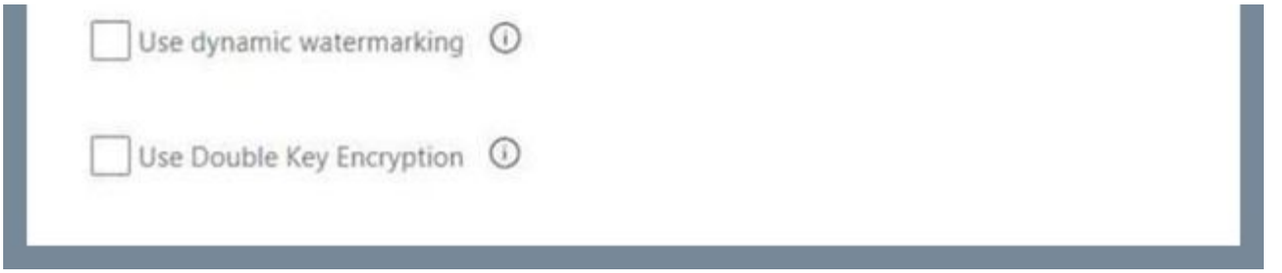
Always

**Assign permissions to specific users and groups** * ⓘ

Assign permissions

2 items

| Users and groups | Permissions | Edit | Delete |
|---|---|---|---|
| contoso.com | Co-Owner | | |
| fabrikam.com | Reviewer | | |




You have the files shown in the following table.

| Name | Sensitivity1 |
|---|---|
| File1 | Automatically applied by using an auto-labeling policy |
| File2 | Applied by User2 |
| File3 | Applied by User1 |

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 |
|---|---|---|
| User1 can edit rights for File1. | ○ | ○ |
| User2 can edit rights for File3. | ○ | ○ |
| User3 can print File2. | ○ | ○ |

**Answer:**


Explanation:
Box 1: Yes
User1 is in the Contoso subscription, and has the email address user1@contoso.com Sensitivity label Sensitiviy1 has assigned contoso.com users Co-owner permissions.

For File1 has Sensitiviy1 been automaticallyapplied by using an auto-labeling policy.
Box 2: Yes
User2 is in the Contoso subscription, and has the email address user2@contoso.com Sensitivity label Sensitiviy1 has assigned contoso.com users Co-owner permissions.
For File3 has Sensitiviy1 been applied by User1.
Box 3: No
User3 is in the Fabrikam subscription, and has the email address user3@fabrikam.com
Sensitivity label Sensitiviy1 has assigned fabrikam.com users reviewer permissions.
For File2 has Sensitiviy1 been applied by User2.
Reference:
https://learn.microsoft.com/en-us/purview/encryption-sensitivity-labels

**NEW QUESTION: 23**
You have a Microsoft 365 tenant that is opt-in for trainable classifiers.
You need to ensure that a user named User1 can create custom trainable classifiers. The solution must use the principle of least privilege.
Which role should you assign to User1?
**A.** Security Administrator
**B.** Compliance Administrator
**C.** Global Administrator
**D.** Security Operator
**Answer: (SHOW ANSWER)**
In Microsoft 365, the minimum required role to create custom trainable classifiers is Compliance Administrator. While Global Administrator and Security Administrator roles may also have the necessary permissions, the Compliance Administrator role is the most directly aligned with this specific task.
Reference:
https://learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with

**NEW QUESTION: 24**
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 Exchange email, SharePoint sites, OneDrive accounts, and Teams chat and channel messages selected.

Does this meet the goal?

**A.** Yes

**B.** No

**Answer: (SHOW ANSWER)**

Correct:

* You create a data loss prevention (DLP) policy that has only the Exchange email location selected.

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.

* You create a data loss prevention (DLP) policy that has Exchange email, SharePoint sites, OneDrive accounts, and Teams chat and channel messages selected.OneDrive accounts, and Teams chat and channel messages selected.

Creating a Data Loss Prevention (DLP) policy that includes Exchange email as a location can help detect and prevent the sharing of sensitive information, like Azure Storage keys, in plain text. By setting up a DLP policy with conditions to identify Azure Storage keys and enforce encryption or blocking actions for Exchange email, the policy will ensure that any emails containing such sensitive information are either encrypted or prevented from being sent.

Incorrect:

* You configure a mail flow rule that matches a sensitive info type.

* You configure a mail flow rule that matches the text patterns.

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.

* You create a data loss prevention (DLP) policy that has all locations selected.

Reference:

https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mail-flow-rules/conditions-and-exceptions

**NEW QUESTION: 25**

You have a Microsoft 365 E5 subscription that contains 500 Windows devices.

You plan to deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI).

You need to ensure that you can monitor user activities on third-party generative AI websites.

Which two prerequisites should you complete for DSPM for AI? Each correct answer presents part of the solution, NOTE: Each correct selection is worth one point.

**A.** Create an Endpoint data loss prevention (Endpoint DLP) policy.
**B.** Onboard the devices to Microsoft Purview.
**C.** Install the Microsoft Purview extension on the devices.
**D.** Create a communication compliance policy.
**E.** Enroll the devices in Microsoft Intune.
**F.** Create a data leaks policy.
**Answer: (SHOW ANSWER)**
Required for monitoring interactions with third-party generative AI sites:
[B] * Devices are onboarded to Microsoft Purview, required for:
- Gaining visibility into sensitive information that's shared with third-party generative AI sites. For example, a user pastes credit card numbers into ChatGPT.
[A]- Applying endpoint DLP policies to warn or block users from sharing sensitive information with third-party generative AI sites. For example, a user identified as elevated risk in Adaptive Protection is blocked with the option to override when they paste credit card numbers into ChatGPT.
Reference:
https://learn.microsoft.com/en-us/purview/dspm-for-ai-considerations

**NEW QUESTION: 26**
You have a Microsoft 365 E5 tenant that has a retention label named Label1.
You need to create an auto-labeling policy that will apply Label1.
To which location can Label1 be applied?
**A.** Teams channel messages
**B.** OneDrive accounts
**C.** on-premises repositories
**D.** Teams chats
**Answer: B (LEAVE A REPLY)**
Correct:
* OneDrive accounts
Incorrect:
* Microsoft Defender for Cloud Apps
* Microsoft Entra security groups
* on-premises repositories
* Teams channel messages
* Teams chats
Note:
A Microsoft 365 auto-labeling policy can be applied to Exchange mailboxes, SharePoint sites, and OneDrive accounts. It can also be applied to content within Teams and other Microsoft 365 Groups, as well as Azure services like Azure SQL and Azure Cosmos DB.
Exchange Online: Applies to emails in transit.
SharePoint: Applies to documents stored at rest in SharePoint sites.

OneDrive: Applies to documents stored at rest in OneDrive accounts.

Teams: Applies to documents stored in the SharePoint sites associated with a Team.

Azure and other data sources: Can be extended to apply to data stored in services like Azure SQL, Azure Cosmos DB, and more.

Reference:
https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically

**NEW QUESTION: 27**

Hotspot Question

You have a Microsoft 365 E5 subscription that contains three users named User, User2, and User3. The subscription contains the groups shown in the following table.

| Name | Members |
|---|---|
| Group1 | User1 |
| Group2 | User2, User3 |
| Group3 | User2, User2, User3 |

The subscription contains the devices shown in the following table.

| Name | Platform |
|---|---|
| Device1 | Windows |
| Device2 | Android |
| Device3 | macOS |

All the devices are onboarded to Microsoft Purview.

You have the data loss prevention (DLP) policies shown in the following table.

| Name | Assigned to | Description |
|---|---|---|
| Policy1 | Group1 | Restrict copying data to USB devices. |
| Policy2 | Group2 | Restrict copying data to a clipboard. |
| Policy3 | Group3 | Restrict accessing corporate content in Microsoft 365 locations. |

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 |
|---|---|---|
| When User1 signs in to Device1, the user will be restricted from copying data to a USB storage device. | ○ | ○ |
| When User2 signs in to Device2, the user will be restricted from copying data to the clipboard. | ○ | ○ |
| When User3 signs in to Device3, the user will be restricted from accessing corporate content in Microsoft SharePoint Online. | ○ | ○ |

**Answer:**

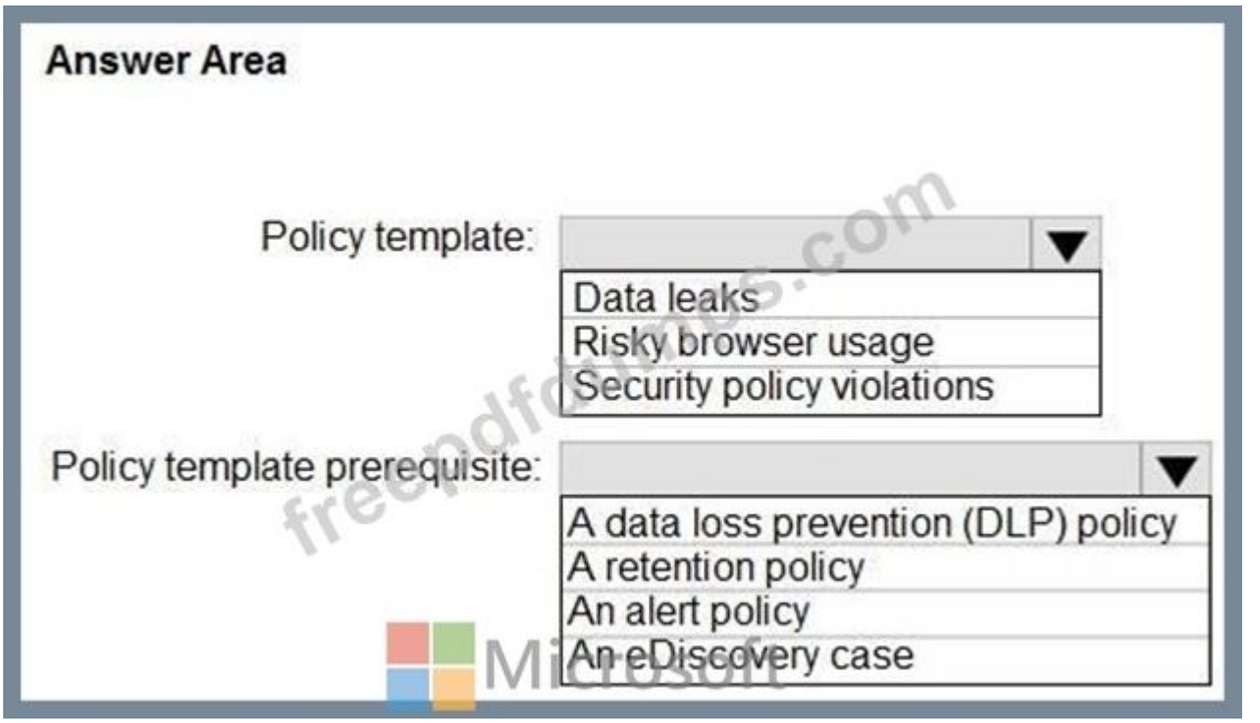
**Answer Area**

| Statements | Yes | No |
|---|---|---|
| When User1 signs in to Device1, the user will be restricted from copying data to a USB storage device. | ○ | ○ |
| When User2 signs in to Device2, the user will be restricted from copying data to the clipboard. | ○ | ○ |
| When User3 signs in to Device3, the user will be restricted from accessing corporate content in Microsoft SharePoint Online. | ○ | ○ |

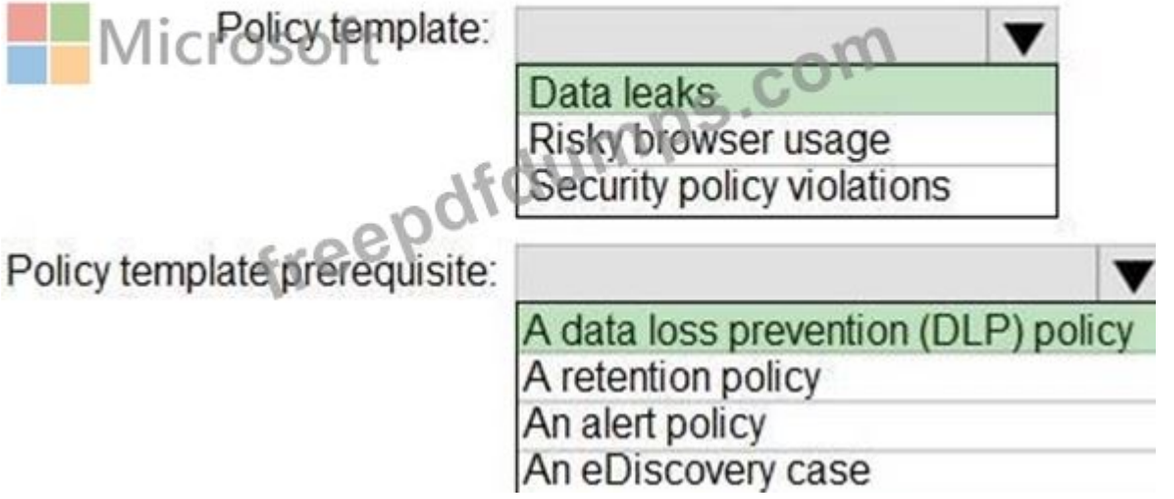


Explanation:
Box 1: Yes
User1 is member of Group1 and of Group3.
Device1 is Windows.
Policy1 is assigned to Group1, and restrict copying to USB [assume this is the intended word] devices.
Note:
Supported actions: Devices
You can tell DLP to Allow, Audit only, Block with override, or Block (the actions) these user activities for onboarded Windows devices.
Box 2: No
User2 is member of Group2 and of Group3.
Device1 is Android.
The device actions do not apply for Android devices.
Box 3: Yes
User3 is member of Group 1, Group2 and of Group3.
Device1 is macOS.
Policy3 is assigned to Group3, and restricts accessing corporate content in Microsoft 365 locations.
Reference:
https://learn.microsoft.com/en-us/purview/dlp-policy-reference

**NEW QUESTION: 28**
Hotspot Question
You have a Microsoft 365 E5 subscription that uses Microsoft Purview.
You need to deploy a compliance solution that will detect the accidental oversharing of information outside of an organization. The solution must minimize administrative effort.
What should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.




**Answer:**




Explanation:

Box 1: Data leaks

When using a Data leaks template, you can assign a DLP policy to trigger indicators in the insider risk policy for high severity alerts in your organization. Whenever a high severity alert is generated by a DLP policy rule is added to the Office 365 audit log, insider risk policies created with this template automatically examine the high severity DLP alert. If the alert contains an in-scope user defined in the insider risk policy, the alert is processed by the insider risk policy as a new alert and assigned an insider risk severity and risk score. You can also choose to assign selected indicators as triggering events for a policy. This flexibility and customization helps scope the policy to only the activities covered by the indicators. This policy allows you to evaluate this alert in context with other activities included in the case.

Box 2: A data loss prevention (DLP) policy
Note: Data leaks
Protecting data and preventing data leaks is a constant challenge for most organizations, particularly with the rapid growth of new data created by users, devices, and services. Users are empowered to create, store, and share information across services and devices that make managing data leaks increasingly more complex and difficult. Data leaks can include *accidental oversharing of information outside your organization* or data theft with malicious intent. With an assigned Microsoft Purview Data Loss Prevention (DLP) policy, built-in, or customizable triggering events, this template starts scoring real-time detections of suspicious SharePoint Online data downloads, file and folder sharing, printing files, and copying data to personal cloud messaging and storage services.
Reference:
https://learn.microsoft.com/en-us/purview/insider-risk-management-policy-templates

**NEW QUESTION: 29**
Hotspot Question
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:**


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: 30**

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 Defender portal create an activity policy.

**B.** From the Microsoft Purview portal start an Advanced eDiscovery search.

**C.** From the Exchange admin center, create a data loss prevention (DLP) policy.

**D.** From the Microsoft Defender portal, create a file policy.

**Answer: (SHOW ANSWER)**

After you connect an app to Defender for Cloud Apps, integrate with Microsoft Purview Information Protection. Then, in the Files page, filter for files labeled Confidential and exclude your domain in the Collaborators filter. If you see that there are confidential files shared outside your organization, you can create a file policy to detect them.

Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/file-filters

https://learn.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers

**NEW QUESTION: 31**

Hotspot Question

You have a Microsoft 365 E5 subscription that contains the sensitive information types (SITs) shown in the following table.

| Name | Detection method |
|---|---|
| SIT1 | Fingerprint |
| SIT2 | Regular expression |

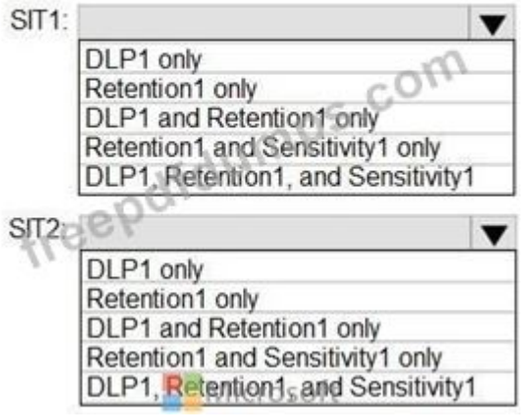
You plan to create the policies shown in the following table and assign them to a Microsoft SharePoint Online site.

| Name | Type |
|---|---|
| DLP1 | Data loss prevention (DLP) policy |
| Retention1 | Retention label auto-labeling policy |
| Sensitivity1 | Sensitivity label auto-labeling policy |

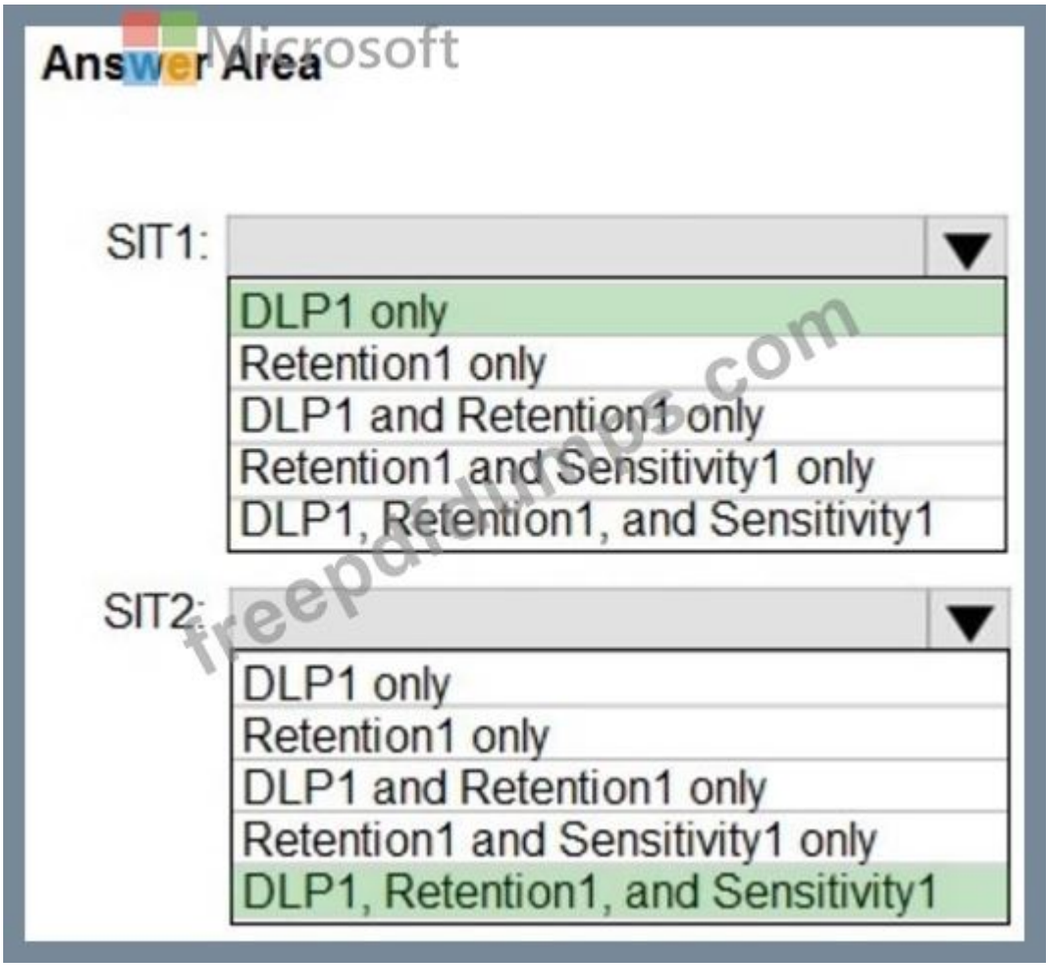
Which policies can use SIT1, and which policies can use SIT2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**




**Answer:**




Explanation:

Box 1: DLP1 only

Document fingerprinting in Microsoft Purview creates sensitive information types (SITs) usable only in Data Loss Prevention (DLP) policies across Exchange, SharePoint, OneDrive, Teams, and Devices, as well as Microsoft Information Protection (MIP) auto-labeling in Exchange, SharePoint, and OneDrive.

Box 2: DLP1, Retention1, and Sensitivity1

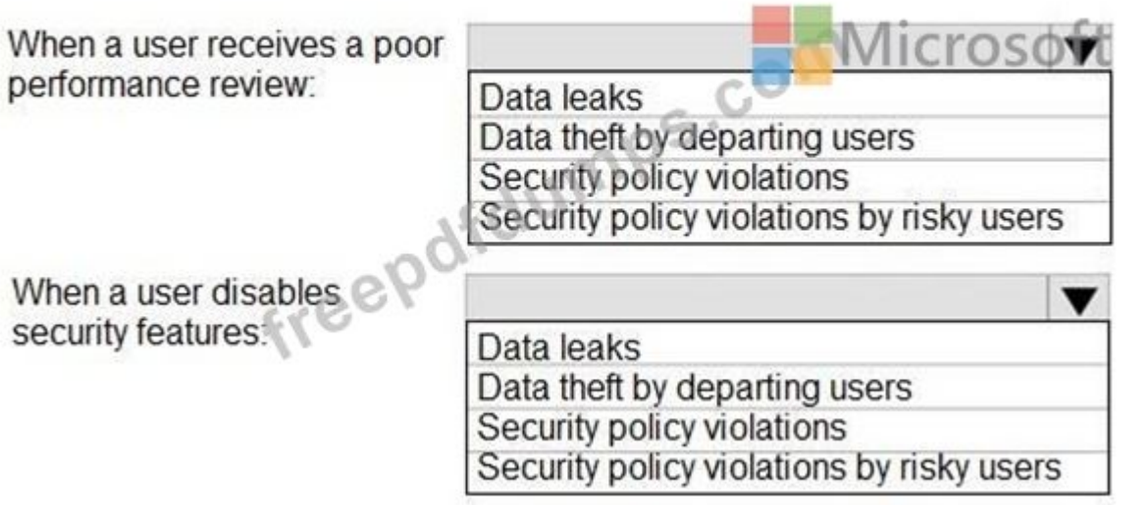
Regex-based custom SITs support broader Purview solutions including DLP policies, retention policies, and sensitivity label auto-apply rules, enabling pattern matching for sensitive data

detection across compliance workloads.
Reference:
https://learn.microsoft.com/en-us/purview/sit-document-fingerprinting
https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically

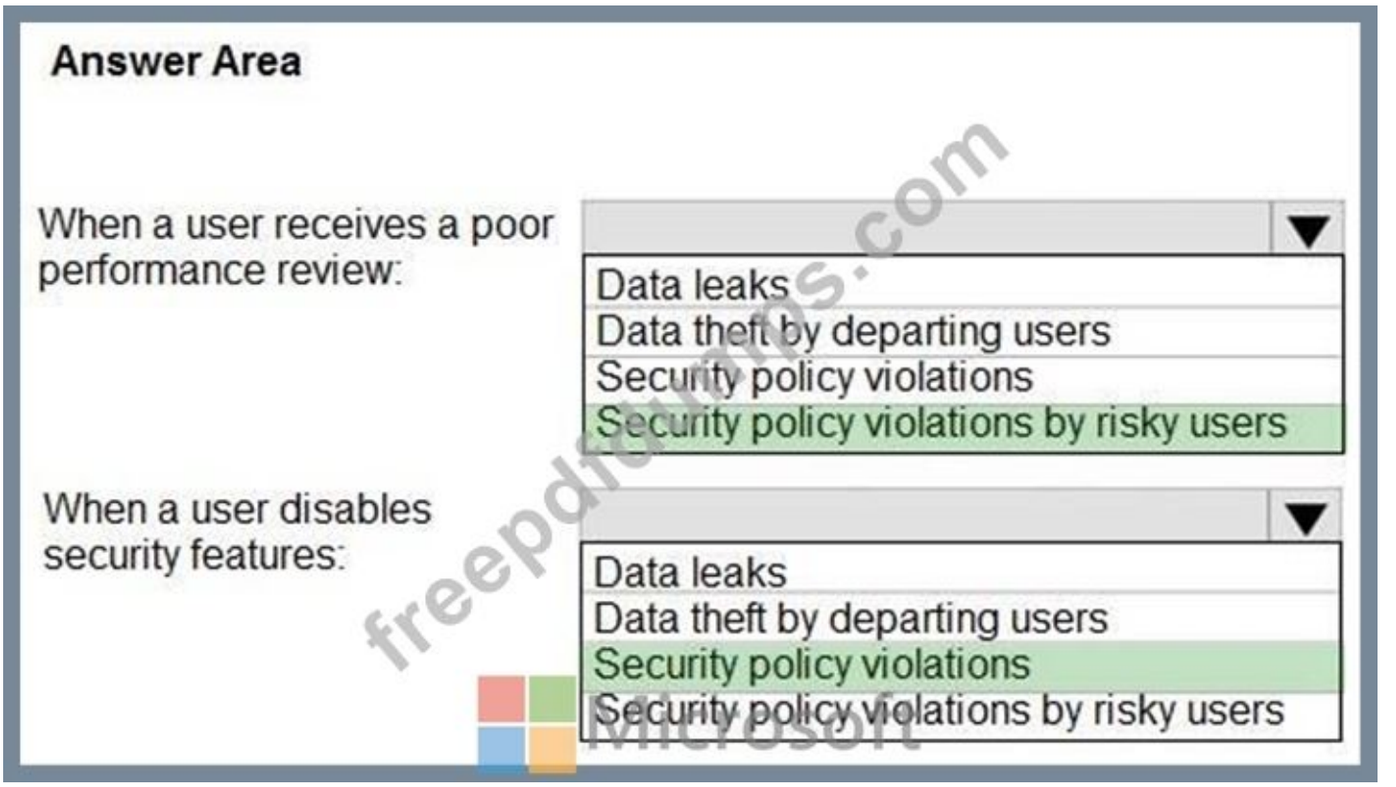


**NEW QUESTION: 32**
Hotspot Question
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft Purview insider risk management.
You need to recommend policy templates that meet the following requirements:
- Contain risk indicators and scoring for when a user receives a poor performance review.
- Contain risk indicators and scoring for when a user disables security features on a device.
Which template should you use for each requirement? To answer, select the appropriate options in the answer area, NOTE: Each correct selection is worth one point.

**Answer Area**




**Answer:**




Explanation:

Box 1: Security policy violations by risky users

Contain risk indicators and scoring for when a user receives a poor performance review.

Security policy violations by risky users

Users that experience employment stressors might be at a higher risk for inadvertent or malicious security policy violations. These stressors could include a user being placed on a performance improvement plan, having a poor performance review, or experiencing a demotion. This policy template starts risk scoring based on these indicators and activities associated with these types of events.

Box 2: Security policy violations

Contain risk indicators and scoring for when a user disables security features on a device.

Security policy violations

In many organizations, users have permission to install software on their devices or to modify device settings to help with their tasks. Either inadvertently or with malicious intent, users might install malware or *disable important security features* that help protect information on their device or on your network resources. This policy template uses security alerts from Microsoft Defender for Endpoint to start scoring these activities and focus detection and alerts to this risk area. Use this template to provide insights for security policy violations in scenarios when users might have a history of security policy violations that might be an indicator of insider risk.

Reference:

https://learn.microsoft.com/en-us/purview/insider-risk-management-policy-templates

**NEW QUESTION: 33**

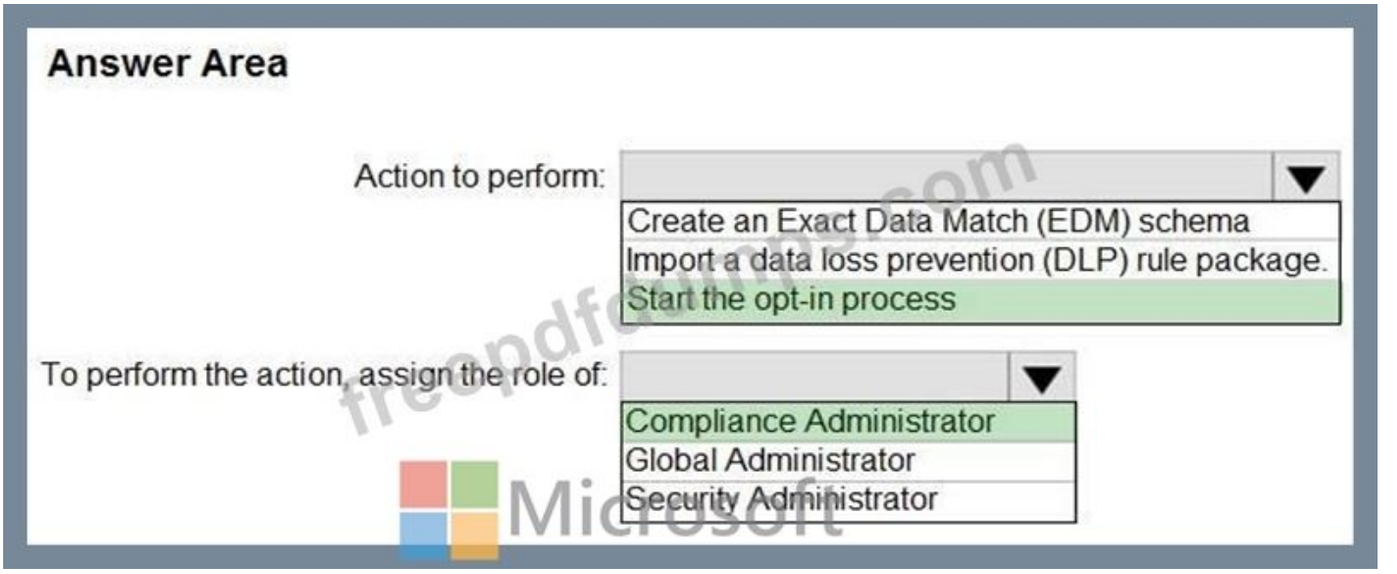
Note: This question is part of a series of questions that present the same scenario. Each question

in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1.
Solution: You run the Set-Mailbox -Identity "User1" -AuditEnabled $true command.
Does that meet the goal?
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
To track who accesses User1's mailbox, you need to enable mailbox auditing for User1. By default, Exchange mailbox auditing is not enabled per mailbox (even though it is enabled tenant-wide).
The Set-Mailbox -Identity "User1" -AuditEnabled $true command enables audit logging for mailbox actions like:
*Read emails
*Delete emails
*Send emails as User1
*Access by delegated users
Once enabled, you can search for future sign-ins and actions in the Microsoft Purview audit logs.

**NEW QUESTION: 34**
Hotspot Question
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**


**Answer:**




Explanation:

The opt-in can't be performed by the Compliance Administrator, the GA is required:

"To access classifiers in the UI:

the Global admin needs to opt in for the tenant to create custom classifiers.

Compliance Administrator role is required to train a classifier."

https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started- with?view=o365-worldwide

**NEW QUESTION: 35**

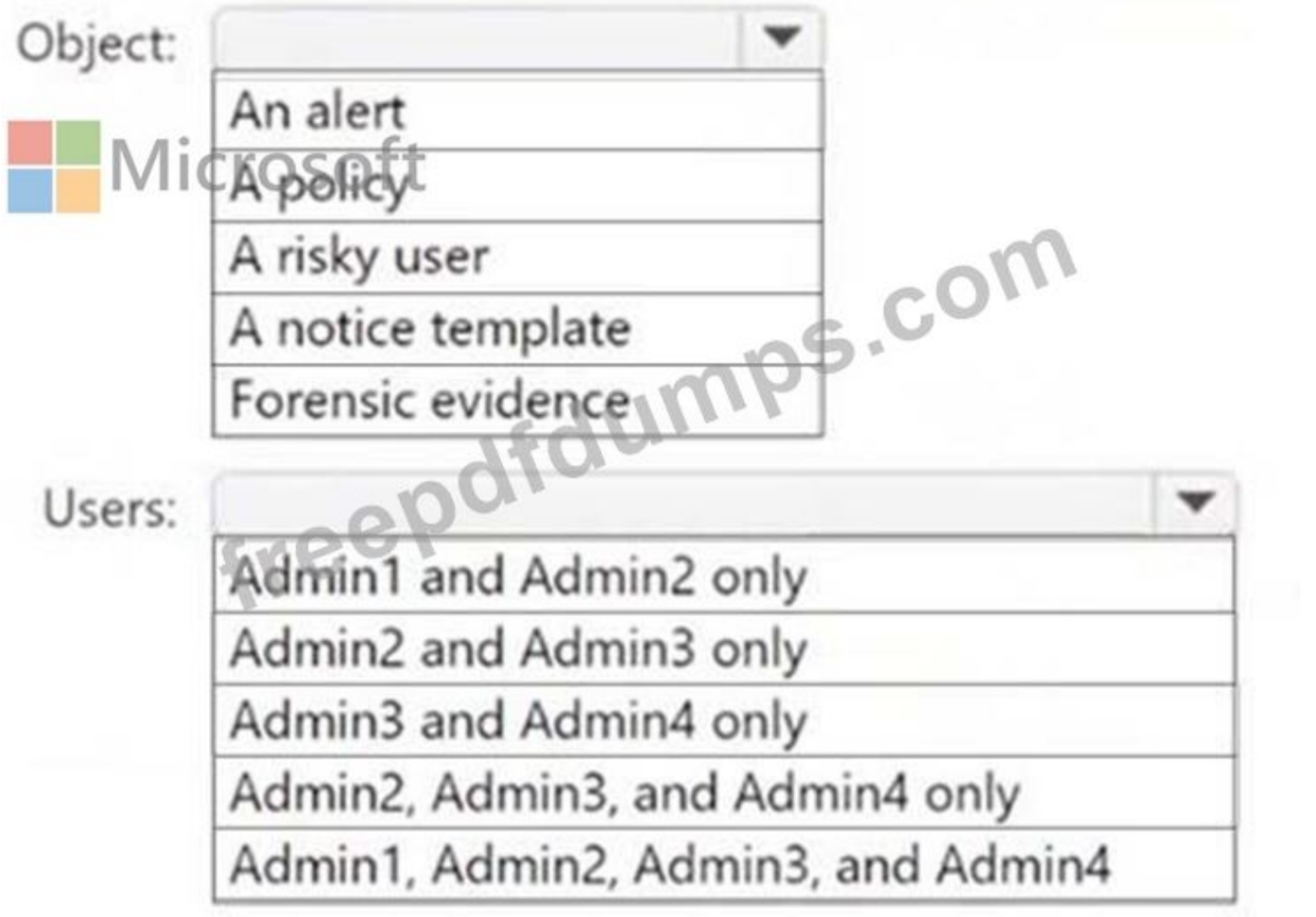
Hotspot Question

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 |

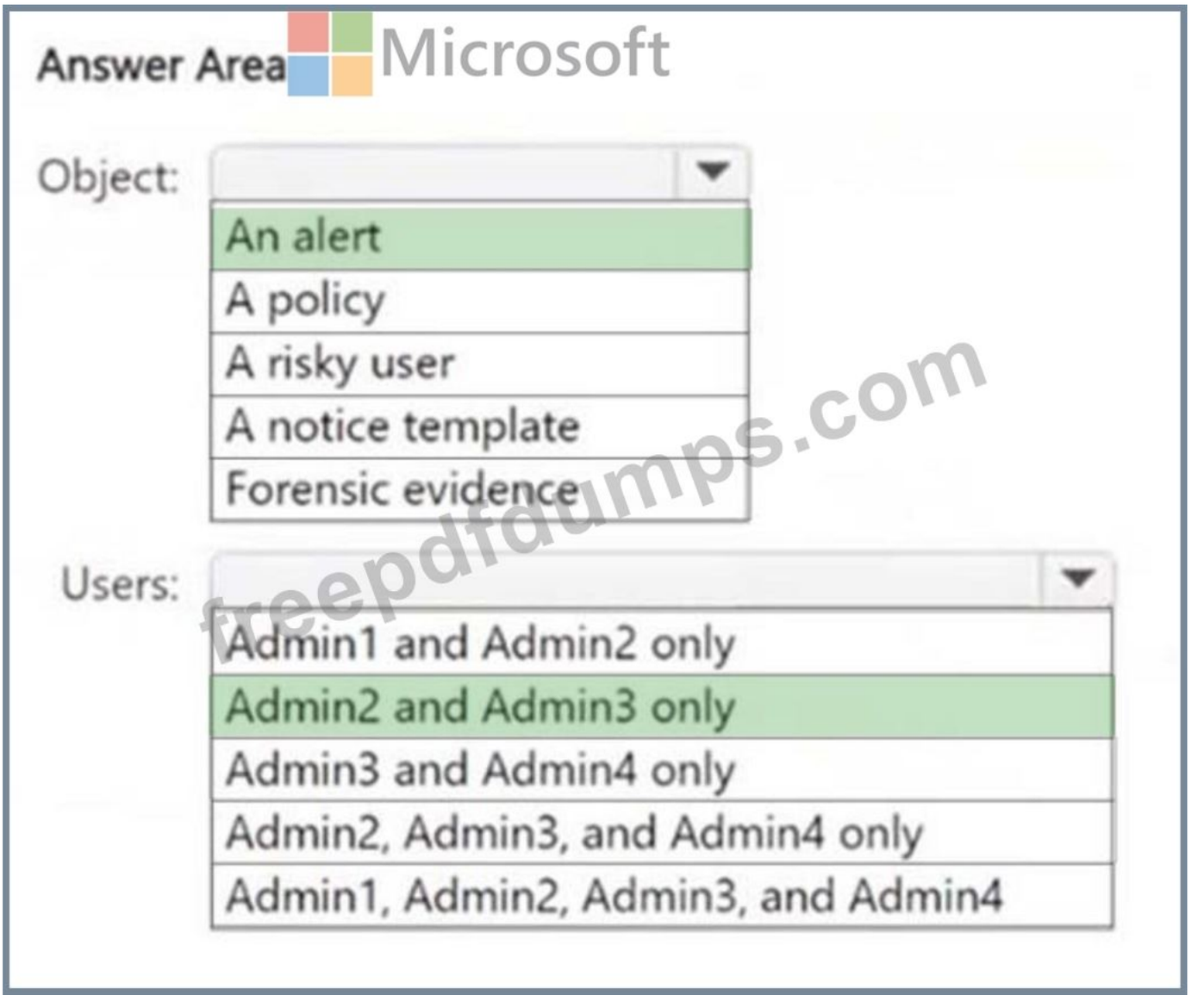
You plan to create a Microsoft Purview insider risk management case named Case1.
Which insider risk management object should you select first, and which users will be added as contributors for Case1 by default?
To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**






**Answer:**





Explanation:

Box 1: An alert

To create a case in Microsoft Purview insider risk management, you always start from an alert.

Box 2: Admin2 and Admin3 only

Only Admin2 and Admin3 are added as contributors by default, because their roles involve investigation and analysis.

**NEW QUESTION: 36**

You have a Microsoft 365 subscription. You create a retention policy and apply the policy to Exchange Online mailboxes.

You need to ensure that the retention policy tags can be assigned to mailbox items as soon as possible.

What should you do?

**A.** From the Microsoft Purview portal, create a data loss prevention (DLP) policy.

**B.** From the Microsoft Purview portal, create a label policy.

**C.** From Exchange Online PowerShell, run Start-ManagedFolderAssistant.

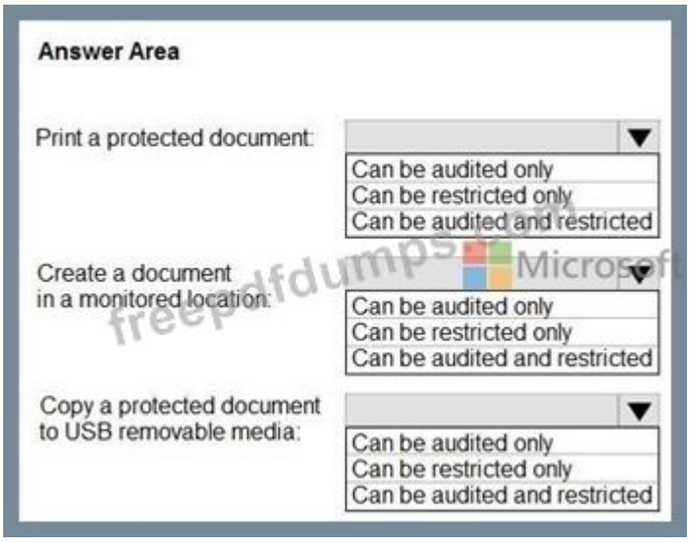
**D.** From Exchange Online PowerShell, run Start-RetentionAutoTagLearning.

**Answer: C (LEAVE A REPLY)**
The Managed Folder Assistant (MFA) is an Exchange Mailbox Assistant that applies and processes the message retention settings that are configured in retention policies.
As in Exchange 2013, the Managed Folder Assistant in Exchange 2016 and Exchange 2019 is a throttle-based assistant that's always running. The MFA doesn't need to be scheduled, and the system resources that are consumed by the MFA can be throttled. You can configure the Managed Folder Assistant to process all mailboxes on a Mailbox server within a certain time period that's known as a work cycle. By default, the work cycle for the MFA is one day (all mailboxes on the server are processed by the MFA every day).
You can also force the MFA to immediately process a specified mailbox.
Reference:
https://learn.microsoft.com/en-us/exchange/policy-and-compliance/mrm/configure-managed-folder-assistant

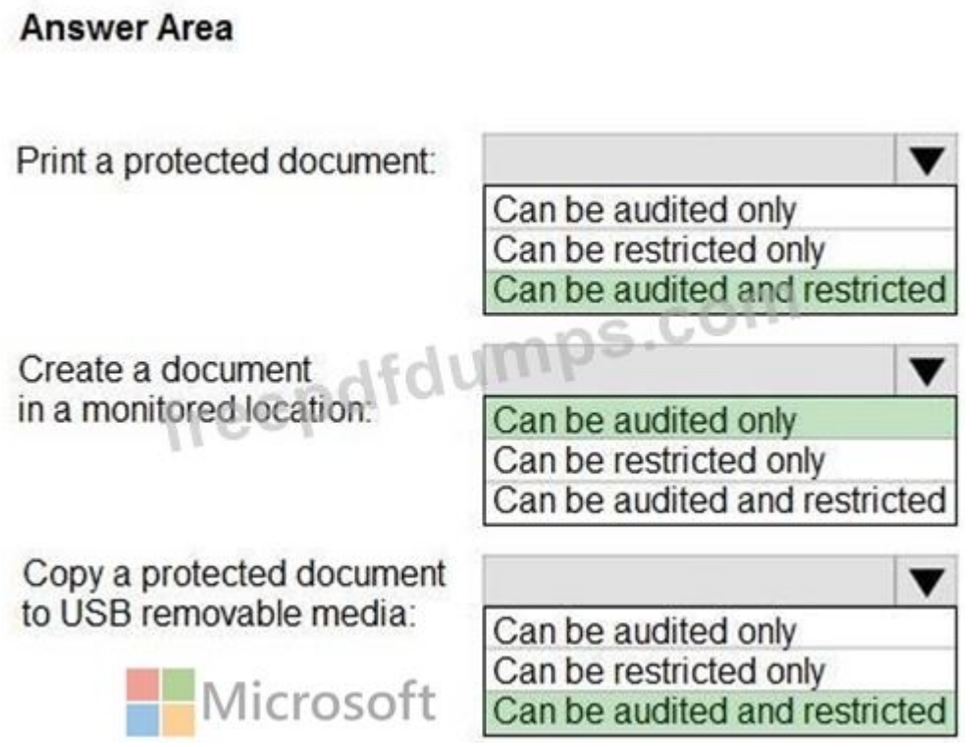
**NEW QUESTION: 37**
You have a Microsoft 365 E5 subscription.
You need to review a Microsoft 365 Copilot usage report.
From where should you review the report?
**A.** Information Protection in the Microsoft Purview portal
**B.** the Microsoft 365 admin center
**C.** DSPM for AI in the Microsoft Purview portal
**D.** the Microsoft Defender portal
**Answer: B (LEAVE A REPLY)**
To review the Microsoft 365 Copilot usage report:
- Go to the Microsoft 365 admin center.
- Navigate to Reports > Usage.
- Select Copilot to view adoption and usage metrics.
The admin center provides insights into how Copilot is being used across your organization, helping you track engagement and effectiveness.
Data Security Posture Management (DSPM) for AI in the Microsoft Purview portal provides insights into AI usage, but it focuses on security and compliance rather than standard usage metrics.
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview

**NEW QUESTION: 38**
Hotspot Question
You plan to implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).
You need to identify which end user activities can be audited on the endpoints, and which activities can be restricted on the endpoints.
What should you identify for each activity? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.




**Answer:**




Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about

**NEW QUESTION: 39**

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 (LEAVE A REPLY)**
Mailflow Rules in Exchange Admin Center and DLP Policies in the Security Center, both can achieve the same, Encrypt emails based on sensitive information types detected in the message body.

**NEW QUESTION: 40**
You have a Microsoft 365 subscription that contains the users shown in the following table.

| Name | Assigned license |
|---|---|
| User1 | Microsoft 365 E3 |
| User2 | Microsoft 365 F3 |
| User3 | Microsoft 365 E5 |

You review the audit retention period of each user.
Which users' audit logs are retained for nine months?
**A.** User3 only
**B.** User1 and User3
**C.** User1, User2, and User3
**D.** User2 and User3
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 41**
Hotspot Question
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 |

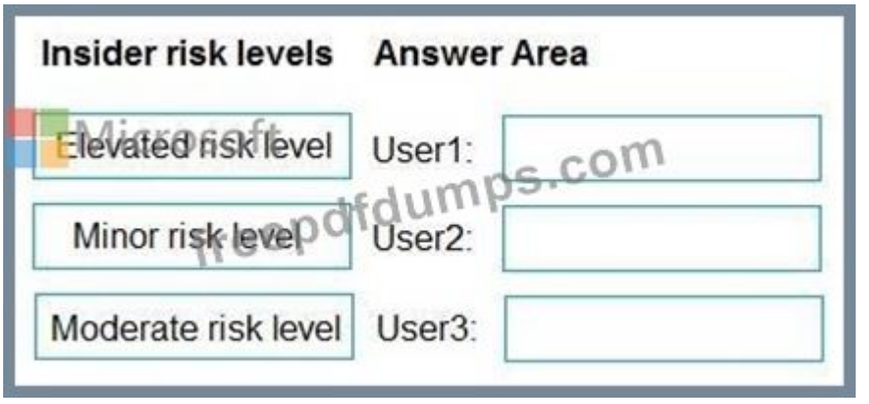
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.


**Answer:**

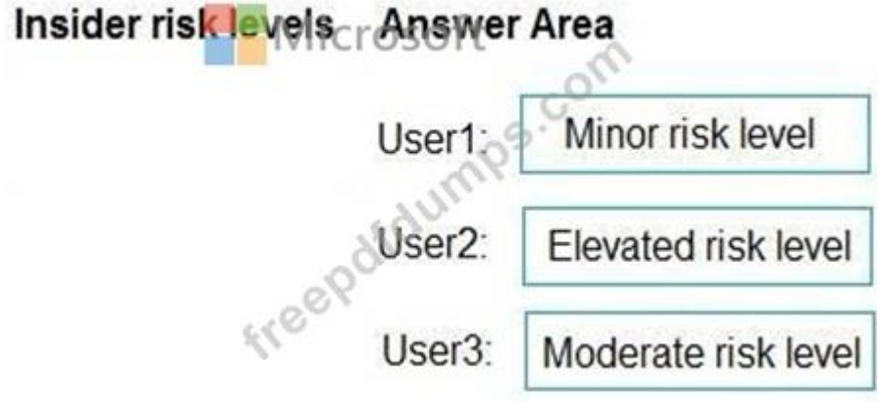

Explanation:
Summary1 is based on File1 and File3. File3 has Label2 applied, and Label2 has content marking enabled, meaning the label persists in derived content. Since File3 contributes to Summary1, Summary1 inherits the sensitivity label from File3.
Summary2 is based on File2, which has Label1 applied. Label1 grants viewer permissions to

authenticated users, but content marking is disabled.
Since the label still applies to the content, Summary2 inherits Label1.
Summary3 is based on File1, File2, and File3. File2 has Label1 applied, and File3 has Label2 applied, meaning the summary will inherit at least one of these labels. Since at least one labeled file is used, the summary inherits a sensitivity label.

**NEW QUESTION: 42**
Drag and Drop Question
You have a Microsoft 365 5 subscription that uses Microsoft Purview insider risk management and contains three users named User1, User2, and User3.
All insider risk management policies have adaptive protection enabled and the default conditions for insider risk levels configured.
The users perform the following activities, which trigger insider risk policy alerts:
- User1 performs at least one data exfiltration activity that results in a high severity risk score.
- User2 performs at least three risky user activities within seven days, that each results in a high severity risk score.
- User3 performs at least two data exfiltration activities within seven days, that each results in a high severity risk score.
Which insider risk level is assigned to each user? To answer, drag the appropriate levels to the correct users. Each level 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.




**Answer:**



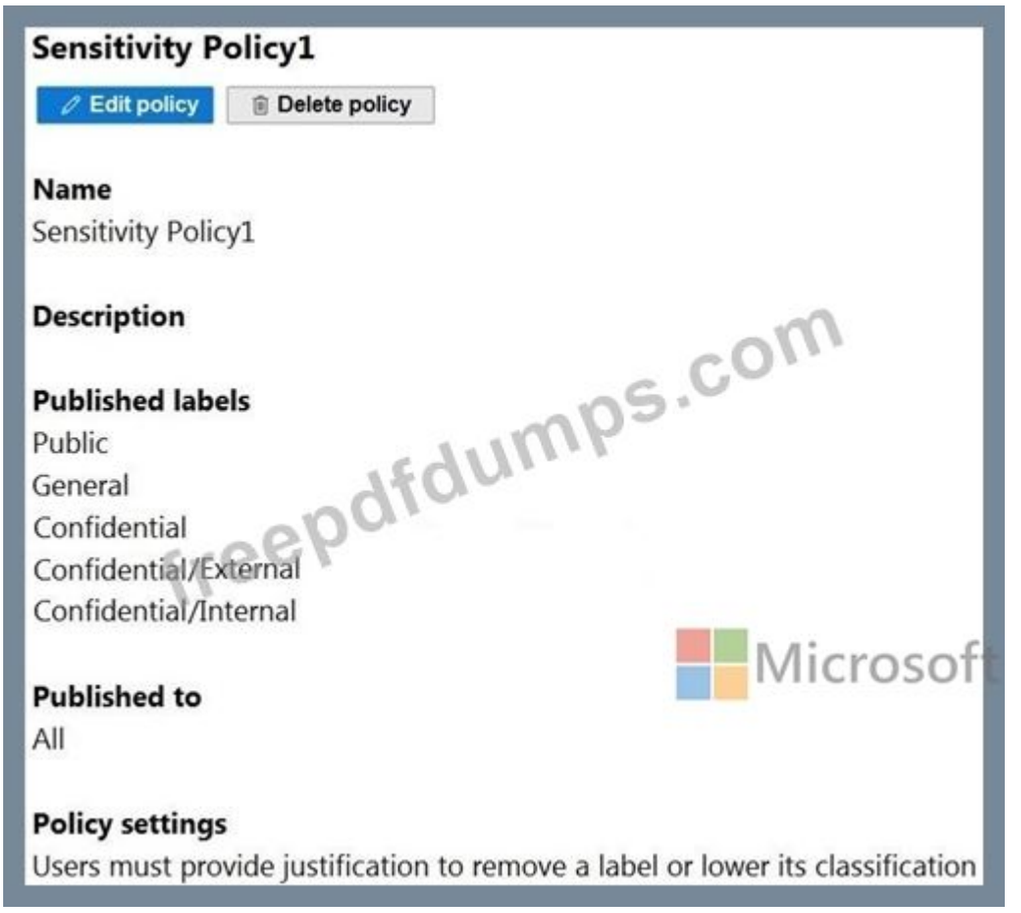

Explanation:

Box 1: Minor risk level
User1 performs at least one data exfiltration activity that results in a high severity risk score.
Minor:
This is the lowest risk level, assigned to users with low-severity alerts or those with at least one high-severity exfiltration activity.
Box 2: Elevated risk level
User2 performs at least three risky user activities within seven days, that each results in a high severity risk score.
Elevated:
This is the highest risk level, assigned to users with high-severity alerts, multiple high-severity insights, or confirmed high-severity alerts.
Box 3: Moderate risk level
User3 performs at least two data exfiltration activities within seven days, that each results in a high severity risk score.
Moderate:
This level indicates a medium risk, assigned to users with medium-severity alerts or those with at least two high-severity exfiltration activities.
Reference:
https://learn.microsoft.com/en-us/purview/insider-risk-management-adaptive-protection

**NEW QUESTION: 43**
Hotspot Question
You have a Microsoft 365 E5 tenant.
You have sensitivity labels as shown in the Sensitivity Labels exhibit. (Click the Sensitivity Labels tab.)



The Confidential/External sensitivity label is configured to encrypt files and emails when applied to content.
The sensitivity labels are published as shown in the Published exhibit. (Click the Published tab.)



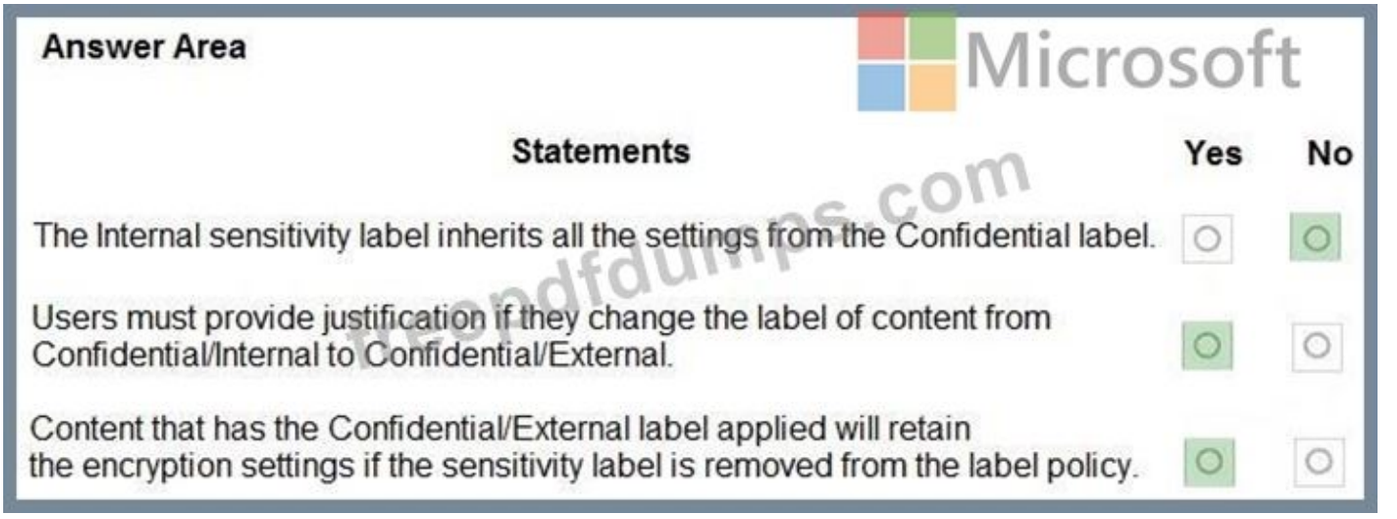

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| The Internal sensitivity label inherits all the settings from the Confidential label. | ○ | ○ |
| Users must provide justification if they change the label of content from Confidential/Internal to Confidential/External. | ○ | ○ |
| Content that has the Confidential/External label applied will retain the encryption settings if the sensitivity label is removed from the label policy. | ○ | ○ |

**Answer:**



**NEW QUESTION: 44**

Hotspot Question

You have the files shown in the following table.

| Name | Location | Date modified | Date created |
|---|---|---|---|
| File1 | Microsoft SharePoint Online site | June 01, 2022 | December 28, 2015 |
| File2 | Microsoft OneDrive account | February 02, 2021 | January 02, 2015 |
| File3 | Microsoft Exchange Online public folder | May 01, 2010 | May 01, 2010 |

You configure a retention policy as shown in the exhibit. (Click the Exhibit tab.)

**RetentionPolicy1**

**Status**
Enabled (Pending)

**Description**
RetentionPolicy1

**Applies to content in these locations**
SharePoint sites

**Settings**
**Retention period**
Keep content, and delete it if it's older than 7 years

**Preservation lock**
No

The start of the retention period is based on when items are created. The current date is January 01, 2025.

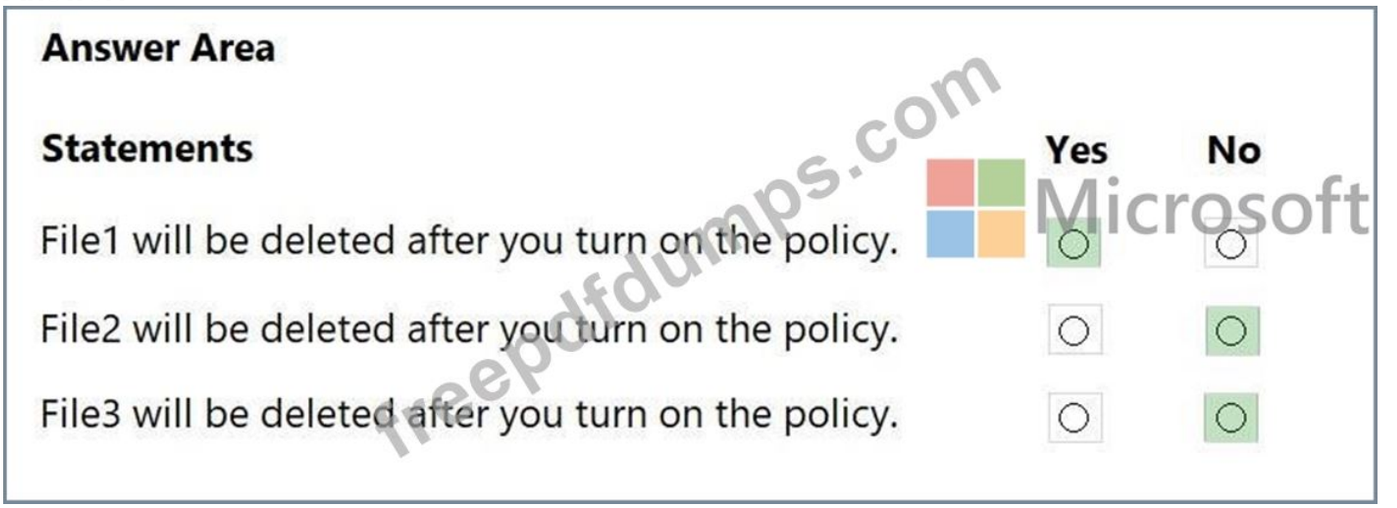
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| File1 will be deleted after you turn on the policy. | ○ | ○ |
| File2 will be deleted after you turn on the policy. | ○ | ○ |
| File3 will be deleted after you turn on the policy. | ○ | ○ |

**Answer:**






Explanation:

https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-sharepoint

**NEW QUESTION: 45**

Hotspot Question

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

| Name | Member of security group |
|---|---|
| User1 | Group1, Group2 |
| User2 | Group2 |
| User3 | Group1, Group3 |

You have the data loss prevention (DLP) policies shown in the following table.

| Name | Location | Included | Number of DLP rules | Rule severity |
|---|---|---|---|---|
| DLP1 | Devices | Group1 | 1 | High |
| DLP2 | Devices | Group2 | 1 | Medium |
| DLP3 | Devices | Group3 | 1 | Medium |

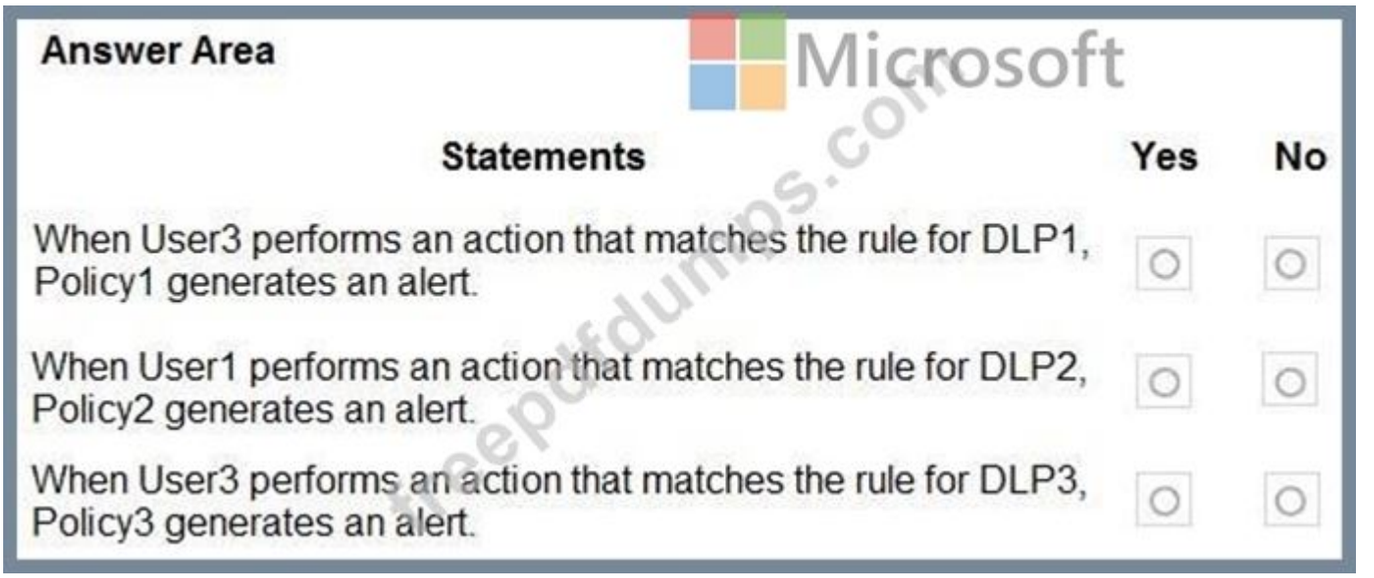
From Insider risk management, you configure a priority user group named PriGroup1 that contains User3 as a member.

You have the insider risk policies shown in the following table.

| Name | Policy template | Trigger | Group |
|---|---|---|---|
| Policy1 | Data leaks | DLP1 | Group1 |
| Policy2 | Data leaks | DLP2 | Group2 |
| Policy3 | Data leaks by priority users | DLP3 | PriGroup1 |

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:**


Explanation:

Reference:

https://learn.microsoft.com/en-us/purview/insider-risk-management-policy-templates

**NEW QUESTION: 46**

SIMULATION

Username and password

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and select the username below.

To enter your password, place your cursor in the Enter password box and select the password below.

Microsoft 365 Username:

admin@WWLx121586.onmicrosoft.com

Microsoft 365 Password: XXXXXXXXX

If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL "https://admin.microsoft.com", and press Enter.

The following information is for technical support purposes only:

Lab Instance: XXXXXXXXX

Task 7

You need to publish the Product Retired retention label only to Exchange mailboxes and SharePoint classic and communication sites.

**Answer:**

To publish a retention label to specific locations, create the label first, then create a static retention label policy in the Microsoft Purview portal, select "Let me choose specific locations," and choose your Exchange mailboxes and SharePoint sites as the policy's scope. For Exchange, you can select "All Exchange mailboxes" or choose specific mailboxes. For SharePoint, you must add classic and communication sites one by one in the policy's settings.

Publish the label with a static policy

Step 1: In the Microsoft Purview portal, go to Data lifecycle management > Policies > Label policies.

Step 2: Click Publish labels and then Choose labels to publish to select the Product Retired label.

Step 3: In the Policy scope section, choose Static and click Next.

Step 4: In the Choose where to publish labels screen, select Let me choose specific locations.

Step 5: For Exchange:

Select Exchange mailboxes. You can choose to apply it to All Exchange mailboxes or select specific ones from the list.

Step 6: For SharePoint:

Select SharePoint sites. You'll need to manually add the specific site collection addresses for both your classic and communication sites. A checkmark will appear next to the sites you add, and you can search for them in the next screen.

Step 7: Click Next, provide a name and description for the policy, and click Submit to create the policy.

Reference:

https://learn.microsoft.com/en-us/purview/create-apply-retention-labels



**NEW QUESTION: 47**

Hotspot Question

You have a Microsoft 365 E5 subscription that uses Microsoft Purview and just-in-time (JIT) protection. Fallback action in case of failure is set to Block users from completing actions.

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.

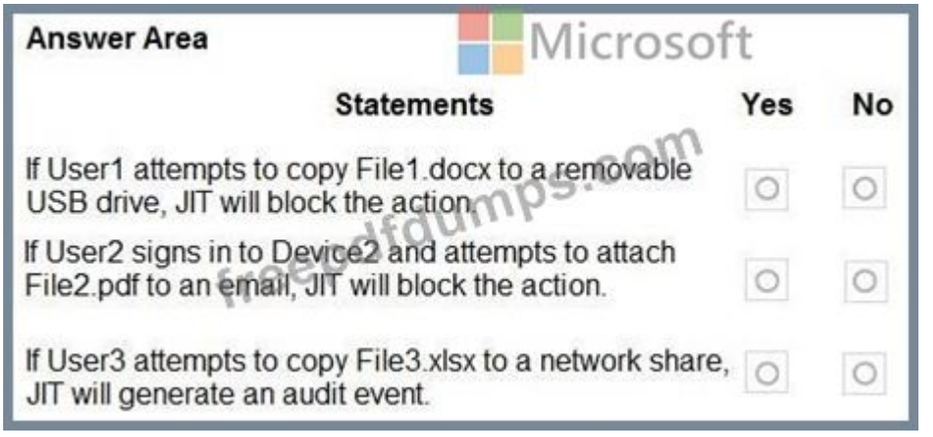
| Name | Microsoft Defender |
|---|---|
| Device1 | Onboarded |
| Device2 | Onboarded |
| Device3 | Not onboarded |

The devices contain the files shown in the following table.

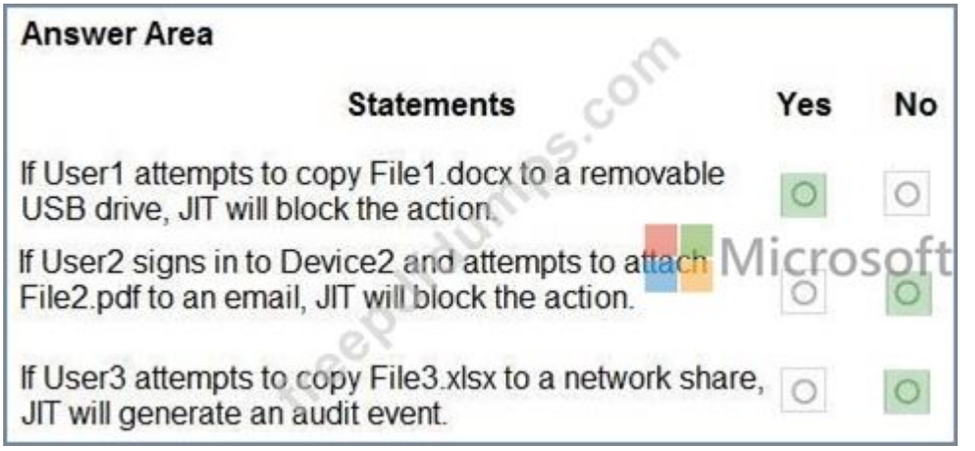
| Name | File classification evaluation status | Location |
|---|---|---|
| File1.docx | Not evaluated | Device1 |
| File2.pdf | Evaluated | Device2 |
| File3.xlsx | Not evaluated | Device3 |

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:**




Explanation:

Box 1: Yes

User1 is included in the JIT protection scope.

File1.docx has the file classification evaluation status of not evaluated, and is located on Device1.

Device1 is onboarded.

JIT will block the action.

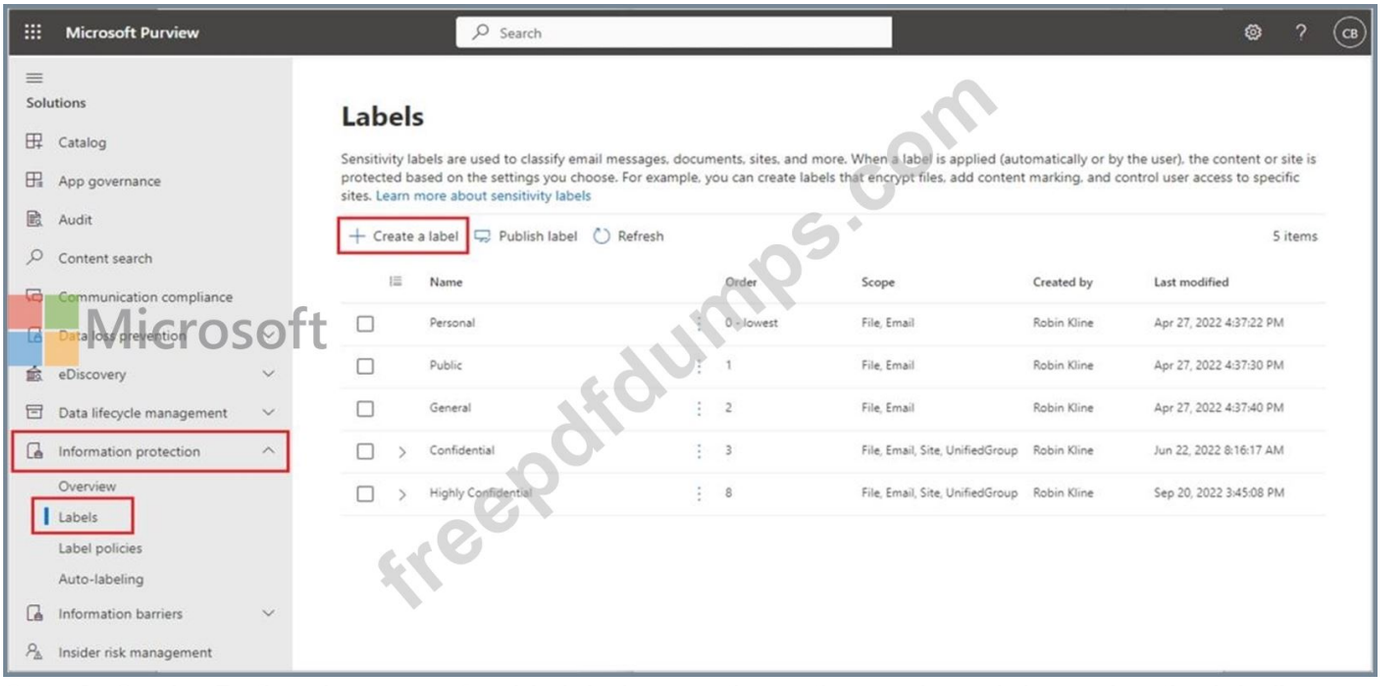
Note: In a Microsoft 365 environment with Purview and Just-in-Time (JIT) protection, a file with a

"not evaluated" classification status will be protected by JIT. When JIT protection is enabled, Endpoint DLP will block all egress activities on monitored files while waiting for policy evaluation to complete, including when the evaluation status is "not evaluated".
Box 2: No
User2 is not within the JIT protection scope.
Box 3: No
User3 is included in the JIT protection scope.
File3.docx has the file classification evaluation status of not evaluated, and is located on Device3.
Device3 is not onbarded.
Reference:
https://learn.microsoft.com/en-us/purview/endpoint-dlp-get-started-jit

**NEW QUESTION: 48**
You have a Microsoft 365 E5 subscription.
You create a sensitivity label named Label1 and publish Label1 to all users and groups.
You have the following files in a SharePoint site:
- File1.doc
- File2.docx
- File3.xlsx
- File4.txt
You need to identify which files can have Label1 applied.
Which files should you identify?
**A.** File2.docx only
**B.** File2.docx and File3.xlsx only
**C.** File1.doc, File2.docx, and File3.xlsx only
**D.** File1.doc, File2.doc, File3.xlsx, and File4.txt
**Answer: B (LEAVE A REPLY)**
n Microsoft 365, sensitivity labels can be applied to various file types including Word (.docx, .docm), Excel (.xlsx, .xlsm, .xlsb), PowerPoint (.pptx, .ppsx), and PDF documents. These labels can be applied to files stored in OneDrive and SharePoint, as well as attachments in Outlook emails.
Reference:
https://support.microsoft.com/en-gb/office/apply-sensitivity-labels-to-your-files-2f96e7cd-d5a4-403b-8bd7-4cc636bae0f9

**NEW QUESTION: 49**
SIMULATION
Username and password
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and select the username below.
To enter your password, place your cursor in the Enter password box and select the password

below.
Microsoft 365 Username:
admin@WWLx971455.onmicrosoft.com
Microsoft 365 Password: XXXXXXXXX
If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL "https://admin microsoft.com", and press Enter.
The following information is for technical support purposes only:
Lab Instance: XXXXXXXX.
Task 3
You plan to automatically apply a watermark to the documents of a project named Falcon.
You need to create a label that will add a watermark of "Project Falcon" in red, size-12 font diagonally across the documents.
**Answer:**
Create and configure sensitivity labels
Step 1: From the Microsoft Purview compliance portal, select Solutions > Information protection > Labels Step 2: On the Labels page, select + Create a label to start the new sensitivity label configuration:




Step 3: On the Define the scope for this label page, the options selected determine the label's scope for the settings that you can configure and where they'll be visible when they're published. In our case select: Items, Files, and select Word documents.


Note: If Items is selected, you can configure settings that apply to apps that support sensitivity labels, such as Office Word and Outlook. Optionally, you can extend these labels to include meetings from Teams and Outlook, and to protecting Teams meetings themselves by enforcing settings for Teams meetings and related chat.

Step 4: Follow the configuration prompts for the label settings. Use the help in the UI for individual settings.

Step 5: In the UI add a watermark of "Project Falcon" in red, size-12 font diagonally across the document.

Note: What sensitivity labels can do

After a sensitivity label is applied to an email, meeting invite, or document, any configured protection settings for that label are enforced on the content. You can configure a sensitivity label to:

* Mark the content when you use Office apps, by adding watermarks, headers, or footers to email, meeting invites, or documents that have the label applied. Watermarks can be applied to documents but not email or meeting invites. Example header and watermark:


Step 6: Finish the Wizard

Reference:

https://learn.microsoft.com/en-us/purview/create-sensitivity-labels

https://answers.microsoft.com/en-us/msteams/forum/all/how-to-automatically-apply-sensitivity-labels-to/2482d1b2-1fe6-4a80-af4a-2b93b9c670de

**NEW QUESTION: 50**

Hotspot Question

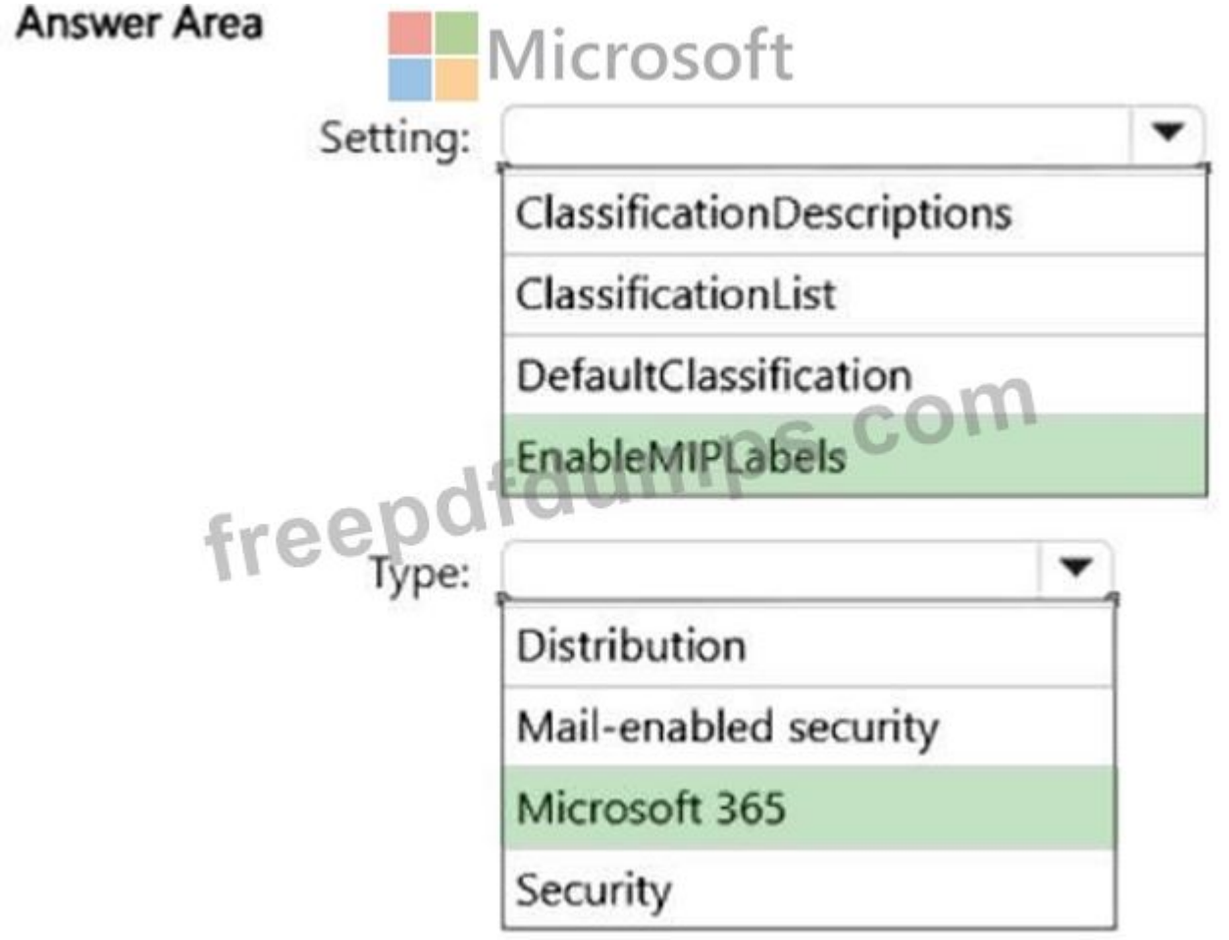
You have a Microsoft 365 E5 tenant that contains a published sensitivity label named Sensitivity1.

You plan to create a Microsoft Entra group named Group1 and assign Sensitivity1 to Group1.

How should you configure Group1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.


**Answer:**




Explanation:

Box 1: EnableMIPLabels

Enable sensitivity label support in PowerShell

To apply published labels to groups, you must first enable the feature. These steps enable the feature in Microsoft Entra ID. The Microsoft Graph PowerShell SDK comes in two modules,

Microsoft.Graph and Microsoft.Graph.Beta.
Box 2: Microsoft 365
Assign sensitivity labels to Microsoft 365 groups in Microsoft Entra ID Microsoft Entra ID supports applying sensitivity labels to Microsoft 365 groups when those labels are published in the Microsoft Purview portal or the Microsoft Purview compliance portal and the labels are configured for groups and sites.
Sensitivity labels can be applied to groups across apps and services such as Outlook, Microsoft Teams, and SharePoint.
Reference:
https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels

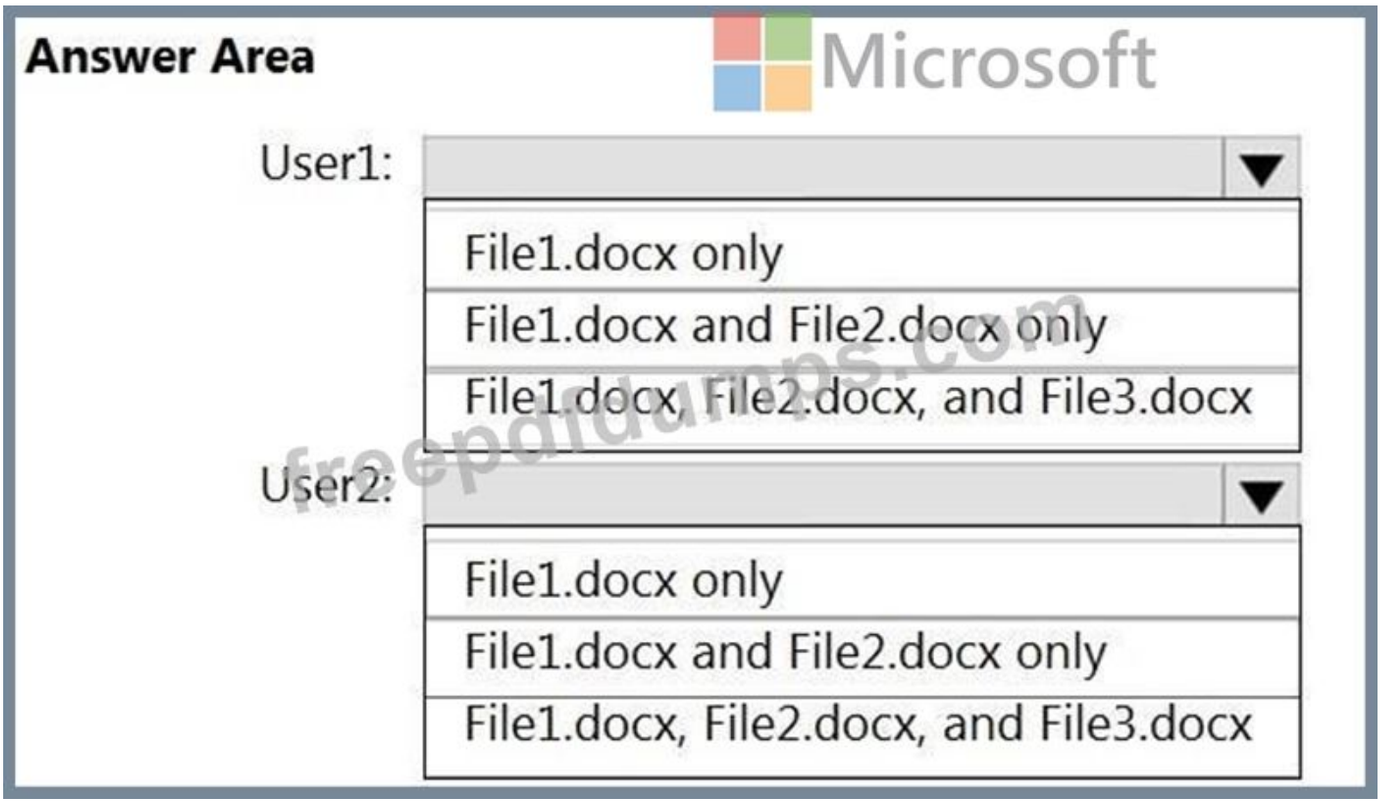
**NEW QUESTION: 51**
Hotspot Question
You have a Microsoft SharePoint Online site that contains the following files.

| Name | Modified by | Data loss prevention (DLP) status |
|---|---|---|
| File1.docx | Manager1 | None |
| File2.docx | Manager1 | Matched by DLP |
| File3.docx | Manager1 | Blocked by DLP |

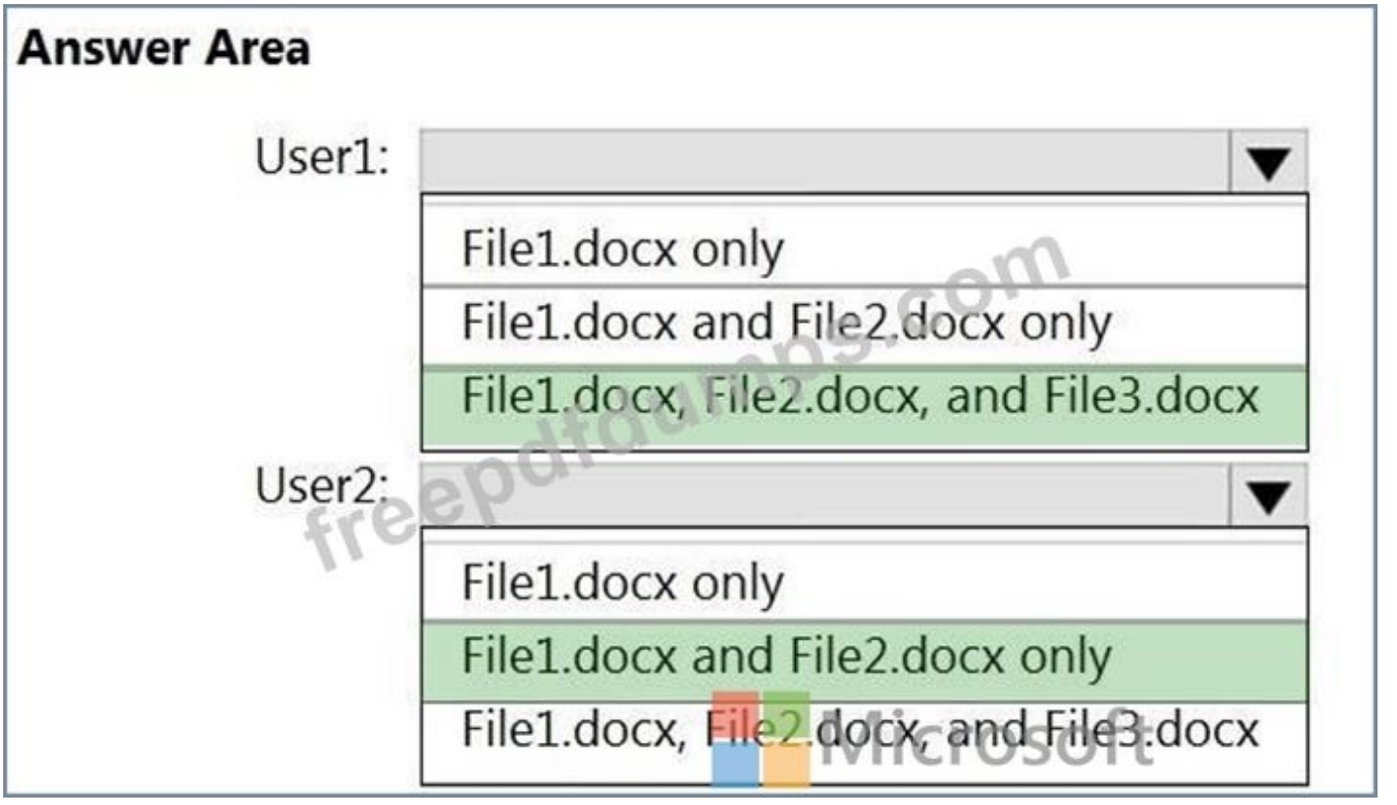
Users are assigned roles for the site as shown in the following table.

| 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.




**Answer:**




Explanation:

User1: User1 is a Site Owner, meaning they have full control over all files in the site. Even though File3.docx is blocked by DLP, a Site Owner can override or manage DLP restrictions and still access all files.

User2: User2 is a Site Member, meaning they have standard permissions to view and edit files unless blocked. File1.docx has no DLP action, so User2 can access it. File2.docx is matched by

DLP, but it is not blocked, so User2 can still access it. File3.docx is blocked by DLP, which means User2 cannot access it.

**NEW QUESTION: 52**

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 contains the files shown in the following table.

| Name | Author |
|---|---|
| File1.docx | User1 |
| File2.docx | User2 |
| File3.docx | USER1 |

In the Microsoft Purview portal, you create a content search named Content1 and configure the search conditions as shown in the following exhibit.




Which files will be returned by Content1?

**A.** File2.docx only

**B.** File3.docx only

**C.** File1.docx and File2.docx only

**D.** File1.docx and File3.docx only

**E.** Filet.docx, File2.docx, and File3.docx

**Answer: D (LEAVE A REPLY)**

Microsoft Purview, Keyword queries and search conditions for eDiscovery Values aren't case-

sensitive. Both User1 (File1.docx) and USER1 (File3.docx) will match the Search condition - Author:USER1.
Reference:
https://learn.microsoft.com/en-us/purview/ediscovery-keyword-queries-and-search-conditions

**NEW QUESTION: 53**
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: (SHOW ANSWER)**
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: 54**
Hotspot Question
You create a retention policy as shown in the following exhibit.

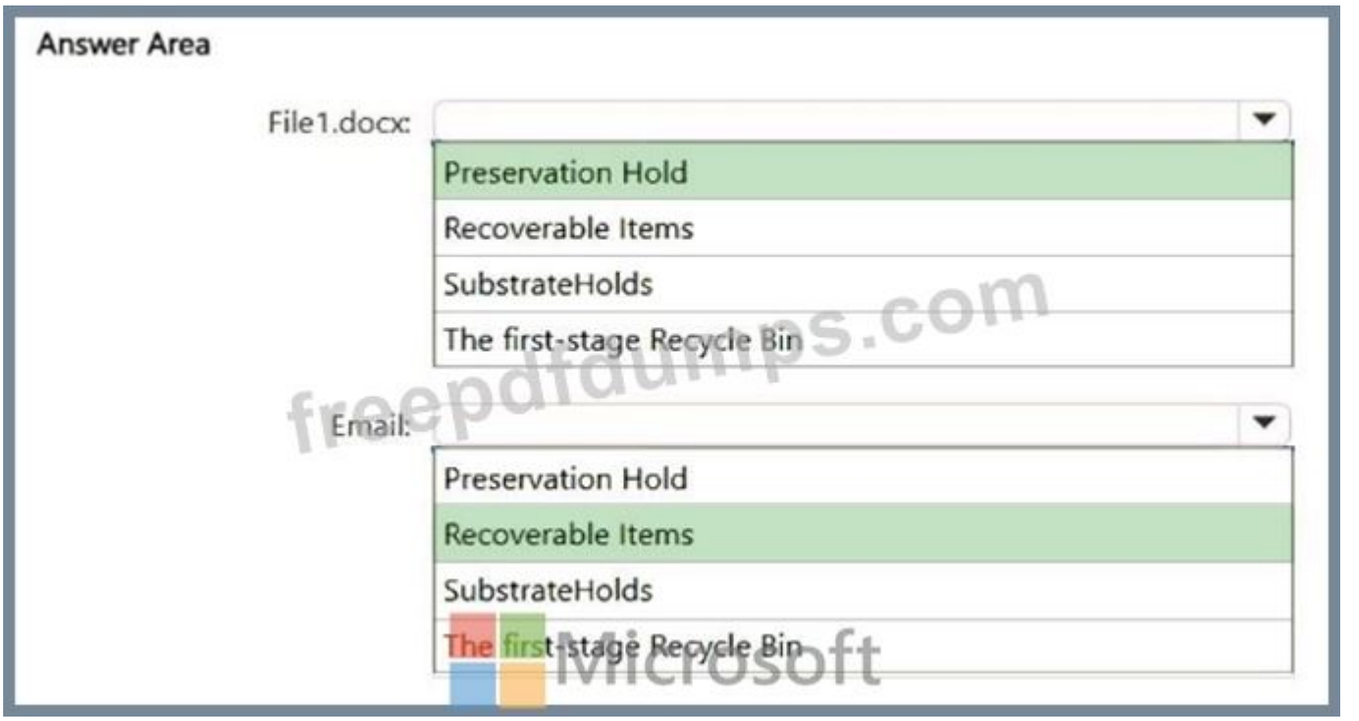

A user named User1 deletes a file named File1.docx from a Microsoft SharePoint Online site named Site1.

A user named User2 deletes an email and empties the Deleted Items folder in Microsoft Outlook.

Where is the content retained one year after deletion? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.


**Answer:**





Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

**NEW QUESTION: 55**

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: (SHOW ANSWER)**

Currently, you can create a document fingerprint only in Security & Compliance PowerShell, and Connect-IPPSSession is how you connect to it.

https://learn.microsoft.com/en-us/purview/document-fingerprinting#create-a-custom-sensitive-information-type-based-on-document-fingerprinting-using-powershell

https://learn.microsoft.com/en-us/powershell/module/exchange/connect-ippssession?view=exchange-ps

**NEW QUESTION: 56**

Your company has Microsoft 369 E5 subscription and plans to use Microsoft Purview Advanced Message Encryption.

Each product group at your company must show a distinct product logo in encrypted emails instead of the standard Microsoft 365 logo.
What should you do to create the branding templates?
**A.** Create an RMS template.
**B.** Create a Transport rule.
**C.** Run the New-OMEConfigurationcmdlet.
**D.** Run the Set-IRMConfigurationcmdlet.
**Answer: C (LEAVE A REPLY)**
https://docs.microsoft.com/en-us/microsoft-365/compliance/add-your-organization-brand-to-encrypted-messages

**NEW QUESTION: 57**
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 (LEAVE A REPLY)**
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: 58**
Hotspot Question
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

| Name | Role |
|---|---|
| User1 | Information Protection Administrator |
| User2 | Information Protection Analyst |
| User3 | Information Protection Investigator |

You need to delegate the following tasks:

- Create and manage data loss prevention (DLP) policies.
- Review classified content by using Content explorer.

The solution must use the principle of least privilege.

Which user should perform each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.


**Answer:**


Explanation:

Box 1: User1

Information Protection Admins

Create, edit, and delete DLP policies, sensitivity labels and their policies, and all classifier types.

Manage endpoint DLP settings and simulation mode for auto-labeling policies.

Note:
User 1 is Information Protection Administrator.
User2 is Information Protection Analyst.
User3 is Information Protection Investigator.
Box 2: User3
Information Protection Investigator
Access and manage DLP alerts, activity explorer, and content explorer. View-only access to DLP policies, sensitivity labels and their policies, and all classifier types.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions

**NEW QUESTION: 59**
You have a Microsoft 365 E5 subscription.
You plan to use insider risk management to collect and investigate forensic evidence.
You need to enable forensic evidence capturing.
What should you do first?
**A.** Configure the information protection scanner.
**B.** Create priority user groups.
**C.** Enable Adaptive Protection.
**D.** Claim capacity.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 60**
You have a Microsoft 365 E5 subscription.
You create a data loss prevention (DLP) policy and select Use Notifications to inform your users and help educate them on the proper use of sensitive info.
Which apps will show the policy tip?
**A.** Outlook on the web only
**B.** Outlook Win32 only
**C.** Outlook for iOS and Android only
**D.** Outlook on the web and Outlook Win32 only
**E.** Outlook Win32 and Outlook for iOS and Android only
**F.** Outlook on the web, Outlook Win32, and Outlook for iOS and Android
**Answer: D (LEAVE A REPLY)**
When you compose a new email in Outlook on the web and Outlook 2013 and later, you'll see a policy tip if you add content that matches a rule in a DLP policy, and that rule uses policy tips. The policy tip appears at the top of the message, above the recipients, while the message is being composed.
Note: Outlook Mobile (iOS, Android)/Outlook Mac: DLP policy tips are not supported on Outlook mobile Support Matrix for DLP policy tips across Microsoft apps.
Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-tips-reference
https://docs.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips

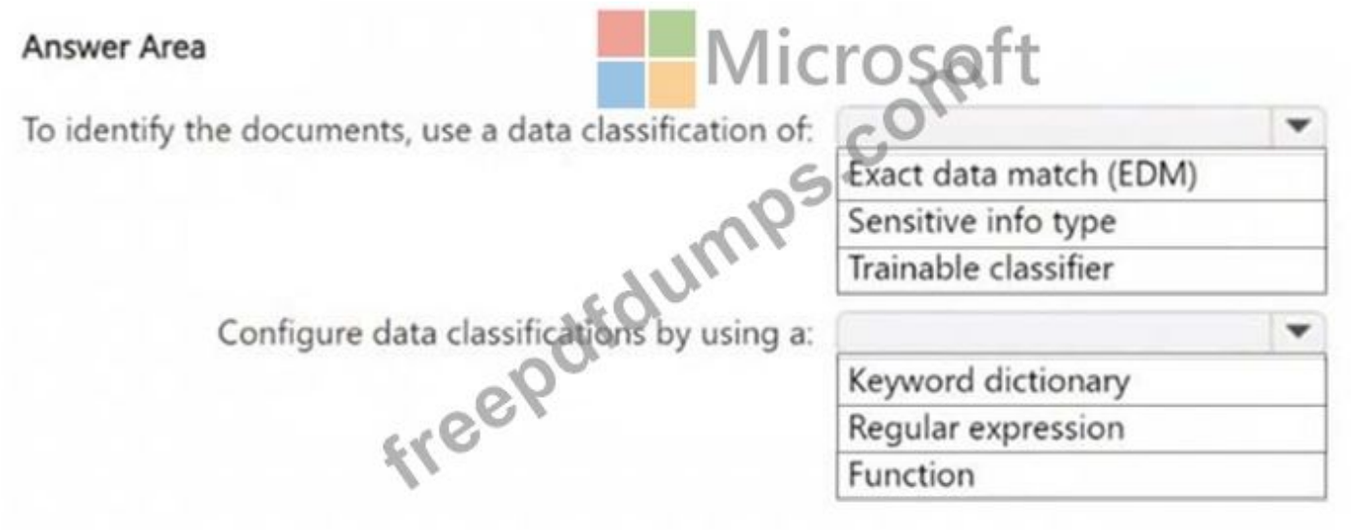
**NEW QUESTION: 61**
You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.
On January 1, you create the sensitivity label shown in the following table.

| Setting | Value |
|---|---|
| Name | Label1 |
| Assign permissions now or let users decide? | Assign permissions now |
| User access to content expires | After 21 days |
| Assign permissions to specific users and groups | Co-Author: User1 and User2 |

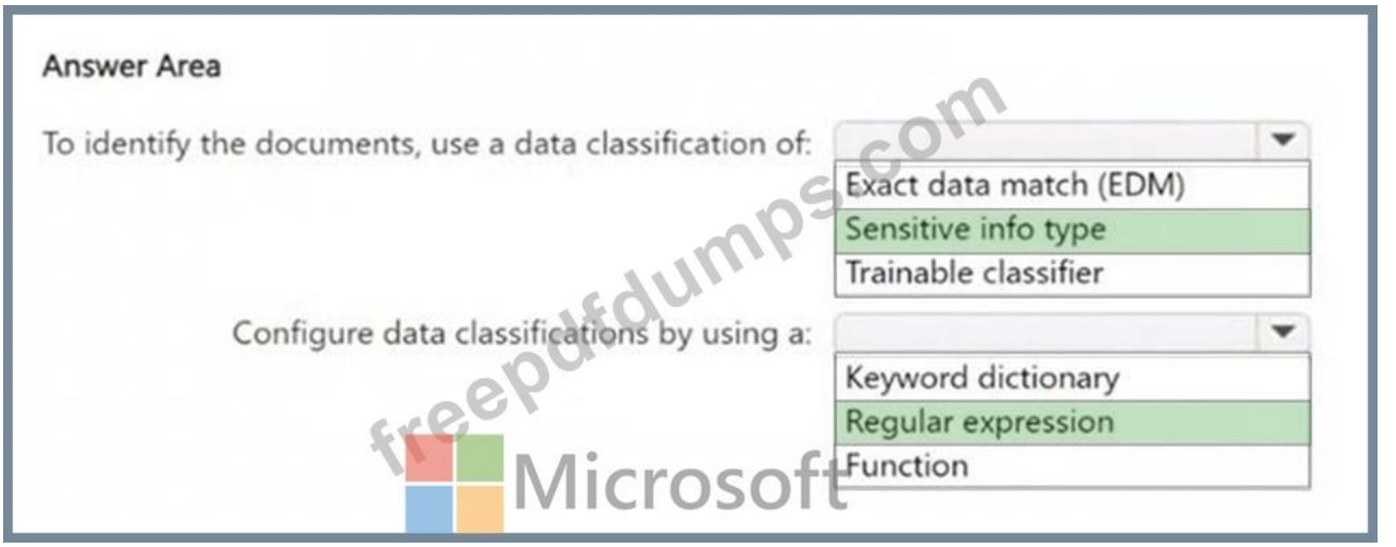
On January 2, you publish Label1 to User.
On January 3, User1 creates a Microsoft Word document named Doc1 and applies Label1 to the document.
On January 4, User2 edits Doc1.
On January 15, you increase the content expiry period for Label1 to 28 days.
When will access to Doc1 expire for User2?
**A.** January 24
**B.** January 25
**C.** January 31
**D.** January 23
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 62**
Hotspot Question
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:**




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: 63**

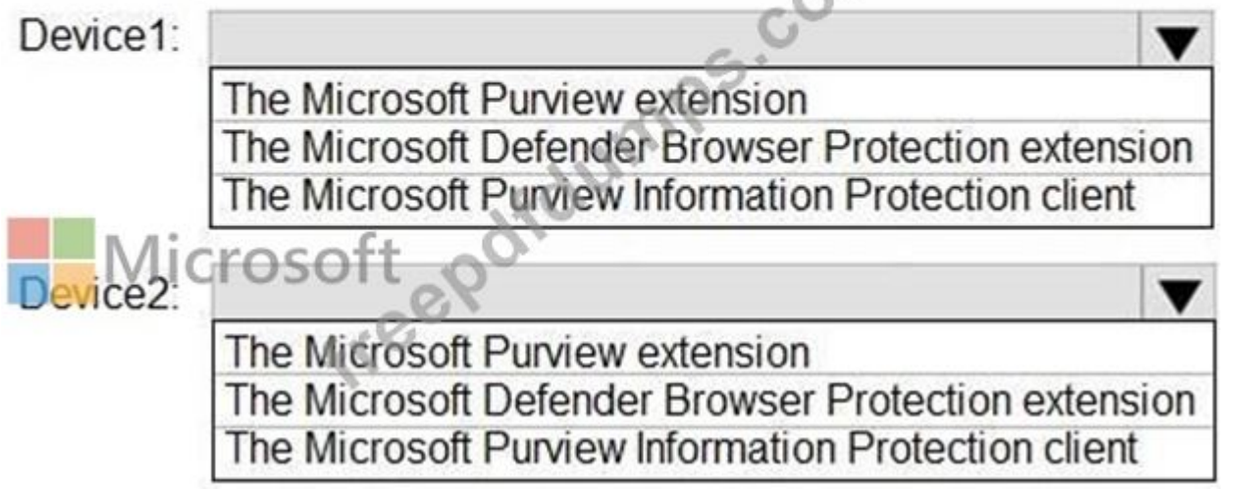
Hotspot Question

You have a Microsoft 365 E5 subscription that contains two Windows devices named Device1 and Device2. Device1 has the default browser set to Microsoft Edge. Device2 has the default browser set to Google Chrome.

You need to ensure that Microsoft Purview insider risk management can collect signals when a

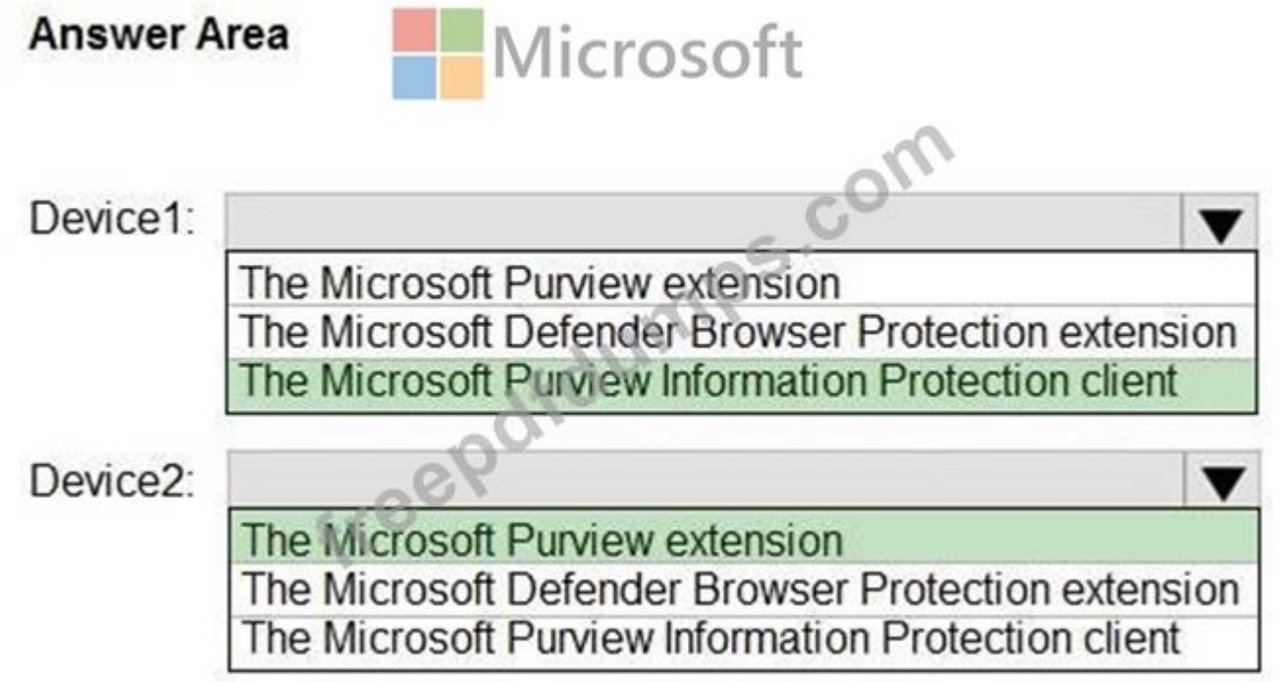
user copies files to a USB device by using their default browser.
What should you deploy to each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**




**Answer:**

**Answer Area**




Explanation:
Box 1: The Microsoft Purview Information protection client
Device1 has the default browser set to Microsoft Edge.
The Microsoft Purview Information Protection client, now integrated with Microsoft Edge, enables organizations to apply data security policies and protect sensitive information within the browser. Specifically, Microsoft Purview Information Protection features like sensitivity labels and data loss prevention (DLP) can be leveraged in Edge for Business to control access and usage of sensitive documents and data.

Box 2: Microsoft Purview extension
Device2 has the default browser set to Google Chrome.
After the installation of the Microsoft Purview extension for Google Chrome, on Windows devices, organizations get the ability to also monitor attempts to access or upload sensitive items to a Cloud service when using the Google Chrome browser, and to actually enforce protective actions via data loss prevention.
The Microsoft Purview extension is used with Google Chrome, but it's not required for Microsoft Edge because Edge has built-in Endpoint DLP capabilities. The extension enhances data loss prevention for non-native applications, particularly for Chrome and other browsers where DLP needs to be explicitly extended.
Reference:
https://learn.microsoft.com/en-us/purview/dlp-chrome-get-started

**NEW QUESTION: 64**
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 (IBs)
**D.** sensitivity labels
**Answer: D (LEAVE A REPLY)**
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: 65**
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 (LEAVE A REPLY)**
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.

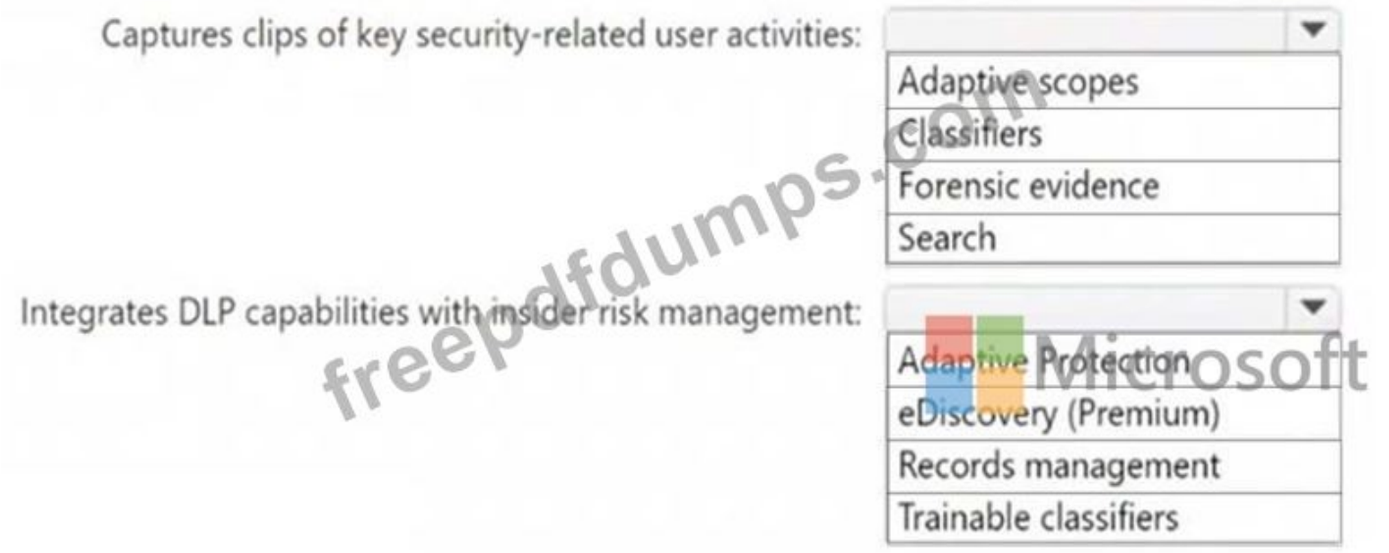
**NEW QUESTION: 66**
You have a Microsoft 365 tenant that uses Microsoft Purview Message Encryption.
You need to ensure that any emails containing attachments and sent to user1@contoso.com are encrypted automatically by using Microsoft Purview Message Encryption.
What should you do?
**A.** From the Exchange admin center, create a mail flow rule.
**B.** From the Exchange admin center, create a new sharing policy.
**C.** From the Microsoft Defender portal, create a Safe Attachments policy.
**D.** From the Microsoft Purview portal, configure an auto-apply retention label policy.
**Answer: (SHOW ANSWER)**
Defining rules for Microsoft Purview Message Encryption
One way to enable Microsoft Purview Message Encryption is for Exchange Online and Exchange Online Protection administrators to define mail flow rules. These rules determine under what conditions email messages should be encrypted. When an encryption action is set for a rule, any messages that match the rule conditions are encrypted before they're sent.
Mail flow rules are flexible, letting you combine conditions so you can meet specific security requirements in a single rule. For example, you can create a rule to encrypt all messages that contain specified keywords and are addressed to external recipients. Microsoft Purview Message Encryption also encrypts replies from recipients of encrypted email.
Reference:
https://learn.microsoft.com/en-us/purview/ome

**NEW QUESTION: 67**
You have a Microsoft SharePoint Online site named Site1 that contains a document library. The library contains more than 1,000 documents. Some of the documents are job applicant resumes. All the documents are in the English language.

You plan to apply a sensitivity label automatically to any document identified as a resume. Only documents that contain work experience, education, and accomplishments must be labeled automatically.
You need to identify and categorize the resumes. The solution must minimize administrative effort.
What should you include in the solution?
**A.** a trainable classifier
**B.** a keyword dictionary
**C.** a function
**D.** an exact data match (EDM) classifier
**Answer: A (LEAVE A REPLY)**
Since you need to automatically apply a sensitivity label to resumes based on their content and structure (work experience, education, accomplishments), a trainable classifier is the best choice. Trainable classifiers use machine learning to identify unstructured data, such as resumes, contracts, or legal documents. Instead of relying on predefined patterns (like keywords or regular expressions), a trainable classifier learns from sample documents and can accurately identify resumes even if they are formatted differently.
Final Approach:
- Train a trainable classifier using sample resumes.
- Deploy the classifier in Microsoft Purview.
- Configure a sensitivity label to be automatically applied when a document matches the classifier.

**NEW QUESTION: 68**
Hotspot Question
You have a Microsoft 365 E5 subscription.
You need to implement a compliance solution that meets the following requirements:
- Captures clips of key security-related user activities, such as the exfiltration of sensitive company data.
- Integrates data loss prevention (DLP) capabilities with insider risk management.
What should you use for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

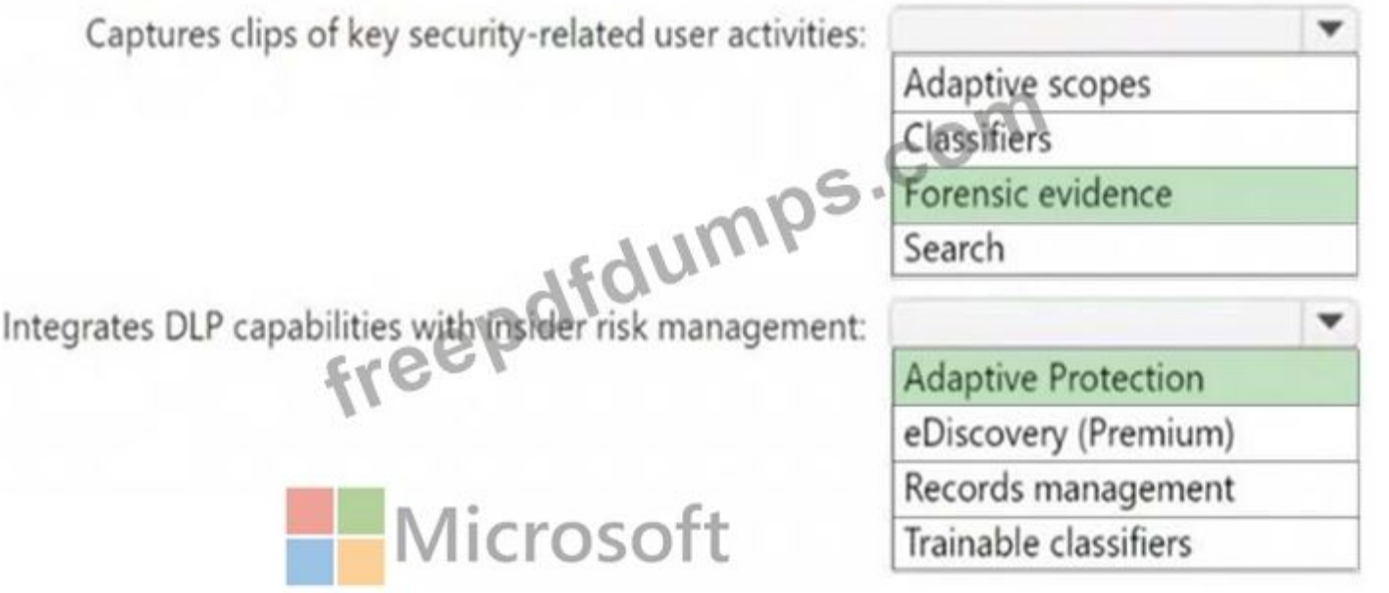
Answer Area






**Answer:**

Answer Area






Explanation:

Box 1: Forensic evidence in Microsoft Purview Insider Risk Management allows organizations to capture screen recordings of security-related user activities, such as attempted exfiltration of sensitive data. This feature provides context around risky behavior, helping investigators analyze incidents more effectively.

Box 2: Adaptive Protection uses Microsoft Purview Insider Risk Management and DLP together to apply protection dynamically based on detected user risks. It enhances DLP policies by automatically adjusting enforcement based on insider risk signals, ensuring that high-risk users receive stricter data controls while minimizing friction for low-risk users.

**NEW QUESTION: 69**

Hotspot Question

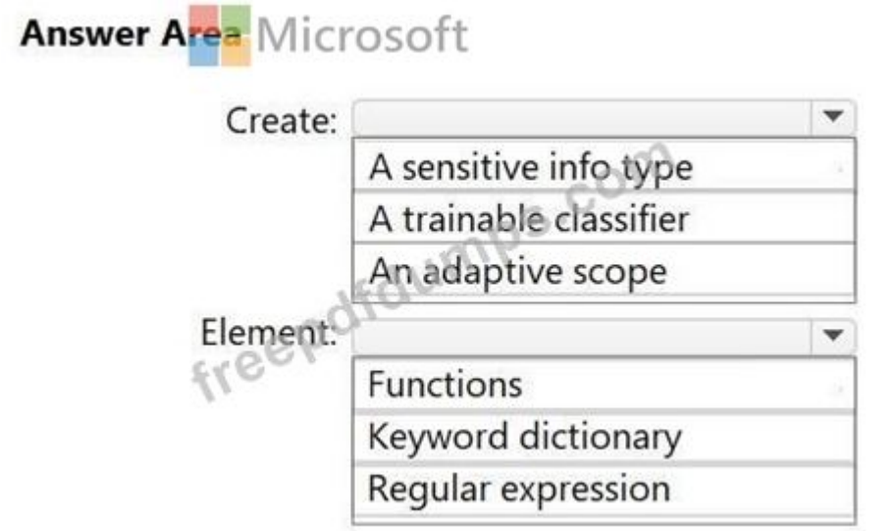
You have a Microsoft 365 E5 subscription.

You have a file named Customer.csv that contains a list of 1,000 customer names.

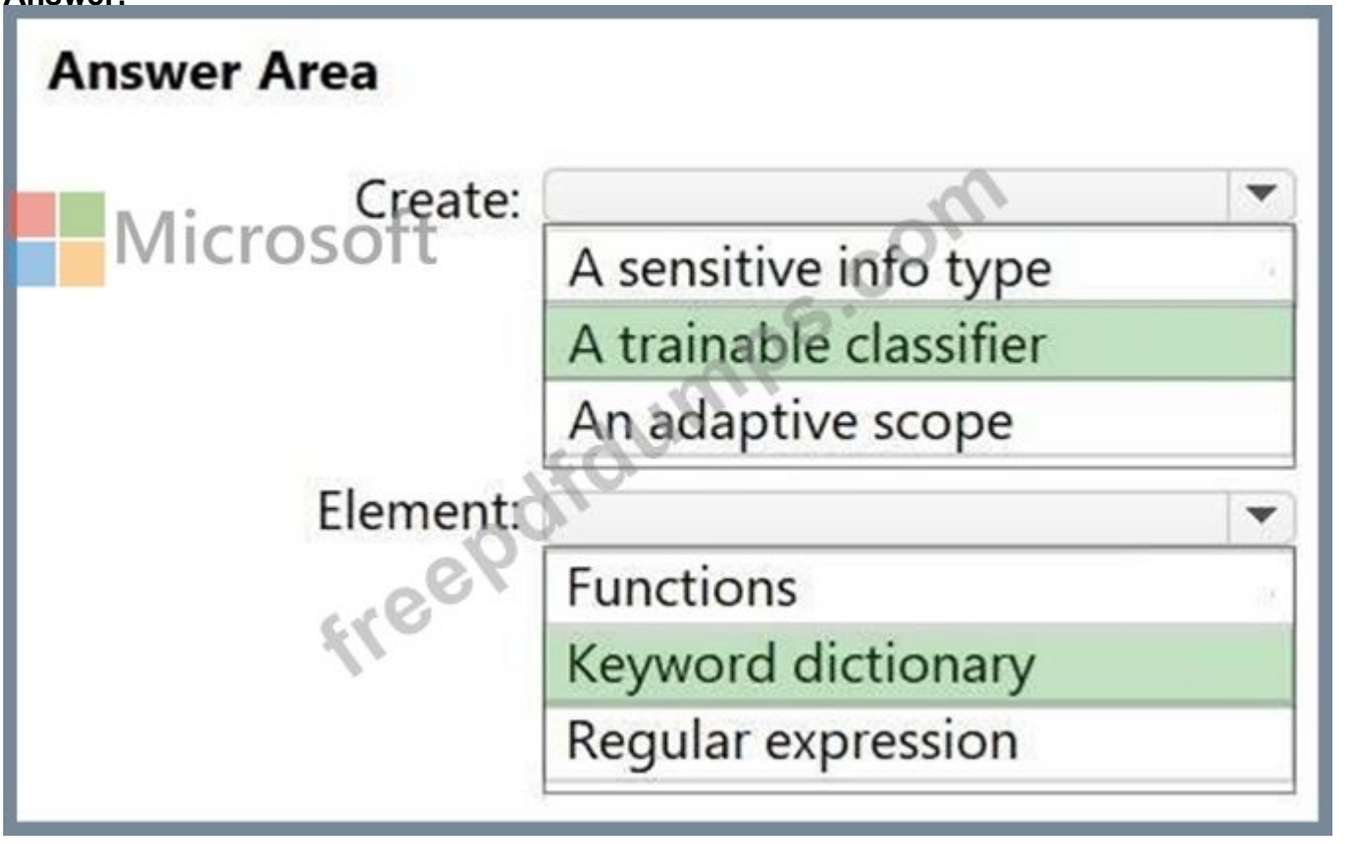
You plan to use Customer.csv to classify documents stored in a Microsoft SharePoint Online library.

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.




**Answer:**




Explanation:

To classify documents in SharePoint Online using Customer.csv, you need to create a trainable classifier. A trainable classifier is best suited for identifying patterns in unstructured data (e.g.,

customer names in documents). A sensitive info type is more suitable for structured data (e.g., credit card numbers, SSNs). An adaptive scope is used to apply policies dynamically based on attributes, not for classifying content.
Since Customer.csv contains a list of names, the best element to use is a keyword dictionary. A keyword dictionary allows you to upload a list of predefined terms (such as customer names) to classify documents based on their presence. Regular expressions are used for pattern-based detection (e.g., credit card numbers, serial numbers), which is not needed here. Functions are used for predefined sensitive data detection (e.g., checksum validation for credit card numbers), which does not apply in this case.

**NEW QUESTION: 70**
Hotspot Question
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

| Name | Member of |
|---|---|
| User1 | Members group of Site1 |
| User2 | Owners group to Site1 |
| Admin1 | SharePoint Administrator role |

You have a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.


You apply DLP1 to Site1
User1 uploads a file named File1 to Site1. File does NOT match any of the DLP1 rules. User2 updates File1 to contain data that matches the DLP1 rules.
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:**


Explanation:

Box 1: No

Note: Actions

Any item that makes it through the conditions filter will have any actions that are defined in the rule applied to it. You'll have to configure the required options to support the action. For example, if you select Exchange with the Restrict access or encrypt the content in Microsoft 365 locations action you need to choose from these options:

Box 2: Yes

User2 is the last modifier of the file.

Box 3: Yes

Users assigned the SharePoint Administrator role have access to the SharePoint admin center and can create and manage sites (previously called "site collections"), designate site admins, manage sharing settings, and more.

Reference:

https://learn.microsoft.com/en-us/sharepoint/sharepoint-admin-role

**NEW QUESTION: 71**

You have a Microsoft 365 E5 subscription that has a Microsoft Purview exact data match (EDM) classifier named EDM1.

You plan to create the Microsoft Purview policies shown in the following table.

| Name | Type |
|---|---|
| DLP1 | Data loss prevention (DLP) |
| Insider1 | Insider risk management |
| Retention1 | Retention |

Which policies can use EDM1?

**A.** DLP1 only

**B.** Retention1 only

**C.** DLP1 and Insider1 only

**D.** Insider1 and Retention1 only

**E.** DLP1, Insider1, and Retention1

**Answer: (SHOW ANSWER)**

EDM SITs can be used in:

Auto-labeling (service and client side) [See note below]

*-> Microsoft Purview Data Loss Prevention [DLP1]

*-> Microsoft Purview Insider Risk Management policies [Insider1]

Microsoft Purview eDiscovery

Microsoft Purview Insider Risk Management

Microsoft Defender for Cloud Apps

Reference:

https://learn.microsoft.com/en-us/purview/sit-get-started-exact-data-match-based-sits-overview

https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically

**NEW QUESTION: 72**

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 (LEAVE A REPLY)**

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: 73**

You have a Microsoft 365 subscription that contains 100 users and a Microsoft 365 group named Group1.

All users have Windows 11 devices and use Microsoft SharePoint Online and Exchange Online.

A sensitivity label named Label1 is published as the default label for Group1.

You add two sublabels named Sublabel1 and Sublabel2 to Label1.

You need to ensure that the settings in Sublabel1 are applied by default to Group1.

What should you do?

**A.** Modify the policy of Label1.

**B.** Duplicate all the settings from Sublabel1 to Label1.

**C.** Delete the policy of Label1 and publish Sublabel1.

**D.** Change the order of Sublabel1.

**Answer: C (LEAVE A REPLY)**

To ensure a sublabel is applied by default to a Microsoft 365 group when the parent label is the default, you must publish the desired sublabel and set it as the default for the group in the Microsoft Purview compliance portal, rather than trying to manipulate the parent label's policy. The original parent label should not be set as the default for the group anymore, as sublabels override the parent's default status.

Reference:

https://learn.microsoft.com/en-us/purview/sensitivity-labels

**NEW QUESTION: 74**

You have a Microsoft 365 E5 tenant and the Windows Client devices shown in the following table.

| Name | Joined to Microsoft Entra | Configuration |
|---|---|---|
| Device1 | Yes | Onboarded to Microsoft Purview |
| Device2 | Yes | Onboarded to Microsoft Defender for Endpoint |
| Device3 | Yes | Enrolled in Microsoft Intune |
| Device4 | No | Enrolled in Microsoft Intune |

To which devices can you apply Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings?

**A.** Device1 only

**B.** Device1 and Device2 only

**C.** Device1 and Device3 only

**D.** Device1, Device3, and Device4 only

**E.** Device1, Device2, Device3, and Device4

**Answer: (SHOW ANSWER)**

https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started

**NEW QUESTION: 75**

Hotspot Question

You have a Microsoft 365 E5 subscription.

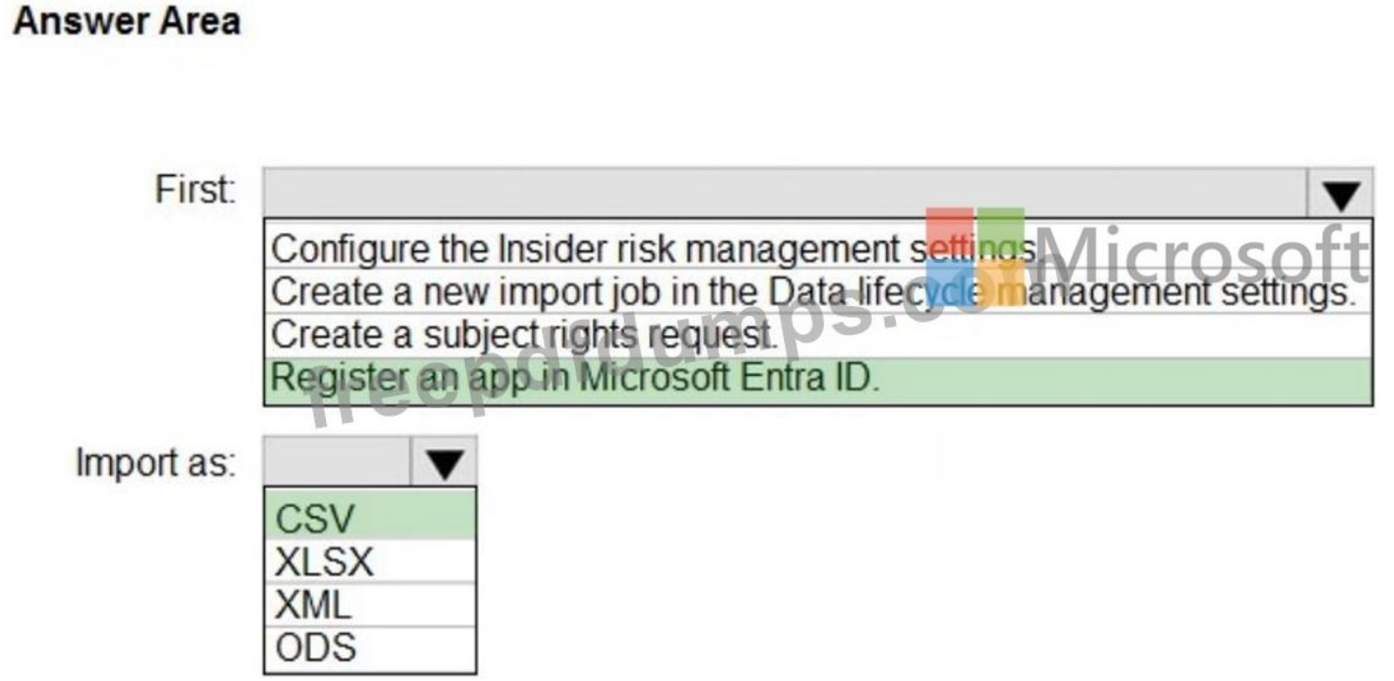
You plan to use the Microsoft Purview portal to map human resources (HR) data for use with insider risk management policies.

You need to add a data connector to import the HR data.

What should you do first, and in which format should you import the data? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.


**Answer:**




Explanation:

Step 1: Prepare a CSV file with your HR data

Step 2: Create an app in Microsoft Entra ID

Step 3: Create the HR connector

Step 4: Run the sample script to upload your HR data

Step 5: Monitor the HR connector

(Optional) Step 6: Schedule the script to run automatically

(Optional) Step 7: Upload data by using Power Automate templates

Reference:

https://learn.microsoft.com/en-us/purview/import-hr-data

**NEW QUESTION: 76**

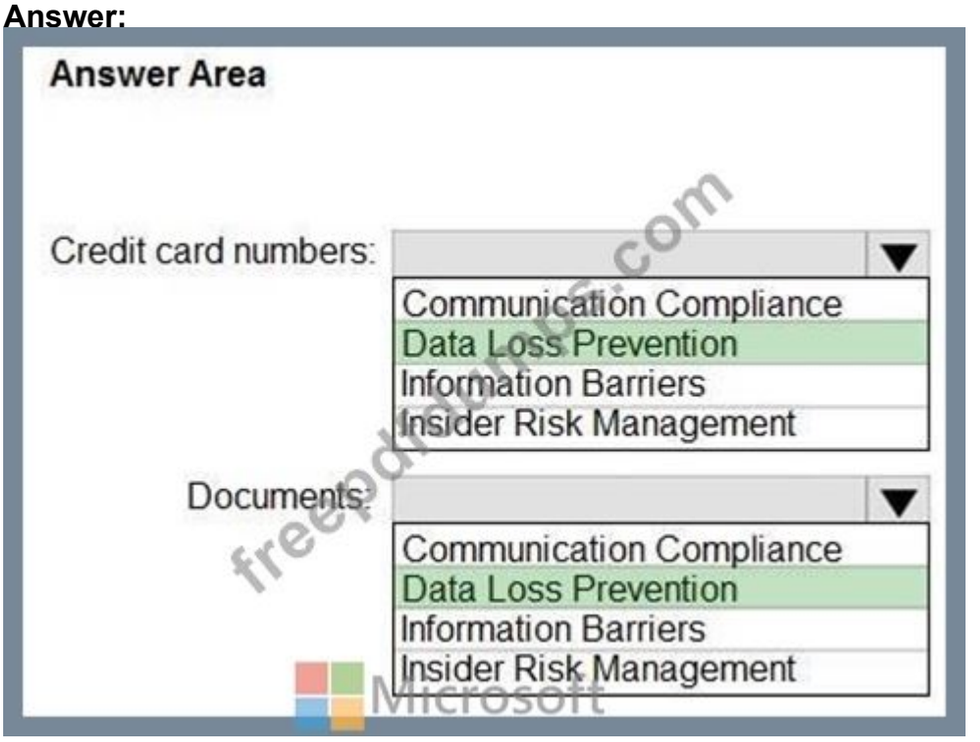
Note: This question is part of a series of questions that present the same scenario. Each question

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 (LEAVE A REPLY)**
Using the "text patterns" condition in the Exchange transport rule would not work.
The condition to be used in the Exchange transport rule would be "The message contains any of this sensitive information..." and select the Sensitive Info Type "Azure Account Storage Key".
https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mail-flow-rules/conditions-and-exceptions?view=exchserver-2019



**NEW QUESTION: 77**
Hotspot Question
You have a Microsoft 365 E5 subscription.
You need to ensure that users are prevented from uploading sensitive data to ChatGPT and Google Gemini. The solution must meet the following requirements:
- Prevent credit card numbers from being pasted into ChatGPT and Gemini.
- Prevent documents that contain classified data from being uploaded to ChatGPT and Gemini.
Which Microsoft Purview solution should you use for each requirement? To answer, select the appropriate options in the answer NOTE: Each correct selection is worth one point.


**Answer:**




Explanation:

Box 1: Data Loss Prevention

Prevent credit card numbers from being pasted into ChatGPT and Gemini.

Microsoft Purview data security and compliance protections for generative AI apps The Data Loss Prevention Policy (DLP) serves as a safeguard against sensitive data being copied, pasted, or uploaded into external AI platforms.

Windows computers that are onboarded to Microsoft Purview can be configured for Endpoint data loss prevention (DLP) policies that warn or block users from sharing sensitive information with third-party generative AI sites that are accessed via a browser. For example, a user is prevented from pasting credit card numbers into ChatGPT, or they see a warning that they can override.

Box 2: Data Loss Prevention

Prevent documents that contain classified data from being uploaded to ChatGPT and Gemini.

Data Loss Prevention (DLP) Policy: Preventing Sensitive Data from Being Shared The Data Loss Prevention Policy (DLP) serves as a safeguard against sensitive data being copied, pasted, or uploaded into external AI platforms. This policy ensures that any confidential, personal, or proprietary information is blocked from being transferred to unauthorized AI websites like

ChatGPT or Google Gemini.
Reference:
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview

**NEW QUESTION: 78**
You have a Microsoft 365 E5 subscription that contains four users named User1, User2, User3, and User4 and a file named File1.docx. File1 has a sensitivity label applied. The label is configured as shown in the following table.

| User | Permission |
|---|---|
| User1 | Owner |
| User2 | Editor |
| User3 | Restricted Editor |
| User4 | Viewer |

Which users can summarize File1 by using Microsoft 365 Copilot?
**A.** User1 only
**B.** User1 and User2 only
**C.** User1, User2, and User3 only
**D.** User1, User2, User3, and User4
**Answer: B (LEAVE A REPLY)**
To summarize a file with a sensitivity label using Microsoft 365 Copilot, a user needs the EXTRACT and VIEW usage rights, especially if the sensitivity label applies encryption, according to Microsoft Learn. These rights are necessary for Copilot to access and process the content of the file, according to Microsoft Learn. If the user doesn't have these rights, Copilot won't be able to summarize the file.
* User1 - Yes
An owner has EXTRACT and VIEW usage rights.
* User2 - Yes
A user with Editor permissions can summarize a file with a sensitivity label using Microsoft 365 Copilot, but only if the sensitivity label grants the necessary usage rights, specifically the "EXTRACT" right, to the user. If the sensitivity label restricts the "EXTRACT" right, Copilot will not be able to summarize the file.
* User3 - No
A Restricted Editor in Microsoft 365 Copilot cannot summarize a file with a sensitivity label that restricts access. Microsoft 365 Copilot respects sensitivity labels and will not process files if the user doesn't have the necessary permissions (like EXTRACT and VIEW). If a user only has VIEW rights, Copilot will provide a reference link to the file instead of summarizing it.
* User4 - No
Reference:
https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture-data-protection-auditing

**NEW QUESTION: 79**

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You need to ensure that you receive an alert when a user uploads a document to a third-party cloud storage service.

What should you use?

**A.** an insider risk policy

**B.** a file policy

**C.** a sensitivity label

**D.** an activity policy

**Answer: (SHOW ANSWER)**

Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies

https://learn.microsoft.com/en-us/defender-cloud-apps/policies-information-protection

**NEW QUESTION: 80**

Hotspot Question

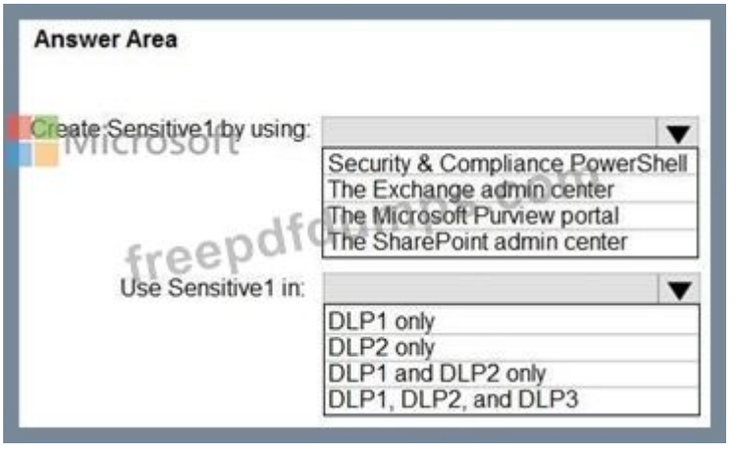
You have a Microsoft 365 E5 subscription that contains the data loss prevention (DLP) policies shown in the following table.

| Name | Applied to |
|---|---|
| DLP1 | Microsoft Exchange Online email |
| DLP2 | Microsoft SharePoint Online sites |
| DLP3 | Microsoft Teams chat and channel messages |

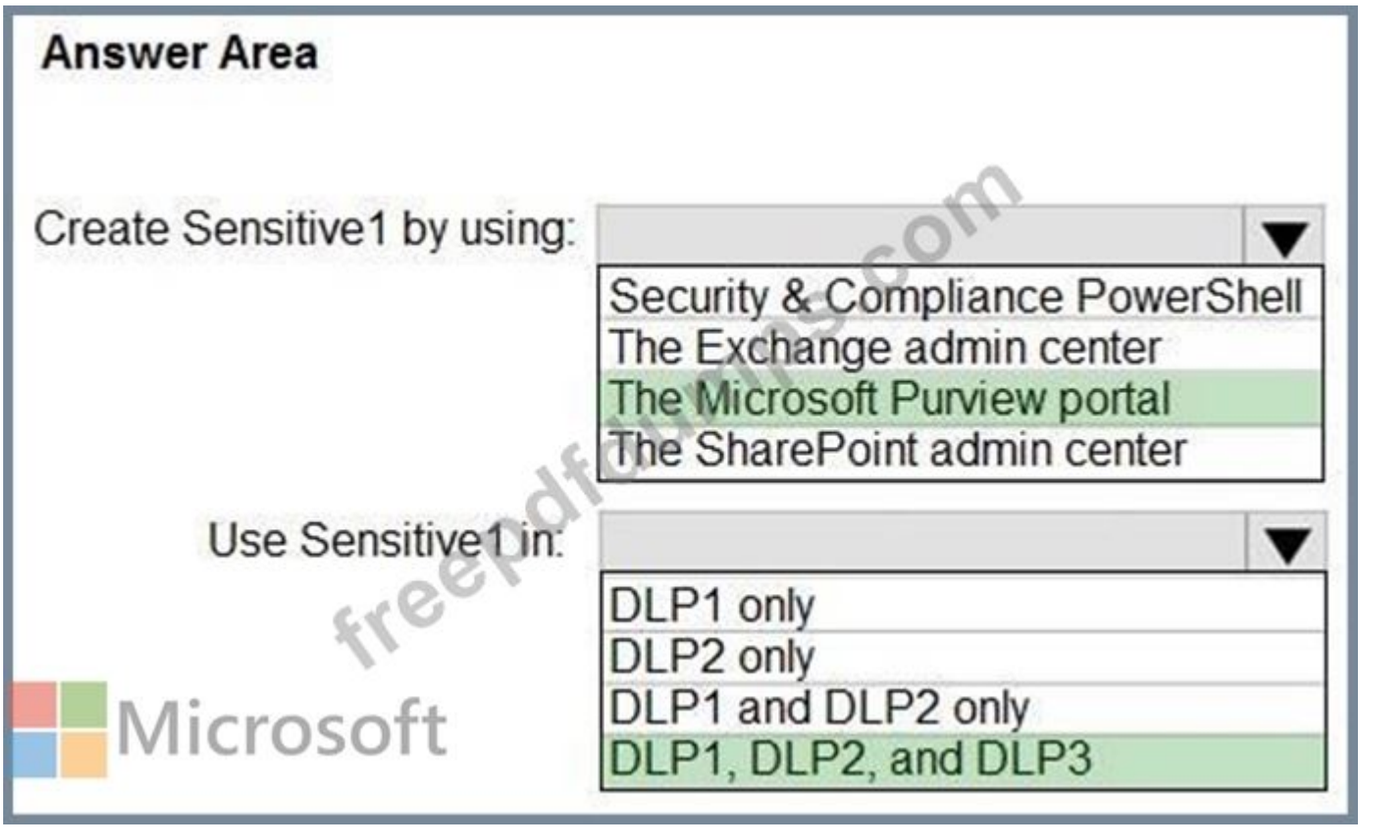
You have a custom employee information form named Template1.docx.

You plan to create a sensitive info type named Sensitive1 that will use the document fingerprint from Template1.docx.

What should you use to create Sensitive1, and in which DLP policies can you use Sensitive1? To answer, select the appropriate options in the answer area.




**Answer:**




Explanation:

Box 1: Microsoft Purview portal

Box 2: DLP1, DLP2, and DLP3

DLP can use document fingerprinting as a detection method in Exchange, SharePoint, OneDrive, Teams, and Devices.

Reference:

https://learn.microsoft.com/en-us/purview/sit-document-fingerprinting

**NEW QUESTION: 81**

SIMULATION

Username and password

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and select the username below.

To enter your password, place your cursor in the Enter password box and select the password below.

Microsoft 365 Username:

admin@WWLx971455.onmicrosoft.com

Microsoft 365 Password: XXXXXXXXX

If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL "https://admin microsoft.com", and press Enter.

The following information is for technical support purposes only:

Lab Instance: XXXXXXXX.

Task 1

You need to provide users with the ability to manually classify files that contain product information that are stored in SharePoint Online sites. The solution must meet the following requirements:

- The users must be able to apply a classification of Product1 to the files.
- Any authenticated user must be able to open files classified as Product1.
- Files classified as Product1 must be encrypted.

**Answer:**

Restrict access to content by using sensitivity labels to apply encryption When you create a sensitivity label, you can restrict access to content that the label will be applied to. For example, with the encryption settings for a sensitivity label, you can protect content so that:

* Only users within your organization can open a confidential document or email.
* Etc.

How to configure a label for encryption

Step 1: From the Microsoft Purview compliance portal, select Solutions > Information protection > Labels Step 2: Locate and select label Product1.

Step 3: On the Define the scope for this label page, the options selected determine the label's scope for the settings that you can configure and where they'll be visible when they're published:



Step 4: Select Items, and Files. Deselect the other options.

Step 5: Then, on the Choose protection settings for the types of items you selected page, make sure you select Control access.


Step 6: On the Access control page, select Configure access control settings: Turns on encryption with rights management and makes the following settings visible:

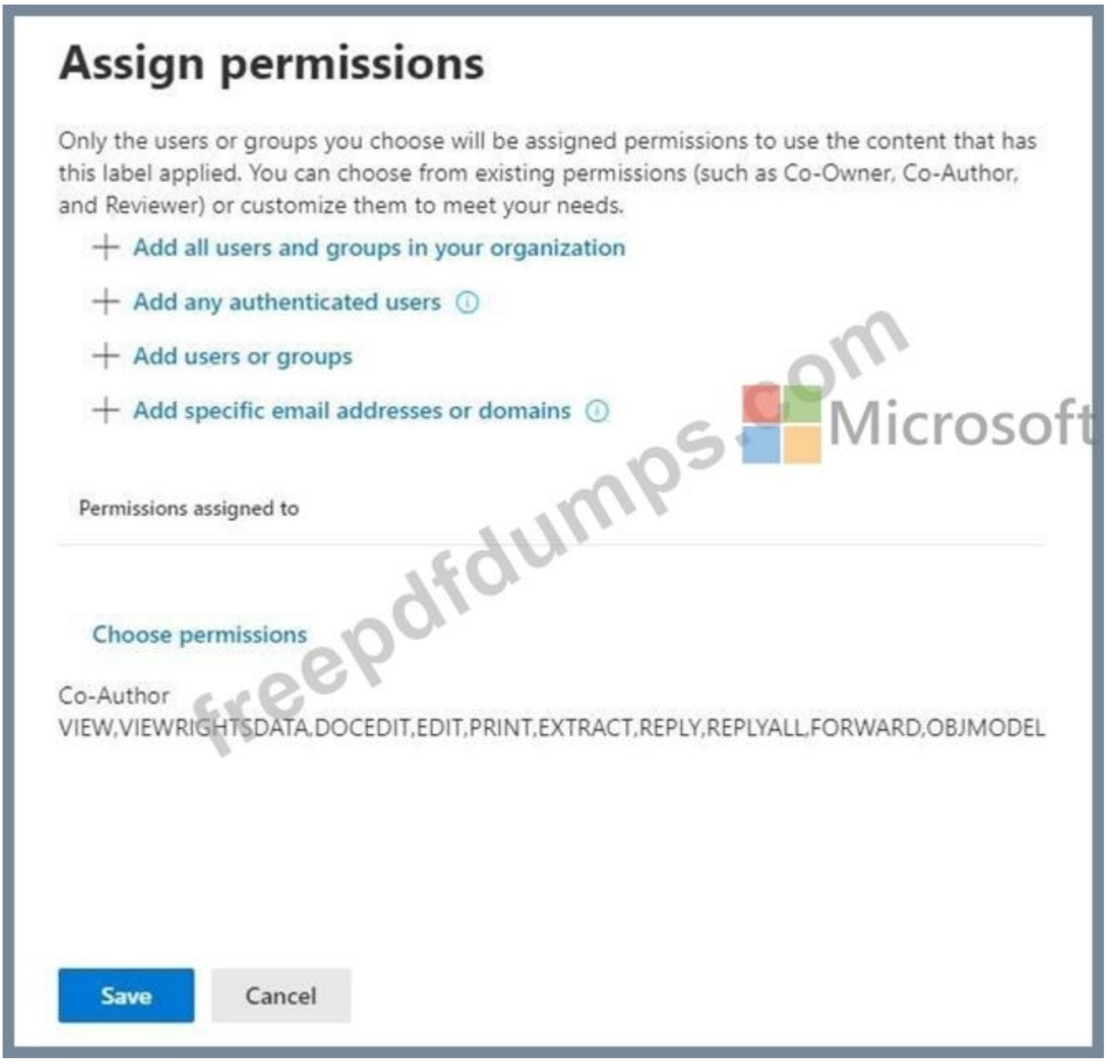

Step 7: Assign permissions to specific users or groups. Add users or groups Step 7a: For users: Any authenticated users.

Step 7b: Permissions: Select View

Note: You can grant permissions to specific people so that only they can interact with the labeled content:

1. First, add users or groups that will be assigned permissions to the labeled content.
2. Then, choose which permissions those users should have for the labeled content.

Assigning permissions:





Step 8: Click Save

Reference:

https://learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with

https://learn.microsoft.com/en-us/purview/encryption-sensitivity-labels

**NEW QUESTION: 82**

You have a Microsoft 365 E5 tenant.

You need to add a new keyword dictionary.

What should you create?

**A.** a trainable classifier

**B.** a retention policy

**C.** a sensitivity label

**D.** a sensitive info type

**Answer: (SHOW ANSWER)**

Connect to the Microsoft Purview compliance portal.
Navigate to Classifications > Sensitive info types.
Select Create and enter a Name and Description for your sensitive info type, then select Next.
https://learn.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword- dictionary?view=o365-worldwide

**NEW QUESTION: 83**
You have a Microsoft 365 E5 subscription that contains two users named User1 and Admin1.
Admin1 manages audit retention policies for the subscription.
You need to ensure that the audit logs of User1 will be retained for 10 years.
What should you do first?
**A.** Assign a Microsoft Purview Audit (Premium) add-on license to Admin1.
**B.** Assign a 10-year audit log retention add-on license to Admin1.
**C.** Assign a Microsoft Purview Audit (Premium) add-on license to User1.
**D.** Assign a 10-year audit log retention add-on license to User1.
**Answer: (SHOW ANSWER)**
To retain a user's Microsoft 365 audit logs for 10 years, you need the 10-Year Audit Log Retention add-on license, which must be assigned to that specific user in addition to an existing Microsoft 365 E5 license or Microsoft 365 E5 Compliance add-on license.
Required Licenses & Components
Microsoft 365 E5 License: This is the base license that enables longer-term retention.
10-Year Audit Log Retention Add-on: This is a separate license that must be purchased and assigned to the specific user whose audit logs you need to retain for 10 years.
Reference:
https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

**NEW QUESTION: 84**
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 implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).
You have computers that run Windows 11 and have Microsoft 365 Apps installed. The computers are joined to a Microsoft Entra tenant.
You need to ensure that Endpoint DLP policies can protect content on the computers.
Solution: You deploy the Microsoft Purview Information Protection client to the computers.
Does this meet the goal?
**A.** Yes
**B.** No
**Answer: (SHOW ANSWER)**

Correct:
* You deploy the Endpoint DLP configuration package to the computers.
* You onboard the computers to Microsoft Defender for Endpoint.
Incorrect:
* You deploy the unified labeling client to the computers.
* You enroll the computers in Microsoft Intune.
* You deploy the Microsoft Purview Information Protection client to the computers.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints

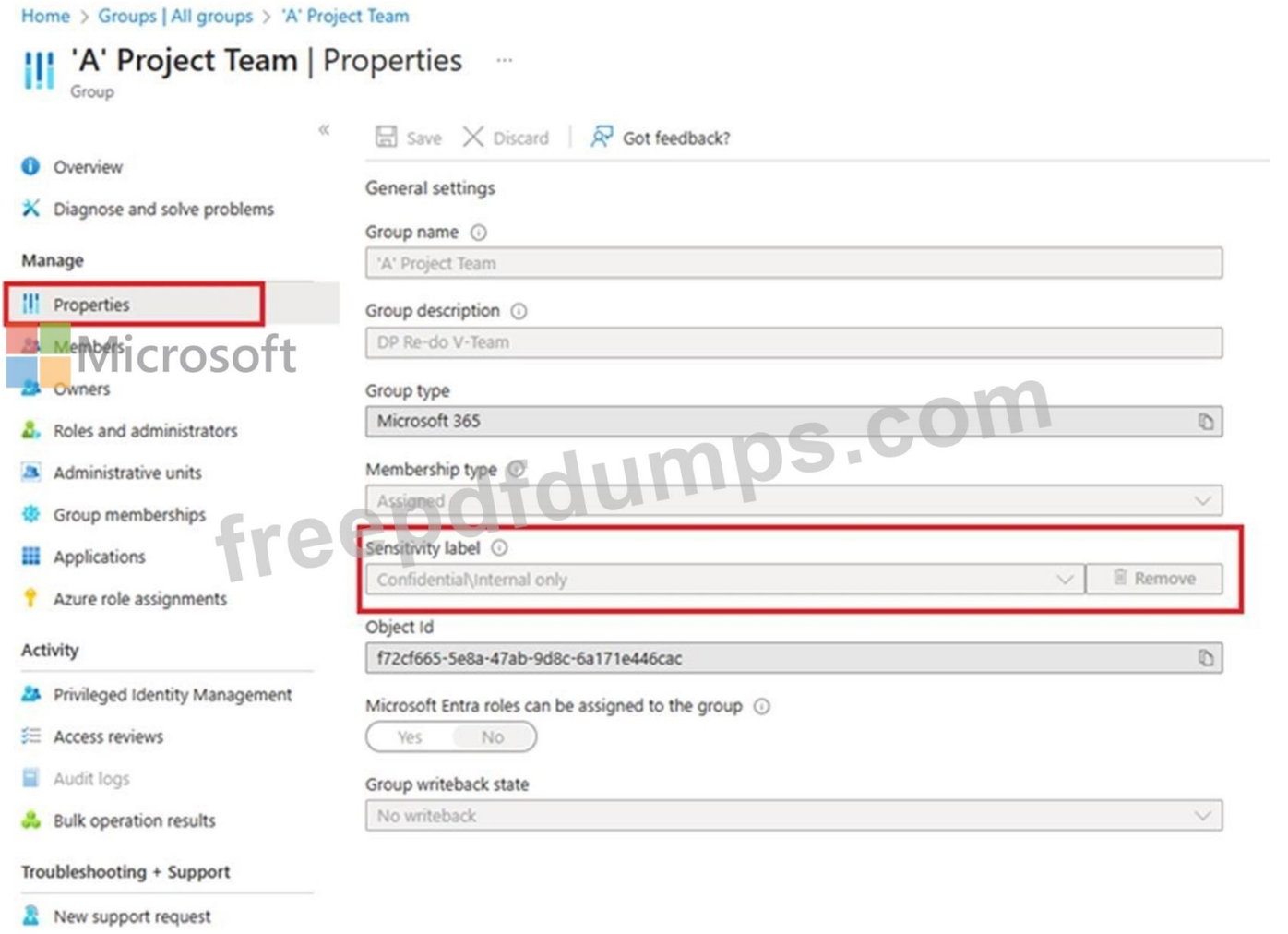
**NEW QUESTION: 85**
You have a Microsoft 365 E5 tenant that has devices onboarded to Microsoft Defender for Endpoint as shown in the following table.

| 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: D (LEAVE A REPLY)**
https://learn.microsoft.com/es-es/purview/endpoint-dlp-getting-started
https://learn.microsoft.com/en-us/purview/device-onboarding-macos-overview#before-you-begin

**NEW QUESTION: 86**
SIMULATION
Username and password
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and select the username below.
To enter your password, place your cursor in the Enter password box and select the password below.
Microsoft 365 Username:
admin@WWLx971455.onmicrosoft.com
Microsoft 365 Password: XXXXXXXXX
If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the

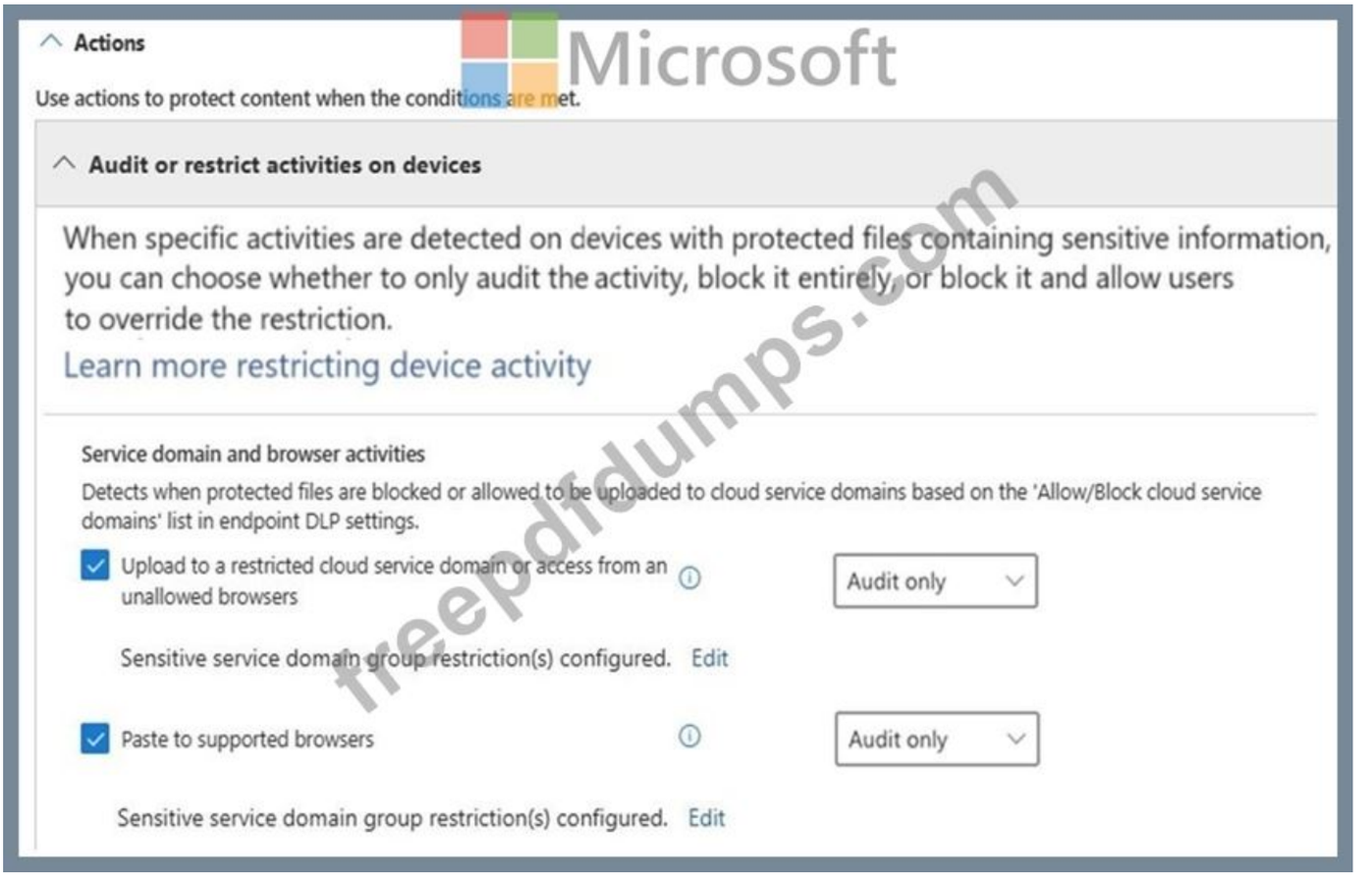
Microsoft Edge browser icon from the task bar, type the URL "https://admin microsoft.com", and press Enter.
The following information is for technical support purposes only:
Lab Instance: XXXXXXXX.
Task 2
You discover that all users can apply the Confidential - Finance label.
You need to ensure that the Confidential - Finance label is available only to the members of the Leadership group.
**Answer:**
Assign sensitivity labels to Microsoft 365 groups in Microsoft Entra ID Microsoft Entra ID supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups. Sensitivity labels apply to groups across services like Outlook, Microsoft Teams, and SharePoint.
Assign a label to an existing group in the Microsoft Entra admin center Step 1: Sign in to the Microsoft Entra admin center as at least a Global Administrator.
Step 2: Select Microsoft Entra ID.
Step 3: Select Groups
Step 4: From the All groups page, select the group that you want to label.
Step 5: On the selected group's page, select Properties and select a sensitivity label from the list.
Select the Confidential - Finance label



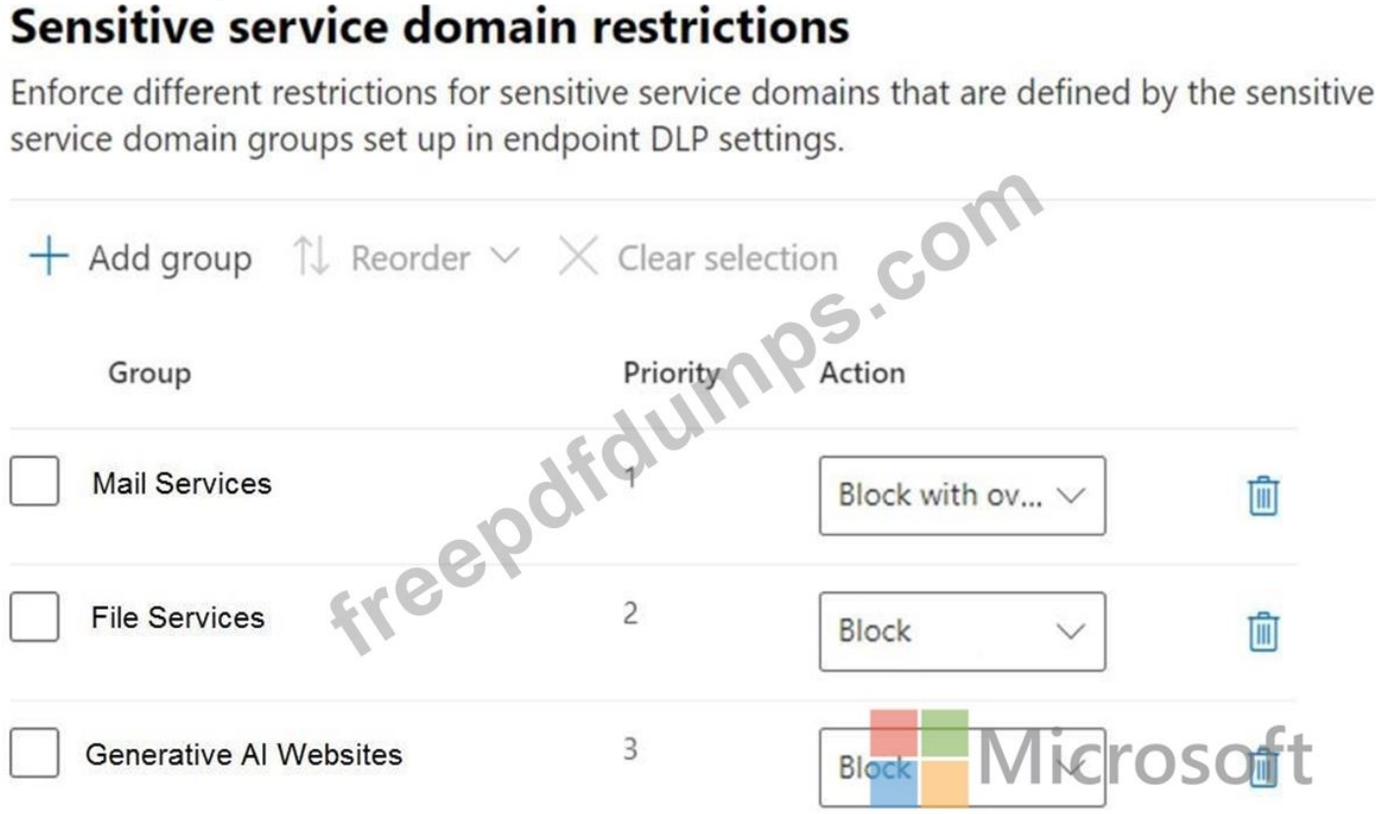



Step 6: Select Save to save your changes.
Reference:
https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels

**NEW QUESTION: 87**
Hotspot Question
You have a Microsoft 365 ES subscription that contains a user named User1. The subscription contains an Endpoint data loss prevention (Endpoint DLP) policy as shown in the Actions exhibit. (Click the Actions tab.)




You configure the Upload to a restricted cloud service domain or access from an unallowed browsers settings as shown in the Upload restrictions exhibit. (Click the Upload restrictions tab.)




You configure the Paste to supported browsers settings as shown in the Paste restrictions exhibit. (Click the Paste restrictions tab.)


When User1 pastes content into ChatGPT, the user receives the error message shown in the Error exhibit. (Click the Error tab.)


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:**

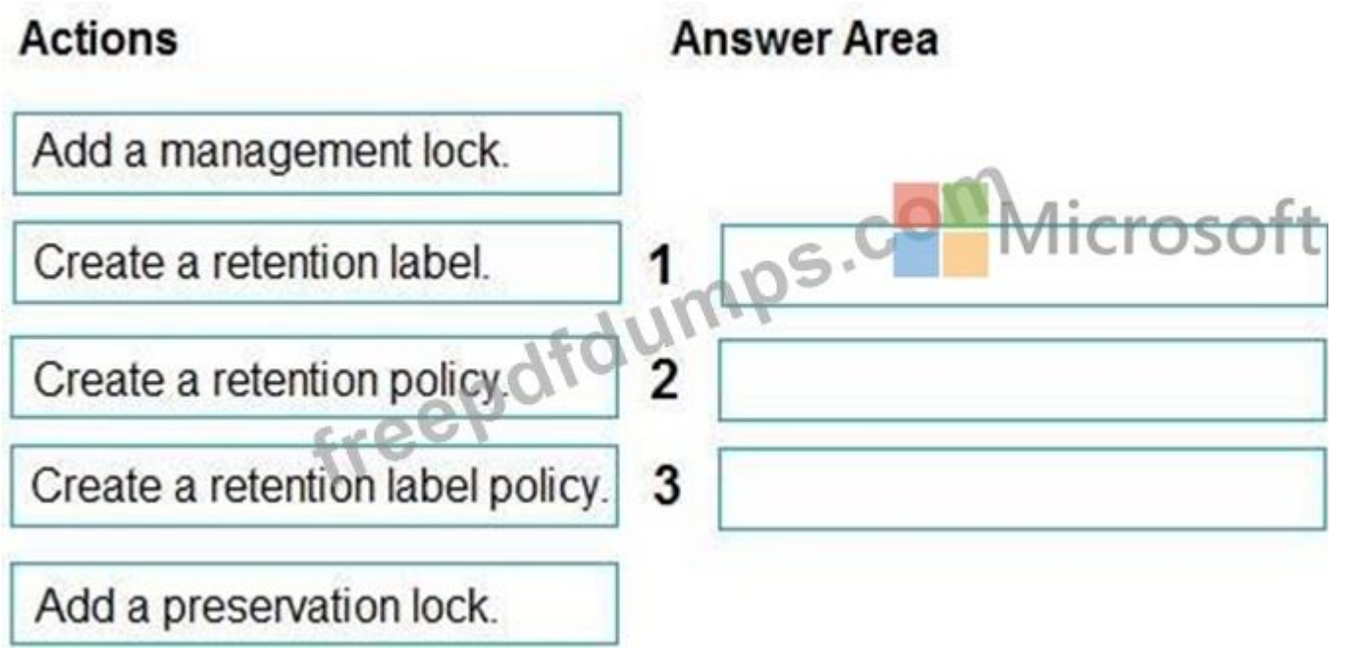
**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 can paste sensitive data from an email to ChatGPT after selecting **Dismiss**. | ○ | ○ |
| User1 can upload emails that contain sensitive data to ChatGPT after selecting **Dismiss**. | ○ | ○ |
| User1 can paste sensitive data from a Microsoft Word document to ChatGPT after selecting **Dismiss**. | ○ | ○ |



Explanation:
Box 1: Yes
We see:
Paste restrictions, Sensitive service domain restrictions, Generate AI Websites: Action: Block with ov..[Block with override].
User1 can override the block.
Box 2: No
We see:
Upload restrictions, Sensitive service domain restrictions, Generate AI Websites: Action: Block
User1 will be blocked.
Box 3: Yes
We see:
Paste restrictions, Sensitive service domain restrictions, Generate AI Websites: Action: Block with ov..[Block with override].
User1 can override the block.
Reference:
https://learn.microsoft.com/en-us/purview/dlp-configure-endpoint-settings

**NEW QUESTION: 88**
Drag and Drop Question
You have a Microsoft 365 tenant.
A new regulatory requirement states that all documents containing a patent ID be labeled, retained for 10 years, and then deleted. The policy used to apply the retention settings must never be disabled or deleted by anyone.
You need to implement the regulatory requirement.
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.




**Answer:**


Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/retention

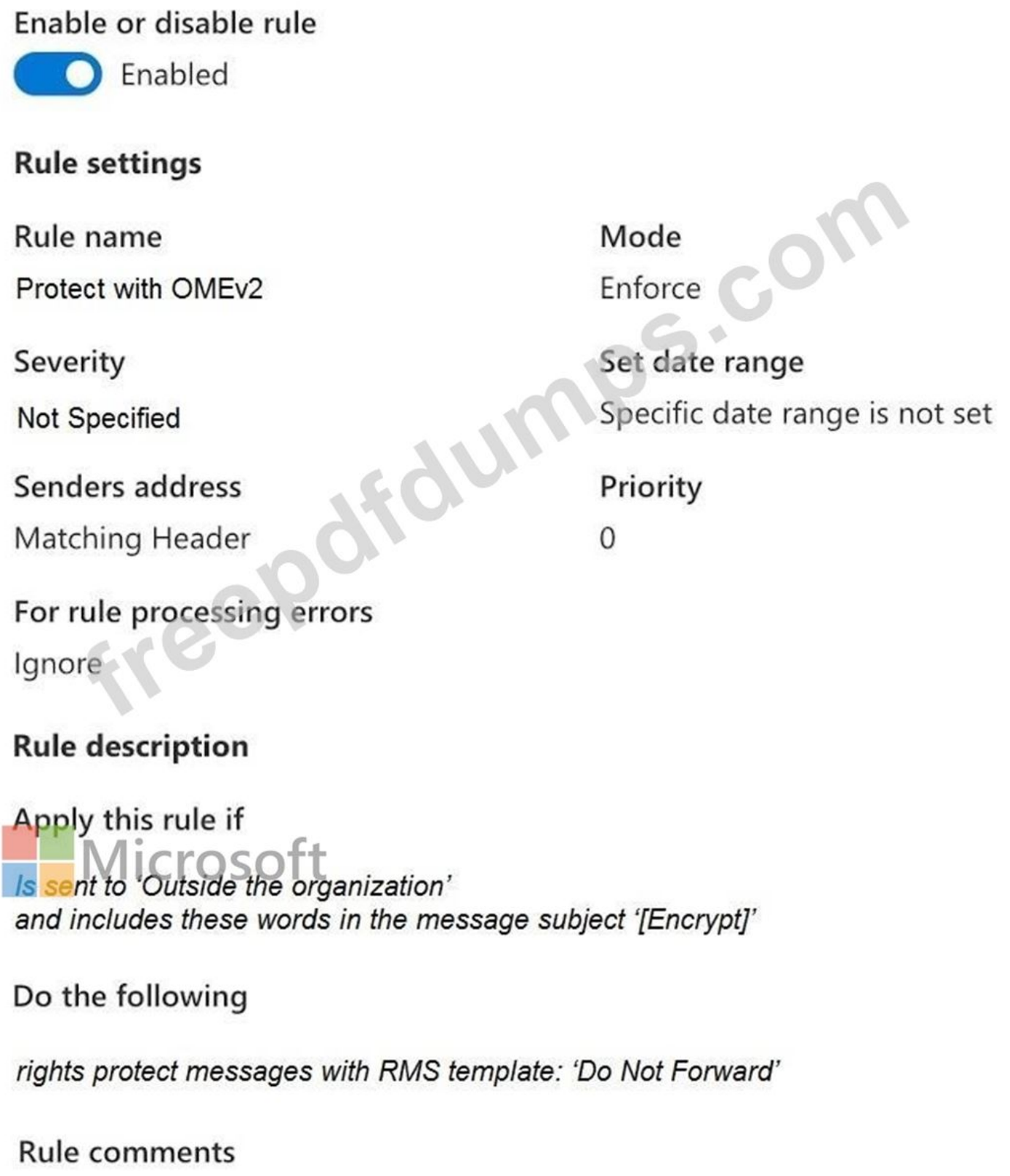
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-preservation-lock

**NEW QUESTION: 89**

Hotspot Question

You have a Microsoft 365 E5 subscription.

In Microsoft Exchange Online, you have the mail flow rule shown in the following exhibit.

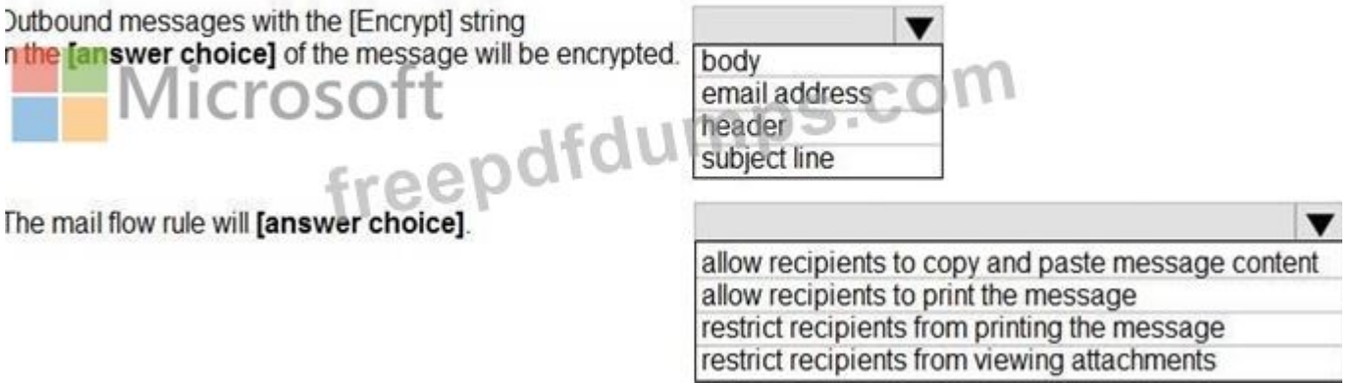




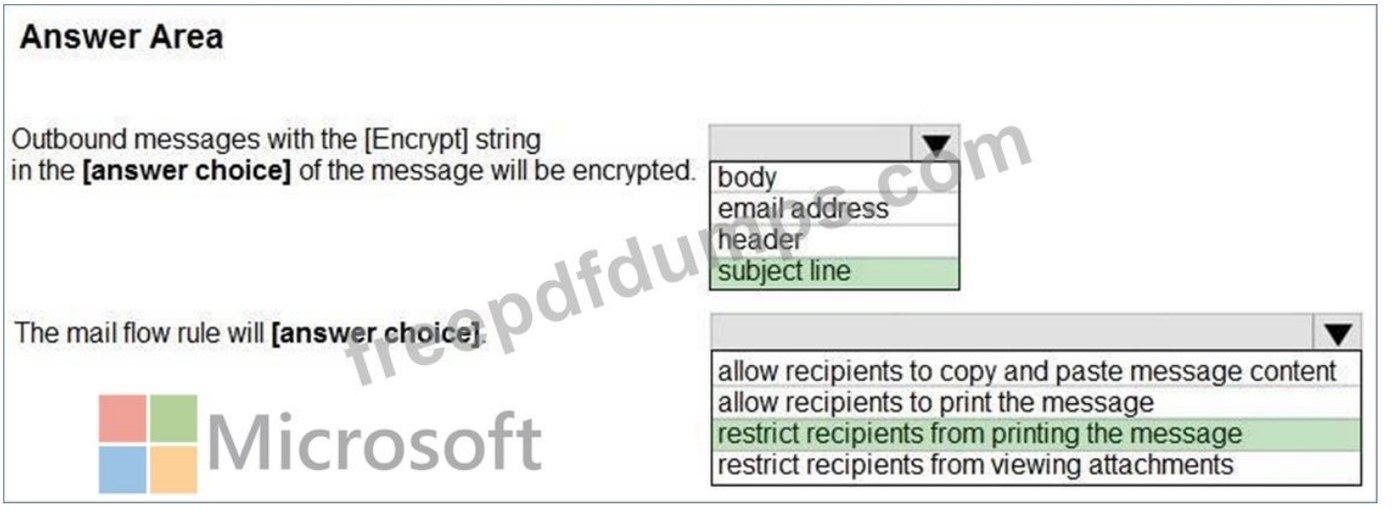

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

**Answer Area**




**Answer:**




Explanation:

Box 1: subject line

Box 2: restrict recipients from printing the message

Note: IRM is an encryption solution that also applies usage restrictions to email messages. It helps prevent sensitive information from being printed, forwarded, or copied by unauthorized people.

IRM capabilities in Microsoft 365 use Azure Rights Management (Azure RMS).

Reference:

https://learn.microsoft.com/en-us/purview/email-encryption

**NEW QUESTION: 90**

You have a Microsoft 365 tenant.

You create the following:

- A sensitivity label
- An auto-labeling policy

You need to ensure that the sensitivity label is applied to all the data discovered by the auto-labeling policy.

What should you do first?

**A.** Run the Enable-TransportRulecmdlet.

**B.** Enable insider risk management.
**C.** Create a trainable classifier
**D.** Run the policy in simulation mode.
**Answer: D (LEAVE A REPLY)**
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically

**NEW QUESTION: 91**
You have a Microsoft 365 E5 subscription that has a sensitivity label named Sensitivity1.
You plan to create an auto-labeling policy that will apply Sensitivity1 to Microsoft Exchange Online mailboxes.
On February 1, you create the auto-labeling policy and enable simulation mode by using the default settings. No modifications are made to the policy in simulation mode.
When will the policy first be turned on?
**A.** February 2
**B.** February 6
**C.** February 15
**D.** never
**Answer: D (LEAVE A REPLY)**
With Microsoft auto-labeling policies in simulation mode, the policy runs a trial run to test its configuration, but it doesn't automatically apply labels to content. Labels will only be applied automatically after the simulation is complete, you've reviewed the results, and you've explicitly enabled the policy for actual labeling.
Enabling for Labeling:
If the simulation results are satisfactory, you then need to enable the policy to start automatically labeling content. This is done by publishing the policy, which essentially switches it from simulation to active mode.
Reference:
https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically



**NEW QUESTION: 92**
Case Study 1 - Contoso, Ltd
Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment

Microsoft 365 Environment

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

| Name | Role |
|---|---|
| Admin1 | Global Reader |
| Admin2 | Compliance Data Administrator |
| Admin3 | Compliance Administrator |
| Admin4 | Security Operator |
| Admin5 | Security Administrator |

Users store data in the following locations:

- SharePoint sites
- OneDrive accounts
- Exchange email
- Exchange public folders
- Teams chats
- Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

| Name | Number of SWIFT codes in the file |
|---|---|
| File1.docx | 1 |
| File2.bmp | 4 |
| File3.txt | 3 |
| File4.xlsx | 7 |

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

| User | Role |
|---|---|
| User1 | Site owner |
| User2 | Site visitor |

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.

Site4 has the following two retention policies applied:

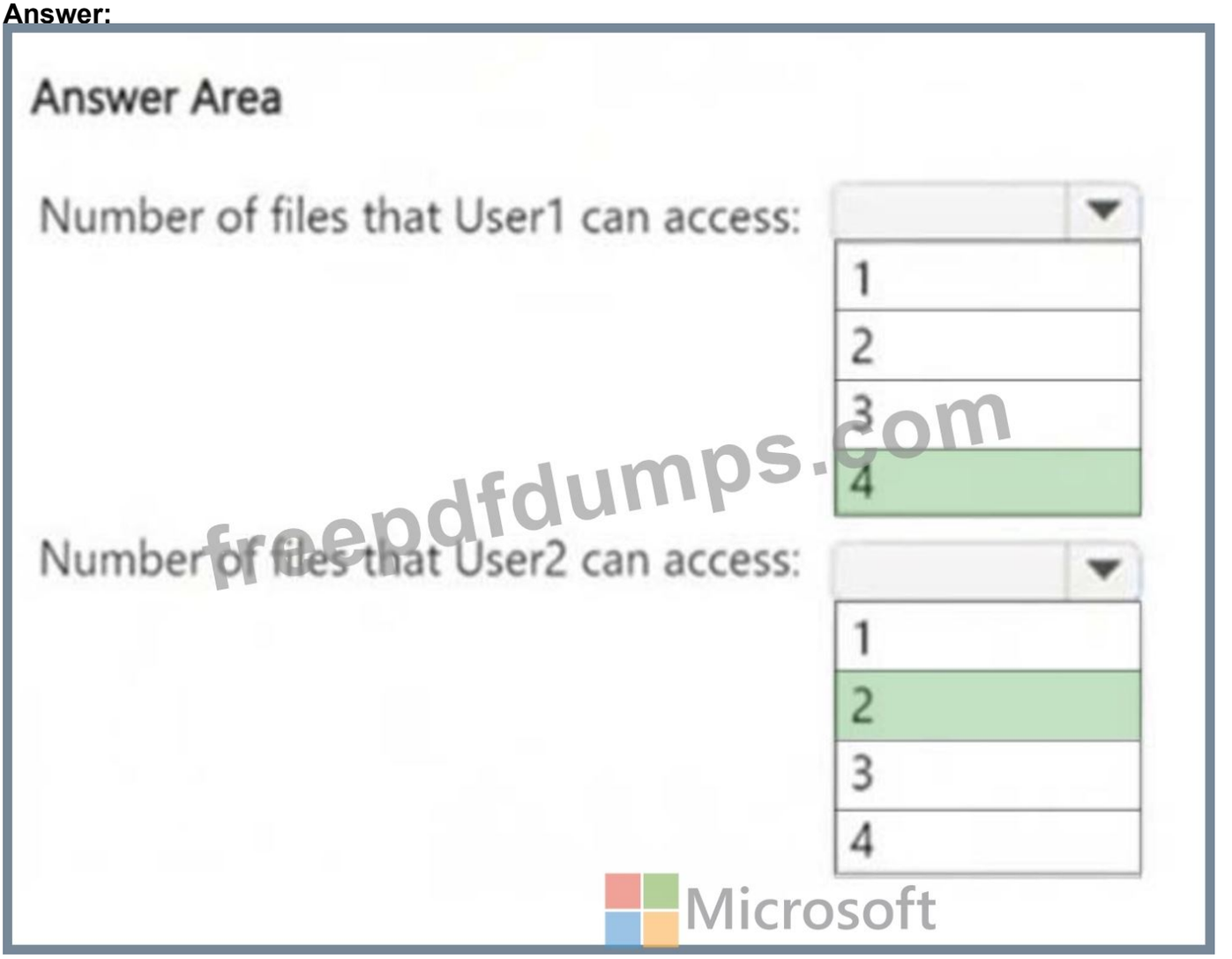
- Name: Site4RetentionPolicy1

Locations to apply the policy: Site4
Delete items older than: 2 years
Delete content based on: When items were created
- Name: Site4RetentionPolicy2
Locations to apply the policy: Site4
Retain items for a specific period: 4 years
Start the retention period based on: When items were created
At the end of the retention period: Do nothing
Problem Statements
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.
Requirements
Planned Changes
Contoso plans to create the following data loss prevention (DLP) policy:
- Name: DLPpolicy1
Locations to apply the policy: Site2
Conditions:
Content contains any of these sensitive info types: SWIFT Code
- Instance count: 2 to any
Actions: Restrict access to the content
Technical Requirements
Contoso must meet the following technical requirements:
- All administrative users must be able to review DLP reports.
- Whenever possible, the principle of least privilege must be used.
- For all users, all Microsoft 365 data must be retained for at least one year.
- Confidential documents must be detected and protected by using Microsoft 365.
- Site1 documents that include credit card numbers must be labeled automatically.
- All administrative users must be able to create Microsoft 365 sensitivity labels.
- After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.
Hotspot Question
How many files in Site2 can User1 and User2 access after you turn on DLPpolicy1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area




**Answer:**





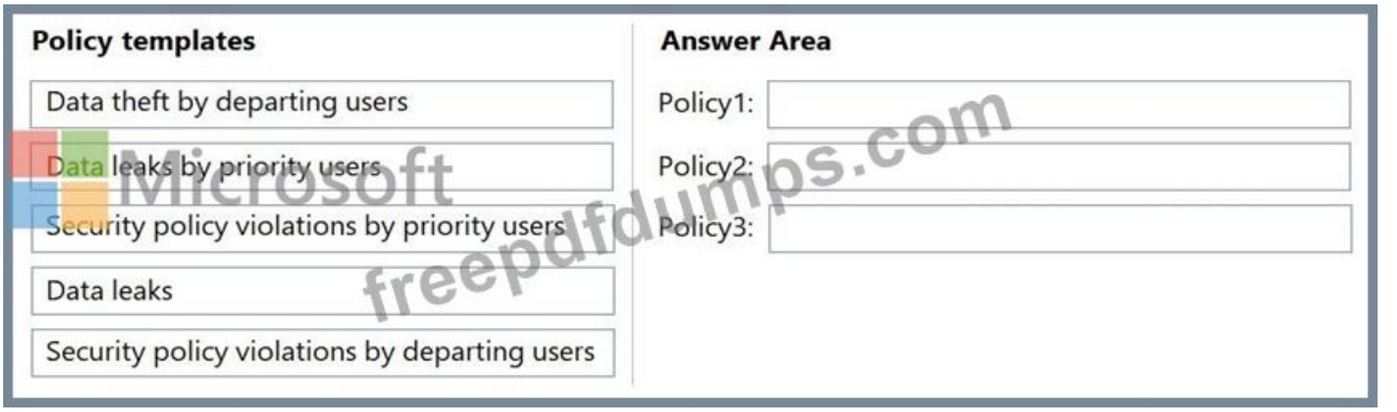

Explanation:

User 1 (Site Owner) - 4 Files
User 2 (Site Visitor) 2 Files
Any item that makes it through the conditions filter has any actions that are defined in the rule applied to it. You have to configure the required options to support the action. For example, if you select Exchange with the Restrict access or encrypt the content in Microsoft 365 locations action, you need to choose from these options:
Block users from accessing shared SharePoint, OneDrive, and Teams content Block everyone. Only the content owner, last modifier, and site admin will continue to have access Block only people from outside your organization. Users inside your organization continue to have access. Encrypt email messages (applies only to content in Exchange)
The actions that are available in a rule depend on the locations that have been selected. The available actions for each individual location are listed below.
https://learn.microsoft.com/en-us/purview/dlp-policy-reference#actions

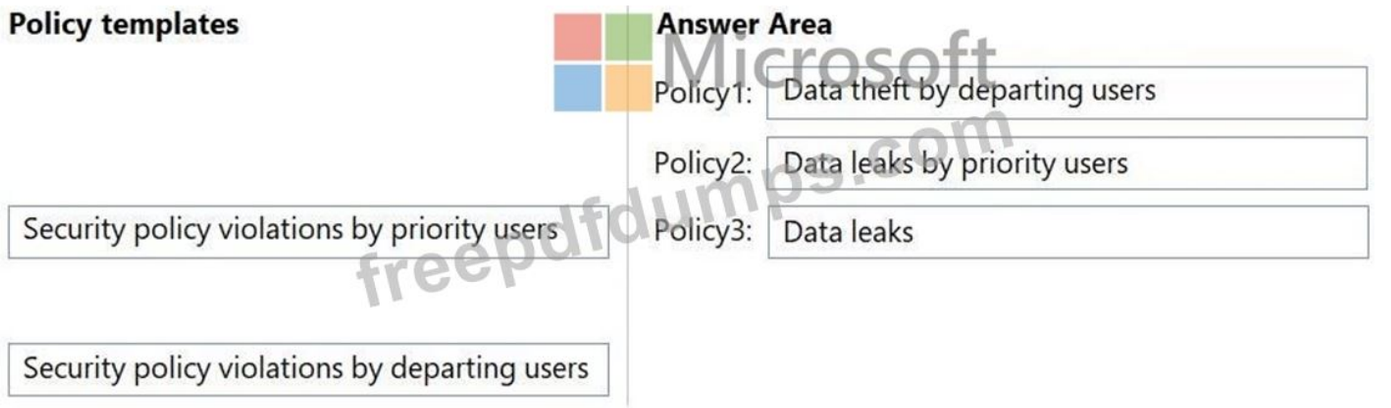
**NEW QUESTION: 93**
Drag and Drop Question
You have a Microsoft 365 E5 subscription.
You need to create the Microsoft Purview insider risk management policies shown in the following table.

| Name | Description |
|---|---|
| Policy1 | Monitors the printing of files by users that submitted their resignation |
| Policy2 | Monitors the accidental sharing of data outside of an organization by users in a priority user group |
| Policy3 | Monitors the downloading of files from Microsoft SharePoint Online to personal cloud storage services |

Which policy template should you use for each policy? To answer, drag the appropriate policy templates to the correct policies. Each template 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.




**Answer:**





Explanation:

Box 1: Data theft by departing users

Policy1: Monitors the printing of files by users that submitted their resignation.

To monitor file printing by departing employees in Microsoft Purview, you should use the Data theft by departing users template and configure a Microsoft 365 HR connector for resignation dates, then add printing as a specific indicator. This template is designed to detect unusual activity from employees who are leaving, and adding the printing indicator will allow you to see specific printing actions in their activity.

Box 2: Data leaks by priority users

Policy2: Monitors the accidental sharing of data of an organization by users in a priority user group.

To detect accidental data sharing by users in a priority user group, you should use the Data leaks by priority users policy template in Microsoft Purview Insider Risk Management. This template is specifically designed to trigger alerts for data leak activities performed by members of a priority user group, making it the most appropriate choice for your scenario.

Box 3: Data leaks

Policy2: Monitors the downloading of files from Microsoft SharePoint Online to personal cloud storage services.

To monitor downloading files from SharePoint Online to personal cloud storage, you should use the Data leaks or Data leaks by priority users policy templates and then configure the policy to use Data Loss Prevention (DLP) indicators. You'll need to create or select an existing DLP policy that identifies the sensitive data being downloaded and configure it to generate alerts for the insider risk management policy.

Reference:

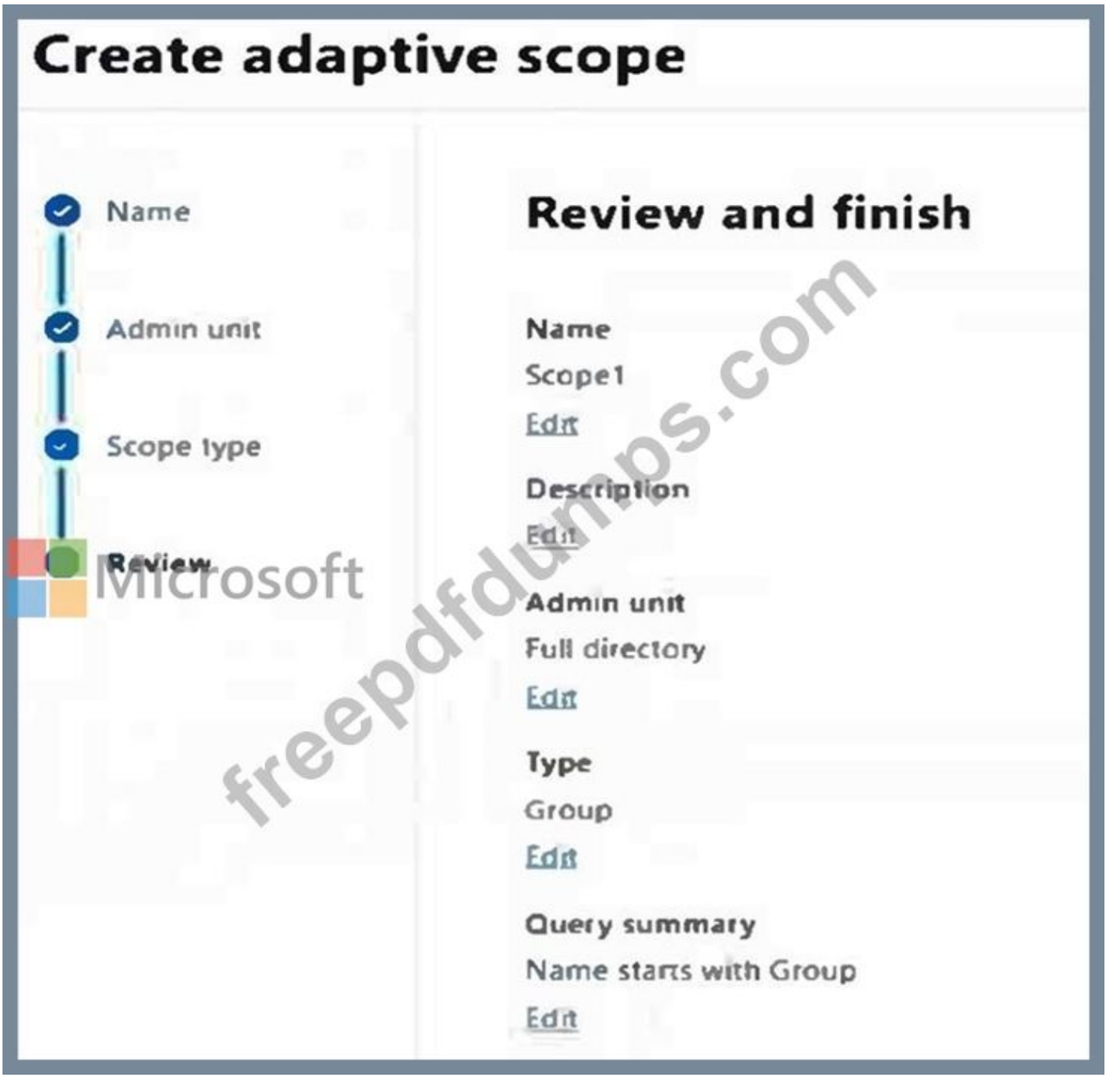
https://learn.microsoft.com/en-us/purview/insider-risk-management-policy-templates

**NEW QUESTION: 94**

Hotspot Question

You have a Microsoft 365 E5 subscription.

You create an adaptive scope named Scope1 as shown in the following exhibit.

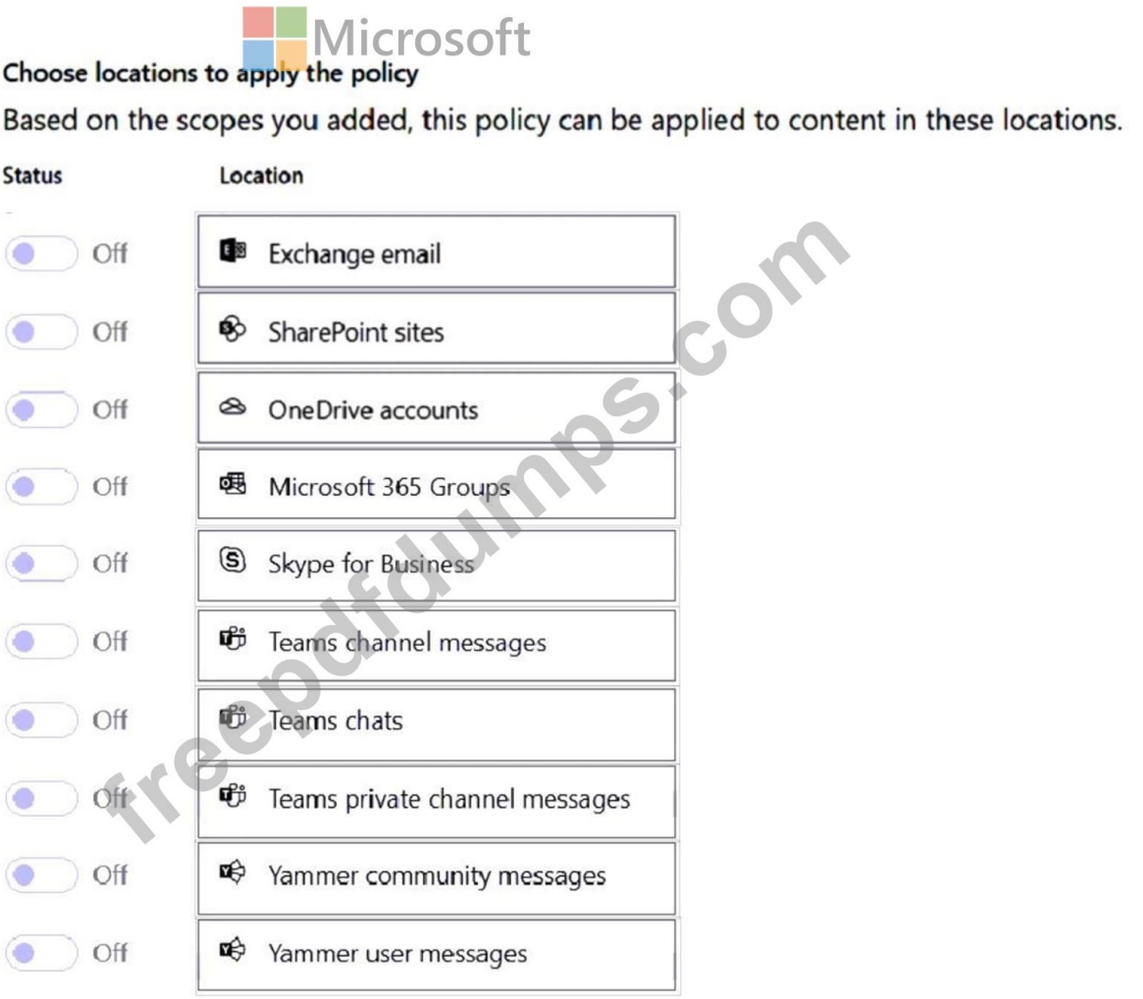



You create a retention policy named Policy1 that includes Scope1.

To which three locations can you apply Policy1? To answer select the appropriate locations in the answer area.

NOTE: Each correct selection is worth one point.

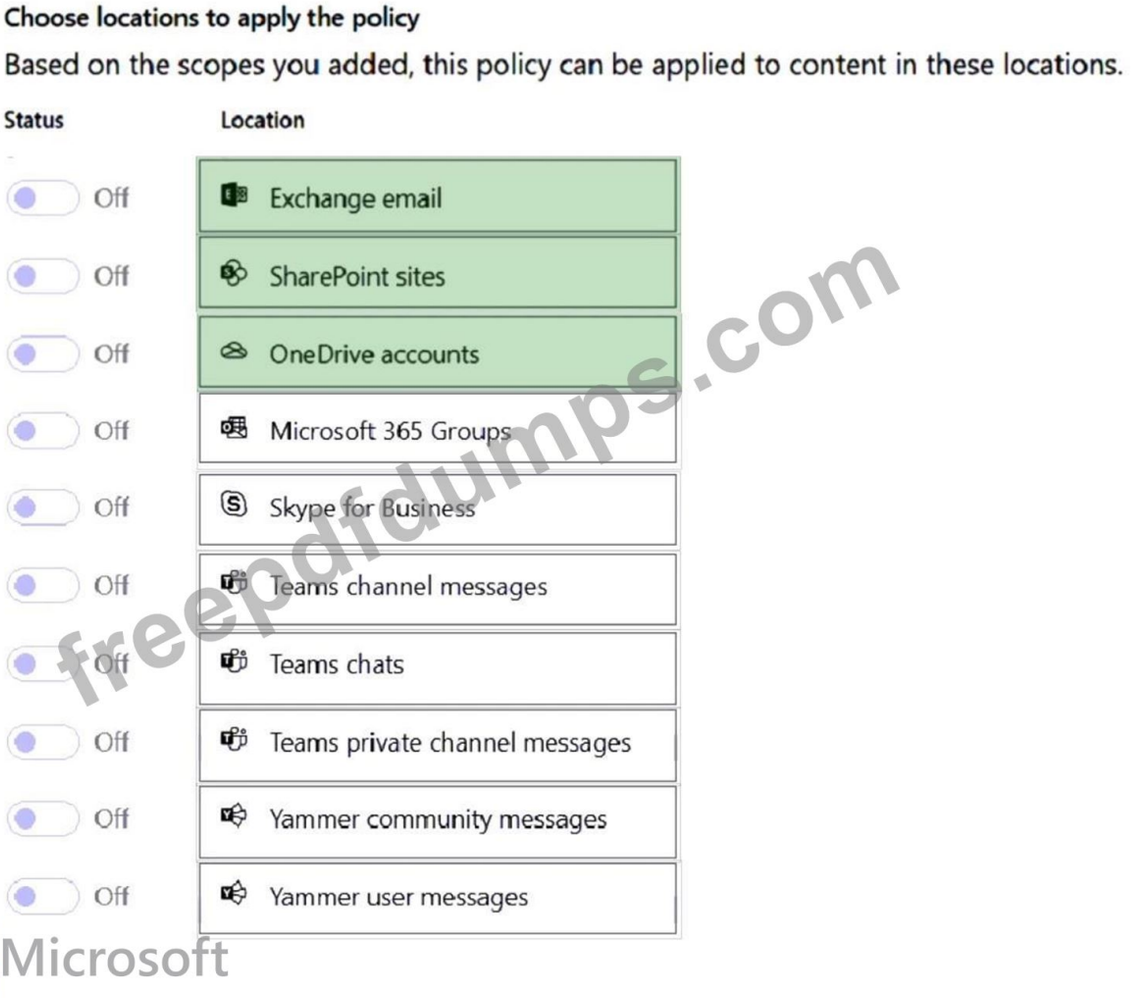
**Answer Area**






**Answer:**

**Answer Area**






Explanation:

A retention policy with an adaptive scope defined by the Microsoft 365 Groups type can be applied to Exchange email, SharePoint sites, and OneDrive accounts. However, the scope is most effective when applied to locations that are a part of the Microsoft 365 Group, such as the group's mailbox (Exchange email) and the group's associated SharePoint site, which includes its OneDrive for Business account.

Box 1: Exchange email

Box 2: SharePoint sites

Box 3: OneDrive accounts

How it works

Adaptive Scopes: These scopes are dynamic filters that automatically identify target locations for a retention policy.

Group Type Scope: When you use the "Microsoft 365 Groups" scope type, it targets content associated with a group, which includes:

The group's mailbox in Exchange.

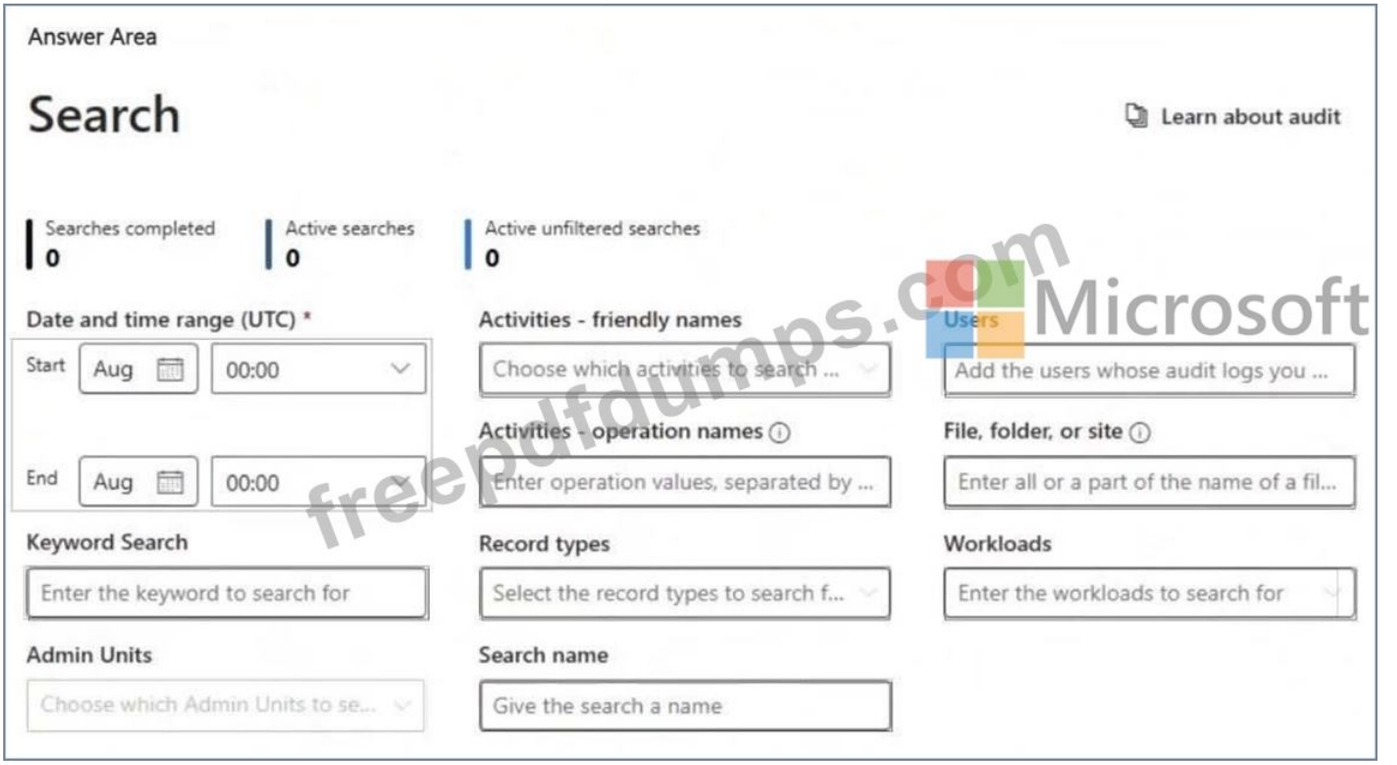
The group's associated SharePoint site.

The group's associated OneDrive for Business account.

Application: The policy is automatically applied to all users and sites within the group, making it a scalable solution for managing retention across the group's entire ecosystem.

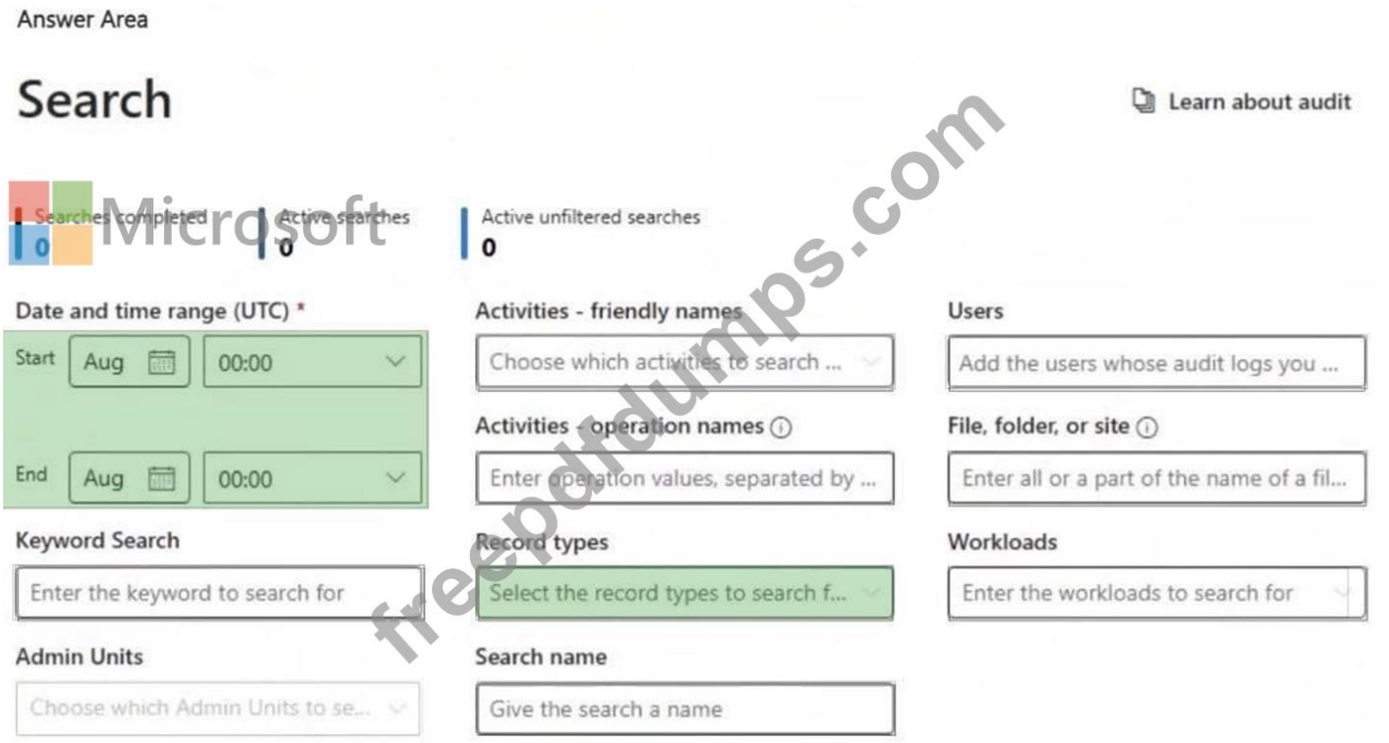
Flexibility: This is particularly useful for organizations where group membership and content locations change frequently, as the policy automatically adapts to these changes.
Reference:
https://learn.microsoft.com/en-us/purview/purview-adaptive-scopes

**NEW QUESTION: 95**
Hotspot Question
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:**

Answer Area




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: 96**

You have a Microsoft 365 subscription that contains the devices shown in the following table.

| Name | Platform | Microsoft Purview | Microsoft Purview client |
|---|---|---|---|
| Device1 | Windows 11 | Not onboarded | Installed |
| Device2 | Windows 10 | Onboarded | Installed |
| Device3 | macOS | Onboarded | Not installed |

From which devices can Microsoft Purview Insider Risk Management capture forensic evidence?

**A.** Device1 only

**B.** Device2 only

**C.** Device1 and Device2 only

**D.** Device2 and Device3 only

**E.** Device1, Device2, and Device3

**Answer: B (LEAVE A REPLY)**

* Device1 - No

Device1 is not onboarded.
* Device2 - Yes
Microsoft Purview Insider Risk Management can capture forensic evidence from both Windows and macOS devices. To do so, devices must be onboarded to Microsoft Purview and have the Microsoft Purview client installed.
* Device3 - No
The Microsoft Purview Client must be installed.
Note:
User devices eligible for forensic evidence capturing must be onboarded to the Microsoft Purview portal and must have the Microsoft Purview Client installed.
Reference:
https://learn.microsoft.com/en-us/purview/insider-risk-management-forensic-evidence-configure

**NEW QUESTION: 97**
You have a Microsoft 365 E5 subscription.
You need to ensure that any message or document containing a credit card number is deleted automatically 12 months after it was created. The solution must minimize administrative effort.
Which two components should you create? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
**A.** an auto-labeling policy for a sensitivity label
**B.** a sensitivity label
**C.** an auto-labeling policy for a retention label
**D.** a retention label
**E.** a sensitive information type (SIT)
**Answer: (SHOW ANSWER)**
1. Create a retention label that retains and delete contents after 12 months
2. Create an Auto Labeling policy "Auto Apply Label" for a retention label

**NEW QUESTION: 98**
You plan to implement Microsoft Purview Advanced Message Encryption.
You need to ensure that encrypted email sent to external recipients expires after seven days.
What should you create first?
**A.** a mail flow rule
**B.** an X.509 version 3 certificate
**C.** a custom branding template
**D.** a remote domain in Microsoft Exchange
**E.** a connector in Microsoft Exchange
**Answer: C (LEAVE A REPLY)**
You can use message expiration on emails that your users send to external recipients who use the OME Portal to access encrypted emails. You force recipients to use the OME portal to view and reply to encrypted emails sent by your organization by using a *custom branded template*

that specifies an expiration date in PowerShell.
Reference:
https://learn.microsoft.com/en-us/purview/ome-advanced-expiration

**NEW QUESTION: 99**
You have a Microsoft 365 subscription linked to a Microsoft Entra tenant that contains a user named User1.
You need to grant User1 permission to search Microsoft 365 audit logs. The solution must use the principle of least privilege.
Which role should you assign to User?
**A.** the View-Only Audit Logs role in the Exchange admin center
**B.** the Reviewer role in the Microsoft Purview portal
**C.** the Security Reader role in the Microsoft Entra admin center
**D.** the Compliance Management role in the Exchange admin center
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 100**
SIMULATION
Username and password
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and select the username below.
To enter your password, place your cursor in the Enter password box and select the password below.
Microsoft 365 Username:
admin@WWLx121586.onmicrosoft.com
Microsoft 365 Password: XXXXXXXXX
If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL "https://admin.microsoft.com", and press Enter.
The following information is for technical support purposes only:
Lab Instance: XXXXXXXXX
Task 4
You need reduce the number of false-positives generated by the General Data Protection Regulation (GDPR) data loss prevention (DLP) policy.
**Answer:**
To reduce false-positives with a GDPR DLP policy, run the policy in audit-only mode first to identify issues, continuously refine the rules based on this data, and train employees on proper data handling.
To run an existing GDPR DLP policy in audit mode, you need to edit the policy in your Microsoft Purview portal and set the policy mode to "simulation" or "test". In the policy configuration, select the option to "Run the policy in simulation mode" or "Test mode" instead of enabling enforcement

immediately. This will log any violations without blocking them, allowing you to review the results before a full deployment.
Steps to run a policy in audit (simulation) mode
Step 1: Navigate to DLP policies: Sign in to the Microsoft Purview portal and go to Data loss prevention > Policies.
Step 2: Edit the policy: Select the existing GDPR policy you want to run and choose to edit it.
Step 3: Locate the policy mode settings: In the policy configuration workflow, find the page for policy mode, which may be labeled as "Policy Mode" or "Simulate or turn on the policy".
Step 4: Enable simulation mode: Choose the option to "Run the policy in simulation mode".
Step 5: Configure optional settings: You can also choose to "Show policy tips" in simulation mode to help educate users about potential violations without actually blocking them. [Skip] Step 6: Save and submit: Proceed through the rest of the wizard and select Next and Submit to save your changes.
Reference:
https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp

**NEW QUESTION: 101**
You have a Microsoft SharePoint Online site named Site1 that contains the files shown in the following table.

| Name | Number of IP addresses in the file |
|---|---|
| File1 | 2 |
| File2 | 3 |

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

| Name | Content contains | Policy tip | If match, stop processing | Priority |
|---|---|---|---|---|
| Rule1 | 1 or more IP addresses | Tip1 | No | 0 |
| Rule2 | 3 or more IP addresses | Tip2 | Yes | 1 |
| Rule3 | 2 or more IP addresses | Tip3 | No | 2 |



You apply DLP1 to Site1.
Which policy tips will appear for File2?
**A.** Tip1 only
**B.** Tip2 only
**C.** Tip3 only
**D.** Tip1 and Tip2 only
**Answer: A (LEAVE A REPLY)**
It's possible for content to match several rules in a DLP policy, but only the policy tip from the most restrictive, highest-priority rule will be shown. For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.
https://learn.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy- tips?view=o365-worldwide

**NEW QUESTION: 102**
You have a Microsoft 365 E5 subscription that contains a user named User1.
You deploy Microsoft Purview Data Security Posture Management for AI (DPSM for AI).
You need to ensure that User1 can review default policies that were created as part of the deployment. The solution must follow the principle of least privilege.
To which role groups should you add User1?
**A.** Compliance Administrator and Compliance Data Administrator
**B.** Content Explorer Content Viewer and View-Only Organization Management for Microsoft Exchange Online
**C.** Security Reader and Insider Risk Management Investigators
**D.** Compliance Management and Organization Management for Microsoft Exchange Online
**Answer: C (LEAVE A REPLY)**
Microsoft Purview Security Reader role group and also Insider Risk Management Investigators.
Note:
Permissions for Data Security Posture Management for AI
Members of your security and compliance teams who are responsible for managing AI apps in the Microsoft Purview Data Security Posture Management for AI need appropriate permissions when they sign in to the Microsoft Purview portal.
Permissions by activities

| Activities | Microsoft Entra Compliance Administrator role | Microsoft Entra Global Administrator role | Microsoft Purview Compliance Administrator role group | Roles or role groups that are view-only* | When not supported, additional role groups required |
|---|---|---|---|---|---|
| View all policies in the policy list | ✓ | ✓ | ✓ | ✓ Excludes: Insider risk management policies<br>Communication compliance policies | For insider risk management polices: Microsoft Purview Insider Risk Management Administrator<br>Microsoft Purview Insider Risk Management Analyst<br>Microsoft Purview Insider Risk Management Investigator |



Note 2:
Roles and role groups that can view, create, and edit in Data Security Posture Management for

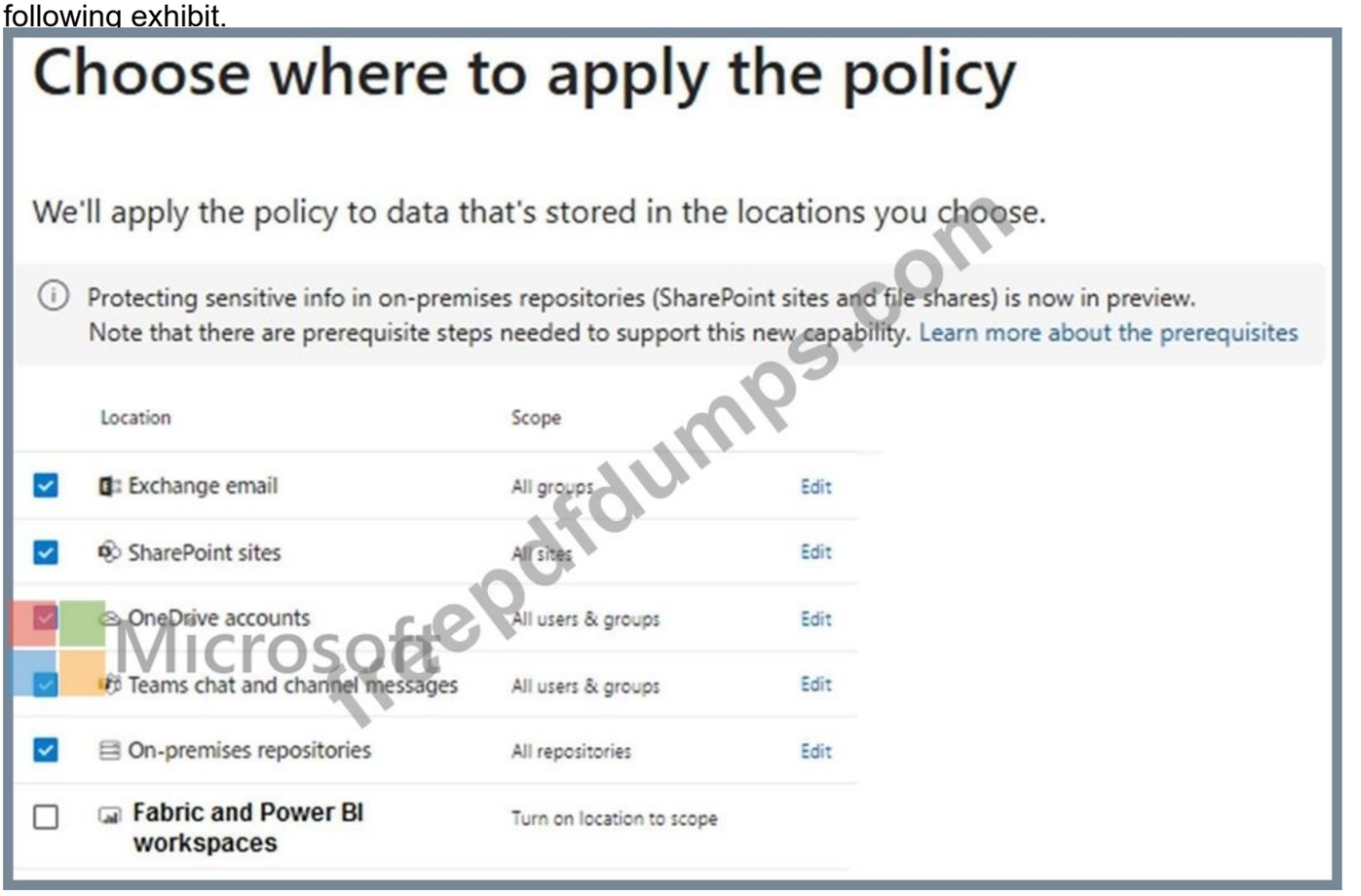
AI:
Microsoft Entra Compliance Administrator role
Microsoft Entra Global Administrator role
Microsoft Purview Compliance Administrator role group
Roles and role groups that can view-only in Data Security Posture Management for AI:
*-> Microsoft Purview Security Reader role group
Purview Data Security AI Viewer role
AI Administrator role from Entra
Purview Data Security AI Content Viewer role for AI interactions only
Purview Data Security Content Explorer Content Viewer role for AI interactions and file details for data risk assessments only Reference:
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-permissions

**NEW QUESTION: 103**
You have a Microsoft 365 E5 tenant that has a retention label named Label1.
You need to create an auto-labeling policy that will apply Label1.
To which location can Label1 be applied?
**A.** OneDrive accounts
**B.** Microsoft Entra security groups
**C.** Microsoft Defender for Cloud Apps
**D.** Teams chats
**Answer: A (LEAVE A REPLY)**
Correct:
* OneDrive accounts
Incorrect:
* Microsoft Defender for Cloud Apps
* Microsoft Entra security groups
* on-premises repositories
* Teams channel messages
* Teams chats
Note:
A Microsoft 365 auto-labeling policy can be applied to Exchange mailboxes, SharePoint sites, and OneDrive accounts. It can also be applied to content within Teams and other Microsoft 365 Groups, as well as Azure services like Azure SQL and Azure Cosmos DB.
Exchange Online: Applies to emails in transit.
SharePoint: Applies to documents stored at rest in SharePoint sites.
OneDrive: Applies to documents stored at rest in OneDrive accounts.
Teams: Applies to documents stored in the SharePoint sites associated with a Team.
Azure and other data sources: Can be extended to apply to data stored in services like Azure SQL, Azure Cosmos DB, and more.
Reference:

https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically

**NEW QUESTION: 104**

You are creating a DLP policy named Policy1 that will be applied to the locations as shown in the following exhibit.




Policy1 contains an advanced data loss prevention (DLP) rule named Rule1.

Which two conditions can you use in Rule1? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

**A.** Document property is

**B.** Attachment's file extension is

**C.** Document size equals or is greater than

**D.** Content is shared from Microsoft 365

**E.** Content contains

**Answer: D,E (LEAVE A REPLY)**

* Content is shared from Microsoft 365

This rule will detect if one of your employees is sharing sensitive info outside of your organization.

* Content contains

Messages or documents that contain sensitive information as defined by Microsoft Purview Data Loss Prevention (DLP) policies.

Reference:

https://learn.microsoft.com/en-us/purview/dlp-exchange-conditions-and-actions

**NEW QUESTION: 105**

Hotspot Question

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You have a Microsoft SharePoint site named Site1. Site1 stores files that contain IP addresses as shown in the following table.

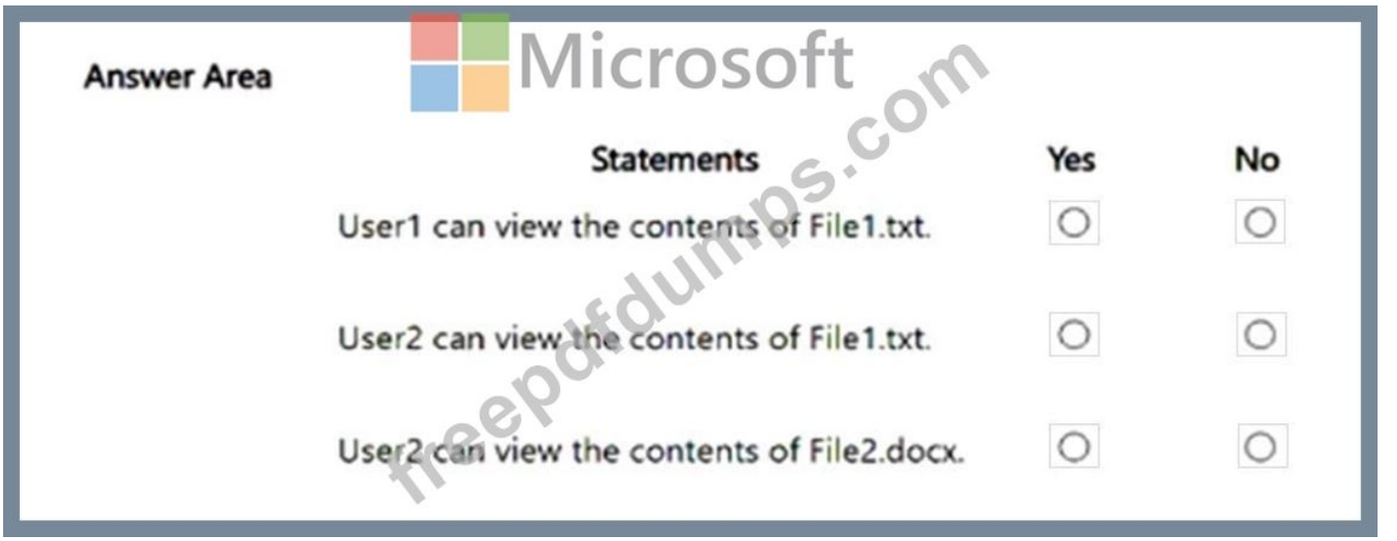
| Name | Number of IP addresses |
|---|---|
| File1.txt | 3 |
| File2.docx | 1 |

User1 is assigned the SharePoint admin role for Site1. User2 is a member of Site1.

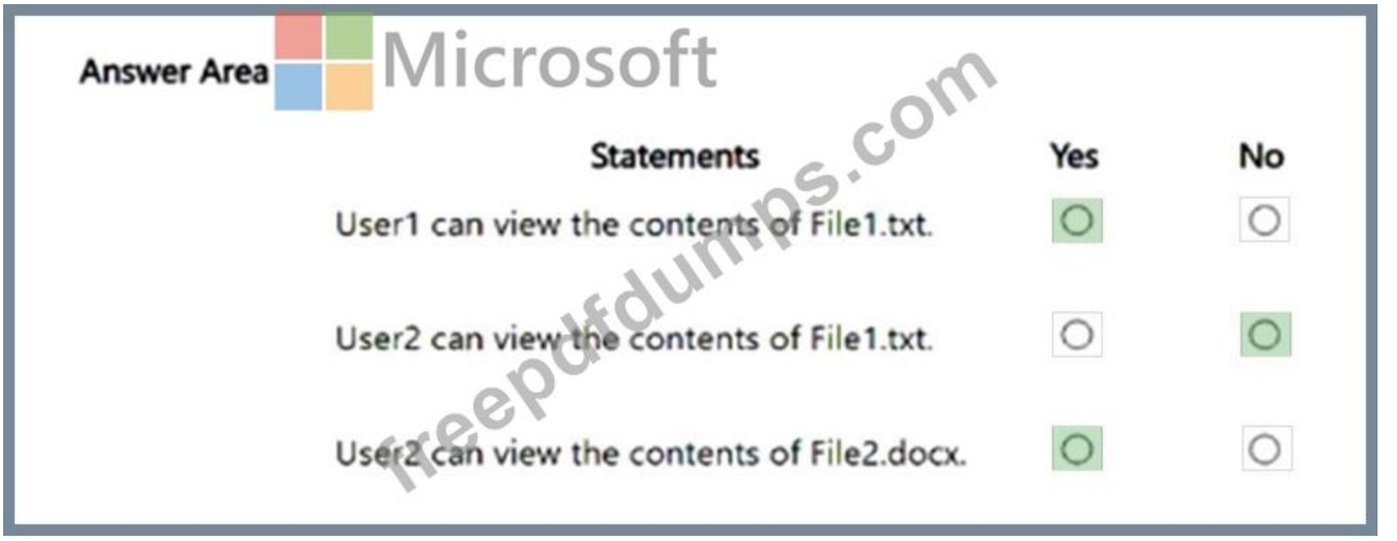
You create the data loss prevention (DLP) policy shown in the following exhibit.




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:**




Explanation:

Box 1: Yes

Note: Key tasks of the SharePoint admin

Here are some of the key tasks users can do when they are assigned to the SharePoint admin role:

Create sites

Delete sites

Manage sharing settings at the organization level

Add and remove site admins

Manage site storage limits

Box 2: No

File1.text contains 3 IP addresses.

Box 3: Yes

File2.docx contains only 1 IP address.

**NEW QUESTION: 106**

Hotspot Question

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

| Name | Type |
|---|---|
| Group1 | Microsoft 365 |
| Group2 | Security |

The subscription contains the resources shown in the following table.

| Name | Type |
|---|---|
| Site1 | Microsoft SharePoint Online site |
| Team1 | Microsoft Teams team |

You create a sensitivity label named Label1.

You need to publish Label1 and have the label apply automatically.

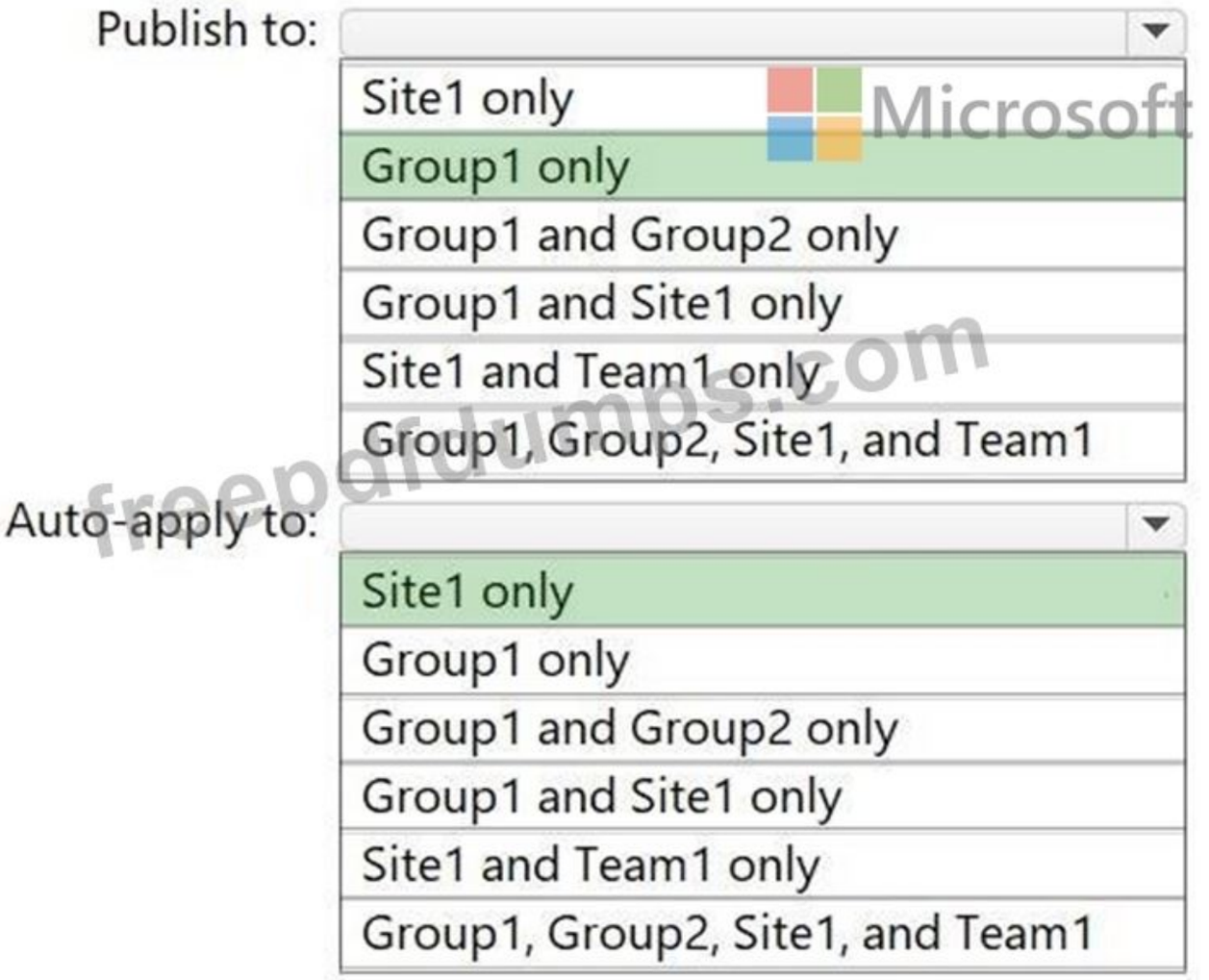
To what can you publish Label1, and to what can Label1 be auto-applied? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.




**Answer:**

**Answer Area**






Explanation:

There are two different methods for automatically applying a sensitivity label to content in Microsoft 365

1. Client-side labeling when users edit documents or compose (also reply or forward) emails

2.Service-side labeling when content is already saved (in SharePoint or OneDrive) or emailed (processed by Exchange Online).



**NEW QUESTION: 107**

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 (LEAVE A REPLY)**
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: 108**
You need to provide a user with the ability to view data loss prevention (DLP) alerts in the Microsoft Purview portal. The solution must use the principle of least privilege.
Which role should you assign to the user?
**A.** Security Operator
**B.** Security Reader
**C.** Compliance Data Administrator
**D.** Compliance Administrator
**Answer: (SHOW ANSWER)**
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies

**NEW QUESTION: 109**
Hotspot Question
You have a Microsoft 365 E5 subscription that uses Microsoft Teams and contains the users shown in the following table.

| Name | Team membership |
|---|---|
| User1 | Team1, Team2 |
| User2 | Team2 |

You have the retention policies shown in the following table.

| Name | Location | Included | Retain items for | Start retention period | At the end of retention period |
|---|---|---|---|---|---|
| Policy1 | Microsoft Teams channel messages | All teams | 7 years | When items are created | Delete items automatically |
| | Microsoft Teams chats | User1 | | | |
| Policy2 | Microsoft Teams channel messages | Team1 | 5 years | When items are created | Delete items automatically |
| | Microsoft Teams chats | User2 | | | |

The users perform the actions shown in the following table.

| User | Location | Action |
|---|---|---|
| User1 | Team1 channel | Edits a message |
| User2 | Private 1:1 chat with User1 | Sends a message to User1 |
| User1 | Team2 channel | Deletes a message |

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 |
|---|---|---|
| The message edited by User1 will be deleted after five years. | ○ | ○ |
| User1 can see the message sent by User2 for up to seven years. | ○ | ○ |
| The message deleted by User1 will be moved to the SubstrateHolds folder. | ○ | ○ |

**Answer:**

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| The message edited by User1 will be deleted after five years. | ○ | ◉ |
| User1 can see the message sent by User2 for up to seven years. | ○ | ◉ |
| The message deleted by User1 will be moved to the SubstrateHolds folder. | ◉ | ○ |

Explanation:

Box 1: No

It will be retained for seven years.

Both Policy1 and Policy2 apply.

If there is a conflict in how long to retain the same content, it is retained in the secured location for the longest retention period.

Note: If you configure a Teams retention policy to retain chats or channel messages, users Box 2: No User2 creates the message in chat. Policy2 applies. The message will be retained for 5 years.

Box 3: Yes

After a retention policy is configured for chat and channel messages, a timer job from the Exchange service periodically evaluates items in the hidden mailbox folder where these Teams messages are stored. The timer job typically takes 1-7 days to run. When these items have

expired their retention period, they are moved to the SubstrateHolds folder-another hidden folder that's in every user or group mailbox to store "soft-deleted" items before they're permanently deleted.
Messages remain in the SubstrateHolds folder for at least 1 day, and then if they're eligible for deletion, the timer job permanently deletes them the next time it runs.
Reference:
https://docs.microsoft.com/en-us/microsoftteams/retention-policies
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-teams

**NEW QUESTION: 110**
Case Study 1 - Contoso, Ltd
Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.
Existing Environment
Microsoft 365 Environment
Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

| Name | Role |
|---|---|
| Admin1 | Global Reader |
| Admin2 | Compliance Data Administrator |
| Admin3 | Compliance Administrator |
| Admin4 | Security Operator |
| Admin5 | Security Administrator |



Users store data in the following locations:
- SharePoint sites
- OneDrive accounts
- Exchange email
- Exchange public folders
- Teams chats
- Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.
SharePoint Online Environment
Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.
Site2 contains the files shown in the following table.

| Name | Number of SWIFT codes in the file |
|---|---|
| File1.docx | 1 |
| File2.bmp | 4 |
| File3.txt | 3 |
| File4.xlsx | 7 |

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

| User | Role |
|---|---|
| User1 | Site owner |
| User2 | Site visitor |

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.

Site4 has the following two retention policies applied:

- Name: Site4RetentionPolicy1

Locations to apply the policy: Site4

Delete items older than: 2 years

Delete content based on: When items were created

- Name: Site4RetentionPolicy2

Locations to apply the policy: Site4

Retain items for a specific period: 4 years

Start the retention period based on: When items were created

At the end of the retention period: Do nothing

Problem Statements

Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements

Planned Changes

Contoso plans to create the following data loss prevention (DLP) policy:

- Name: DLPpolicy1

Locations to apply the policy: Site2

Conditions:

Content contains any of these sensitive info types: SWIFT Code

- Instance count: 2 to any

Actions: Restrict access to the content

Technical Requirements

Contoso must meet the following technical requirements:

- All administrative users must be able to review DLP reports.
- Whenever possible, the principle of least privilege must be used.
- For all users, all Microsoft 365 data must be retained for at least one year.
- Confidential documents must be detected and protected by using Microsoft 365.

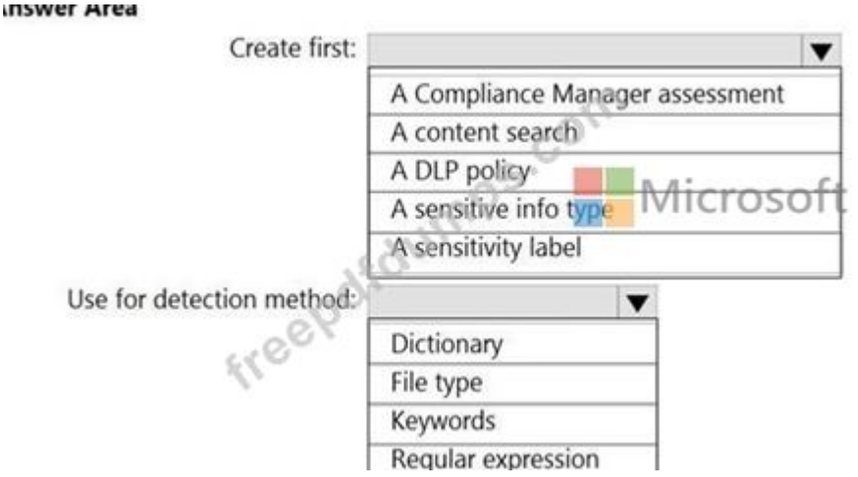
- Site1 documents that include credit card numbers must be labeled automatically.
- All administrative users must be able to create Microsoft 365 sensitivity labels.
- After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

Hotspot Question

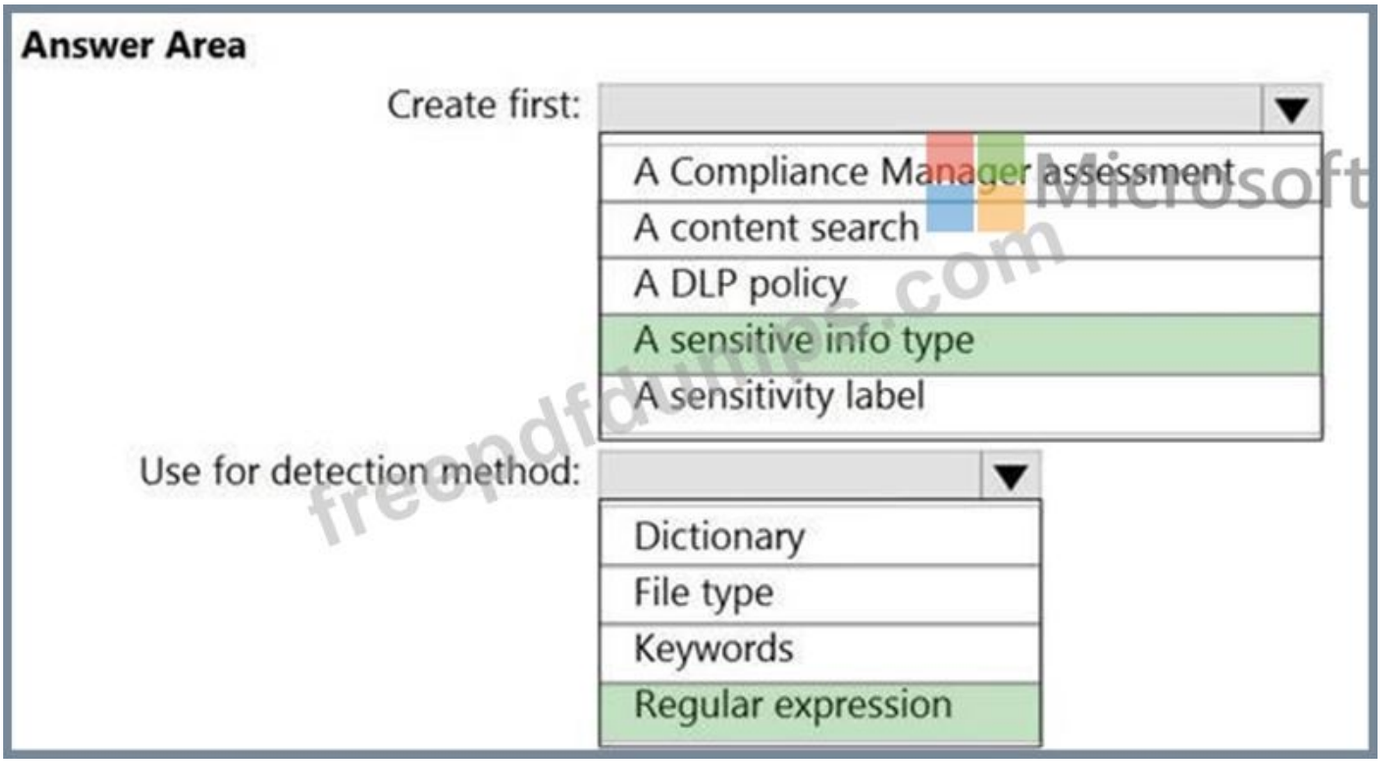
You need to meet the technical requirements for the confidential documents.

What should you create first, and what should you use for the detection method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.




**Answer:**




Explanation:

Sensitive information types :

Identifies sensitive data by using built-in or custom regular expressions or a function.

Corroborative evidence includes keywords, confidence levels, and proximity.
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide

**NEW QUESTION: 111**
Hotspot Question
You have a Microsoft 365 E5 subscription that contains the sensitive information types (SITs) shown in the following table.

| Name | Primary element | Character proximity | Supporting elements | Additional checks |
|---|---|---|---|---|
| SIT1 | Regular expression: `prd:\d{4}` | 15 | Keyword: product | *None* |
| SIT2 | Regular expression: `(\d{10}\d{12})` | *None* | *None* | Exclude specific values: 111-111-1111 |
| SIT3 | Function: `Func_credit_card` | *None* | *None* | *None* |

A user sends the email messages shown in the following table.

| Name | Content |
|---|---|
| Email1 | The product code you requested for the bicycle is prd:1234. |
| Email2 | The bank account number is 123456789012. Contact your account rep at 111-111-1111. |
| Email3 | Please use my credit card that ends with 0023 and has an expiration date of 01/25. |

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 |
|---|---|---|
| SIT1 will identify and match the content in Email1. | ○ | ○ |
| SIT2 will identify and match the content in Email2. | ○ | ○ |
| SIT3 will identify and match the content in Email3. | ○ | ○ |

**Answer:**

Answer Area

| Statements | Yes | No |
|---|---|---|
| SIT1 will identify and match the content in Email1. | ○ | ○ |
| SIT2 will identify and match the content in Email2. | ○ | ○ |
| SIT3 will identify and match the content in Email3. | ○ | ○ |

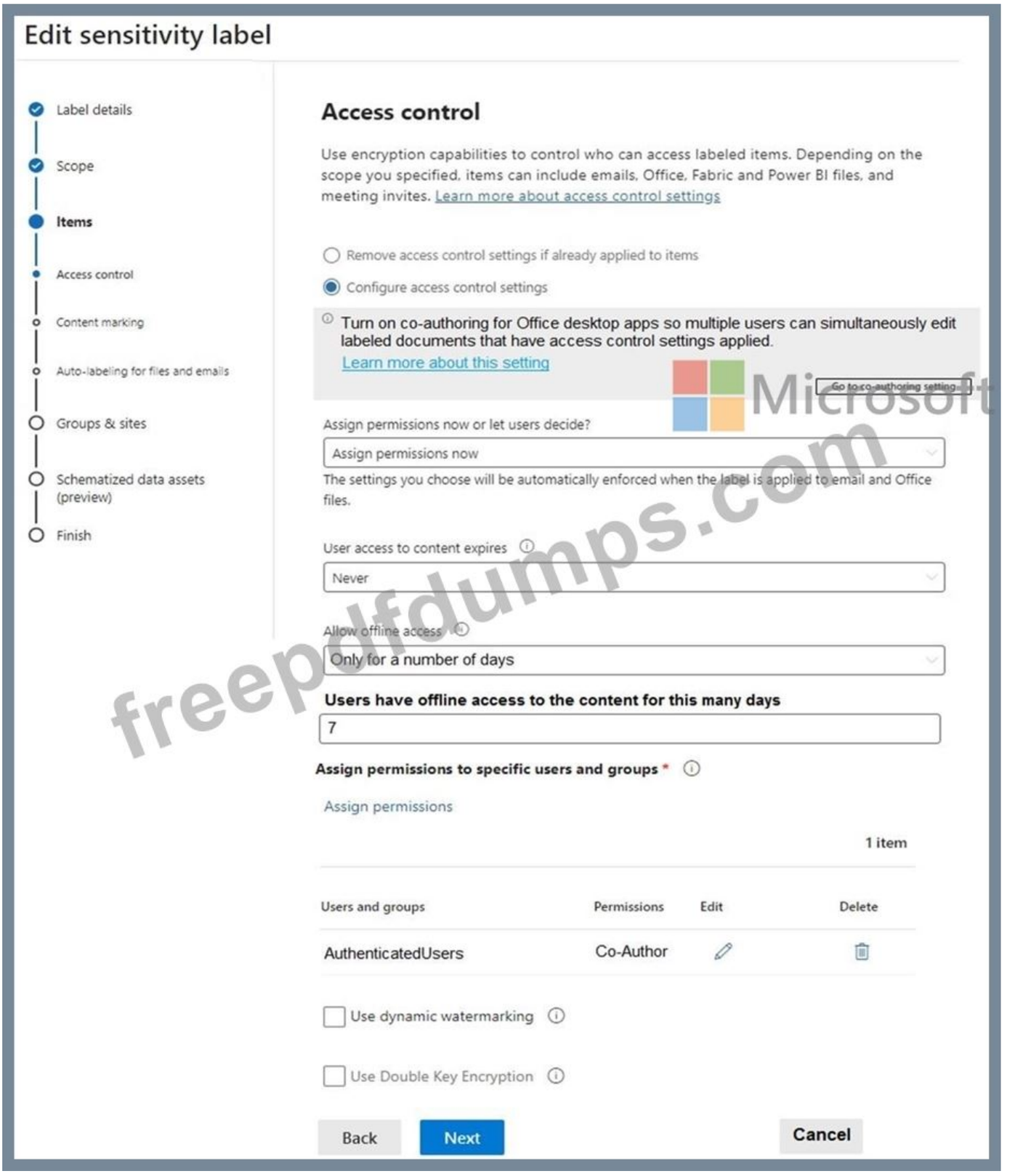


Explanation:
Box 1: Yes
Prd:1234 will match the regular expression of SIT1.
Box 2: Yes
111-111-1111 will match the exclusion of SIT2.
However, 123456789012 will match the regular expression of SIT2.
Box 3: No
The full credit card number is not inclued in Email3.
Note:
Sensitive information types (SIT) can use functions as primary elements for identifying sensitive items. For example, the Credit Card Number SIT uses the Func_credit_card function to detect credit card number.
Reference:
https://learn.microsoft.com/en-us/purview/sit-regex-validators-additional-checks#sensitive-information-type-regular-expression-validators
https://learn.microsoft.com/en-us/purview/sit-functions

**NEW QUESTION: 112**
Hotspot Question
You have a Microsoft 365 subscription that contains a sensitivity label named Contoso Confidential.
You publish Contoso Confidential to all users.
Contoso Confidential is configured as shown in the Configuration exhibit. (Click the Configuration tab.)




The Access control settings of Contoso Confidential are configured as shown in the Access control exhibit. (Click the Access control tab.)






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:**


**NEW QUESTION: 113**

You have a Microsoft 365 E5 subscription.

You plan to use Microsoft Purview insider risk management.

You need to create an insider risk management policy that will detect data theft from Microsoft SharePoint Online by users that submitted their resignation or are near their employment termination date.

What should you do first?

**A.** Configure a Physical badging connector.

**B.** Configure a HR data connector.

**C.** Configure Office indicators.

**D.** Onboard devices to Microsoft Defender for Endpoint.

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 114**

Hotspot Question

You have a Microsoft 365 E5 tenant that contains a trainable classifier named Classifier1.

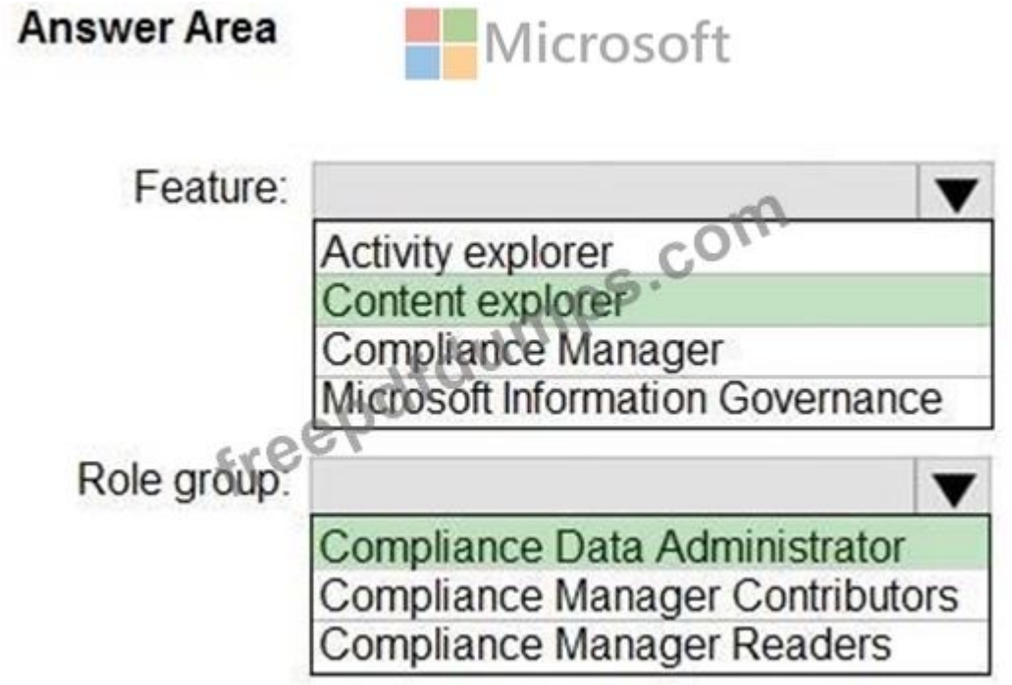
You need to increase the accuracy of Classifier1. The solution must use the principle of least privilege.

Which feature should you use and to which role group should you be added? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**


**Answer:**




Explanation:

Box 1: Content Explorer

Increase classifier accuracy

Classifiers, like sensitive information types (SIT) and trainable classifiers are used in various kinds of policies to identify sensitive information. Like most such models, sometimes they identify an item as being sensitive that isn't. Or, they may not identify an item as being sensitive when it actually is. These are called false positives and false negatives.

Box 2: Compliance data administrator

Permissions

In order to get access to the content explorer tab, an account must be assigned membership in any one of these roles or role groups.

Microsoft 365 role groups

Global administrator

Compliance administrator

Security administrator
*-> Compliance data administrator
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-increase-accuracy
https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-content-explorer

**NEW QUESTION: 115**
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 group.
**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 (LEAVE A REPLY)**
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: 116**
You have a Microsoft 365 E5 tenant that contains the policies shown in the following table.

| Name | Type | Retention period | Start the retention period based on | At the end of the retention period |
|---|---|---|---|---|
| Label1 | Label | 5 years | When items were created | Delete items automatically |
| Label2 | Retention | 7 years | When items were created | Delete items automatically |
| Labe3 | Retention | 10 years | When items were created | Do nothing |

A file named File1 has all the policies applied.
How long will File1 be retained?
**A.** File1 will be deleted automatically after 10 years.

**B.** File1 will be deleted automatically after five years.
**C.** File1 will be retained until the file is deleted manually.
**D.** File1 will be deleted automatically after seven years.
**Answer: A (LEAVE A REPLY)**
Retention always takes precedence over permanent deletion, with the longest retention period taking preference.
The delete action from a retention label always takes precedence over the delete action from a retention policy.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#the-principles-of-retention-or-what-takes-precedence

**NEW QUESTION: 117**
You have a Microsoft 365 E5 subscription that contains the adaptive scopes shown in the following table.

| Name | Type | Query |
|---|---|---|
| Scope1 | Users | `FirstName starts with User` |
| Scope2 | SharePoint Online sites | `SiteTitle starts with Site` |

You create the retention policies shown in the following table.

| Name | Type | Location |
|---|---|---|
| RPolicy1 | Adaptive | Scope1 |
| RPolicy2 | Adaptive | Scope2 |
| RPolicy3 | Static | Microsoft 365 groups |

Which retention policies support a preservation lock?
**A.** RPolicy2 only
**B.** RPolicy3 only
**C.** RPolicy1 and RPolicy2 only
**D.** RPolicy1 and RPolicy3 only
**E.** RPolicy1, RPolicy2, and RPolicy3
**Answer: (SHOW ANSWER)**
Use Preservation Lock to restrict changes to retention policies and retention label policies
Important Currently, adaptive policy scopes don't support Preservation Lock.
Reference:
https://learn.microsoft.com/en-us/purview/retention-preservation-lock