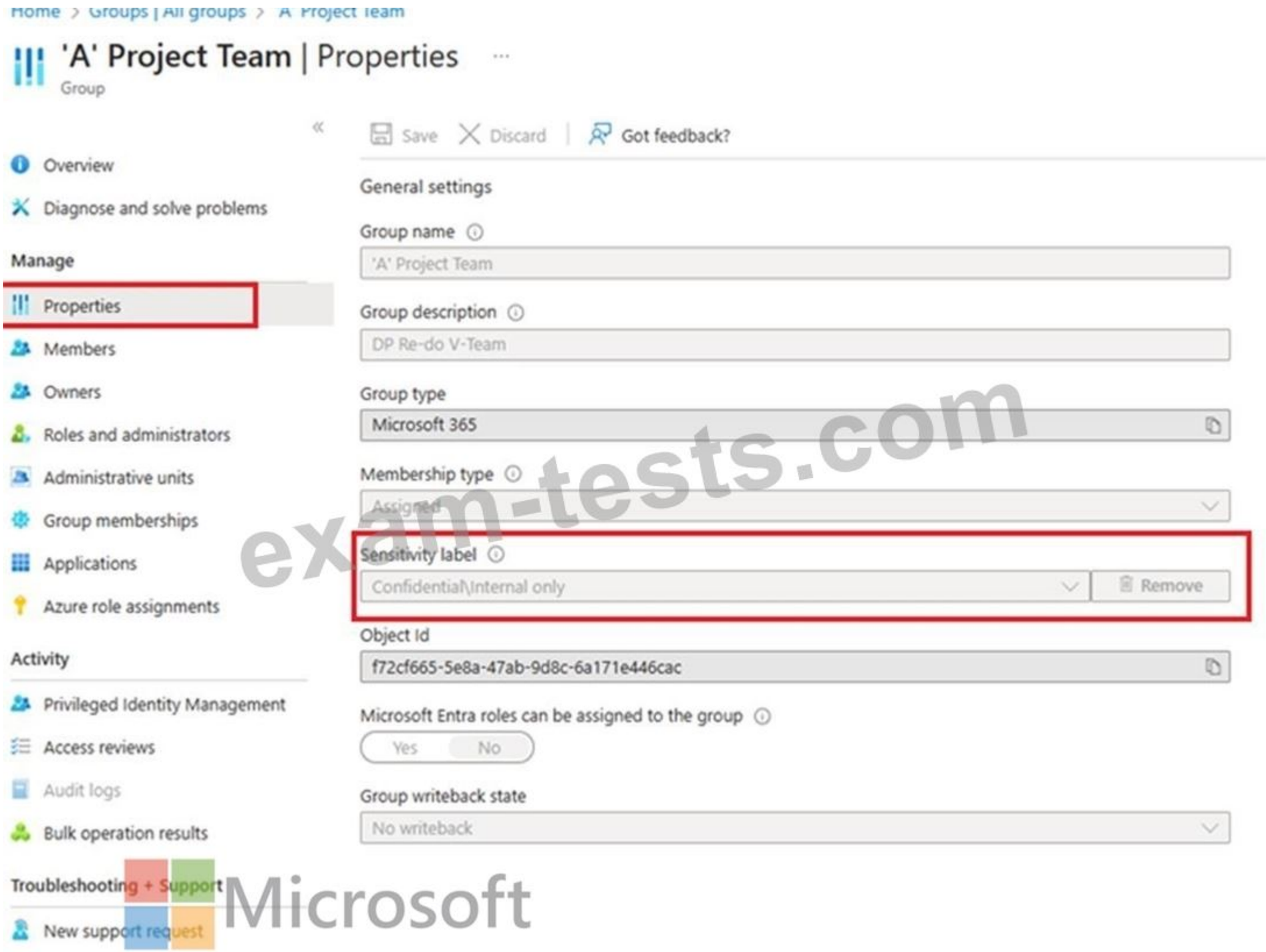
Microsoft.SC-401.v2026-07-25.q124

Exam Code:	SC-401
Exam Name:	Administering Information Security in Microsoft 365
Certification Provider:	Microsoft
Free Question Number:	124
Version:	v2026-07-25
# of views:	124
# of Questions views:	1240
https://www.exam-tests.com/SC-401-exam/Microsoft.SC-401.v2026-07-25.q124.html	

NEW QUESTION: 1
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: (SHOW ANSWER)
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: 2
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: 3
You have a Microsoft 365 subscription.
You identify the following data loss prevention (DLP) requirements:

* Send notifications to users if they attempt to send attachments that contain an EU Social Security Number (SSN) or Equivalent ID.
* Prevent any email messages that contain credit card numbers from being sent outside your organization.
* Block the external sharing of Microsoft OneDrive content that contains EU passport numbers.
* Send administrators email alerts if any rule matches occur.

What is the minimum number of DLP policies and rules you must create to meet the requirements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

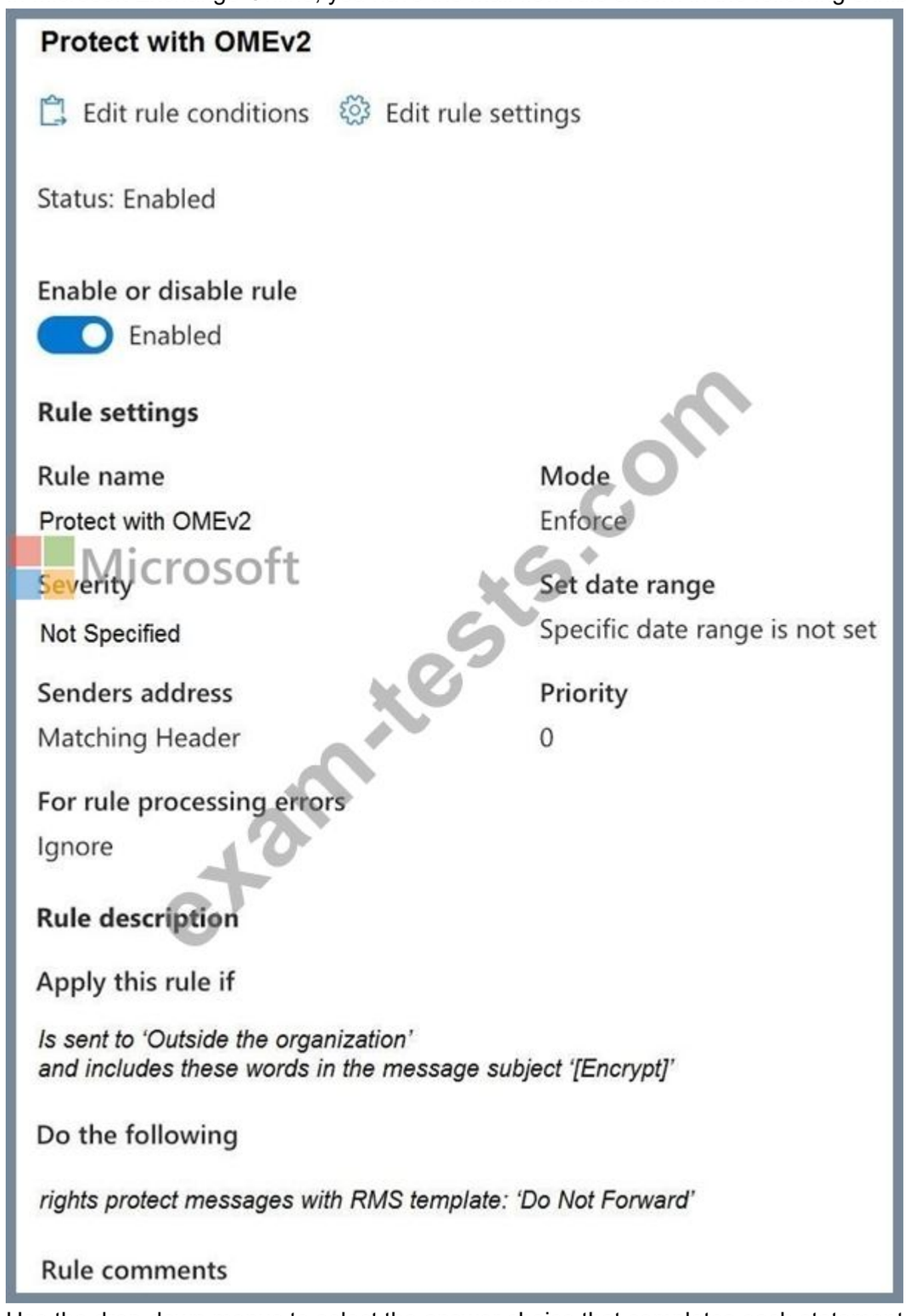
Explanation:

NEW QUESTION: 4

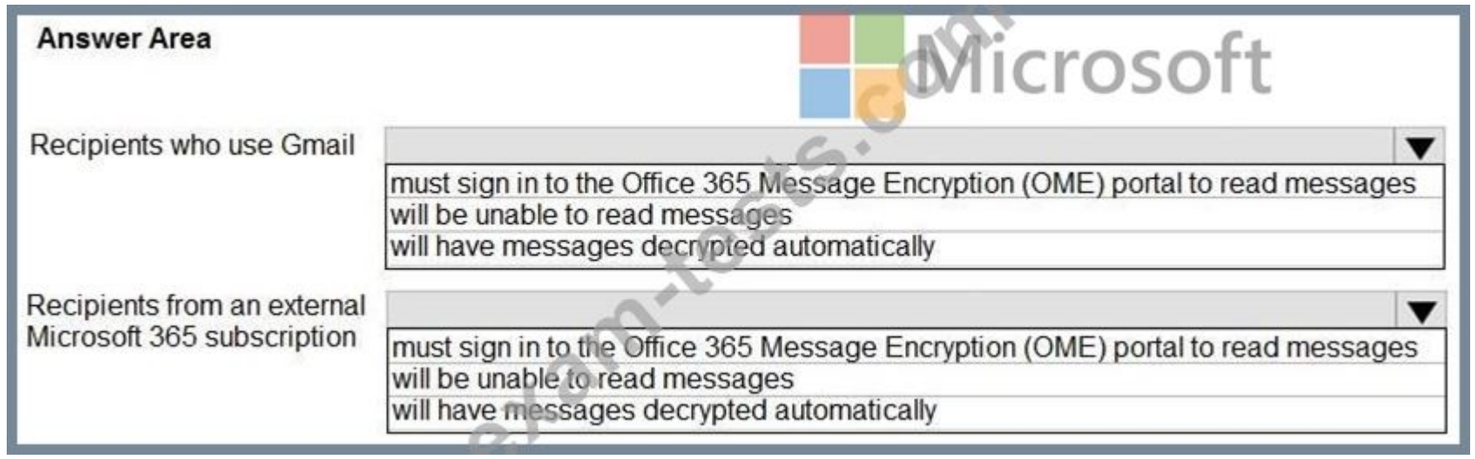
Hotspot Question

You have a Microsoft 365 E5 subscription.

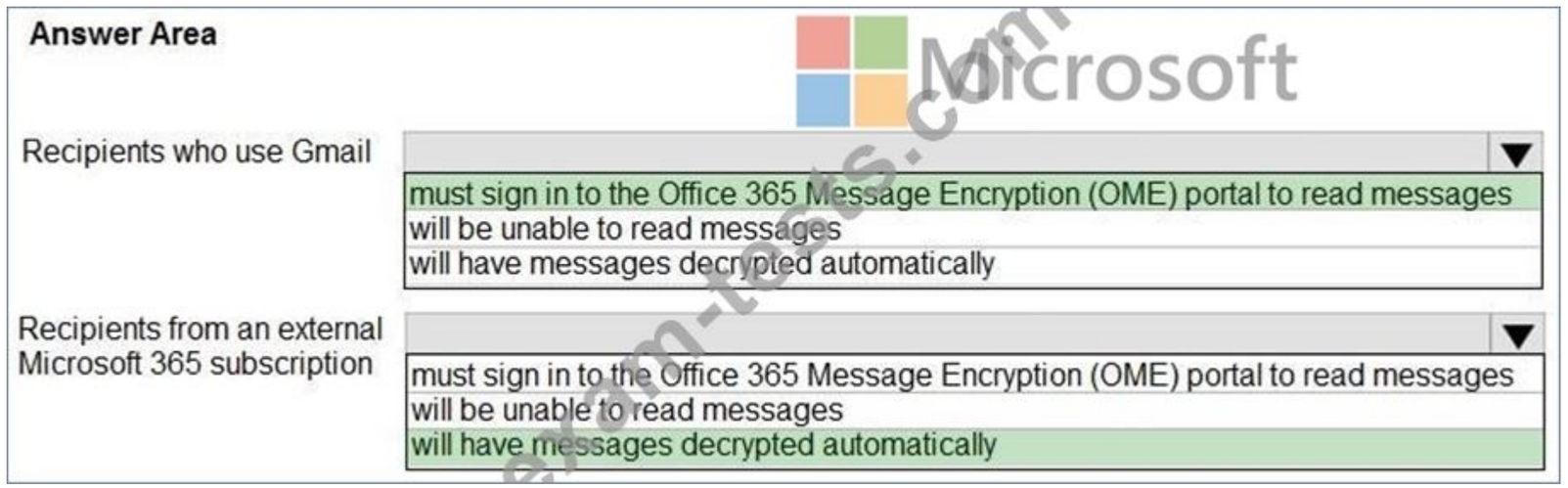
In Microsoft Exchange Online, you have the mail flow rule shown in the following exhibit.



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: 5

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You are creating an exact data match (EDM) classifier named EDM1.

For EDM1, you upload a schema file that contains the fields shown in the following table.

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

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

A. 1

B. 2

C. 3

D. 4

Answer: B (LEAVE A REPLY)

In Microsoft Purview Exact Data Match (EDM) classifiers, a primary element is a unique, identifying field used for data matching. EDM allows up to two primary elements per schema.

From the provided table, the Match mode indicates how data is analyzed:

- PP (EU Passport Number) Likely a primary element because it's unique.
- Name (All Full Names) Typically not a primary element as names are common.
- DateOfBirth (Single-token) Usually a secondary element, not unique.
- AccountNumber (Multi-token) Can be a primary element, as it's a unique identifier.
- Since EDM supports a maximum of two primary elements, the correct answer is 2.

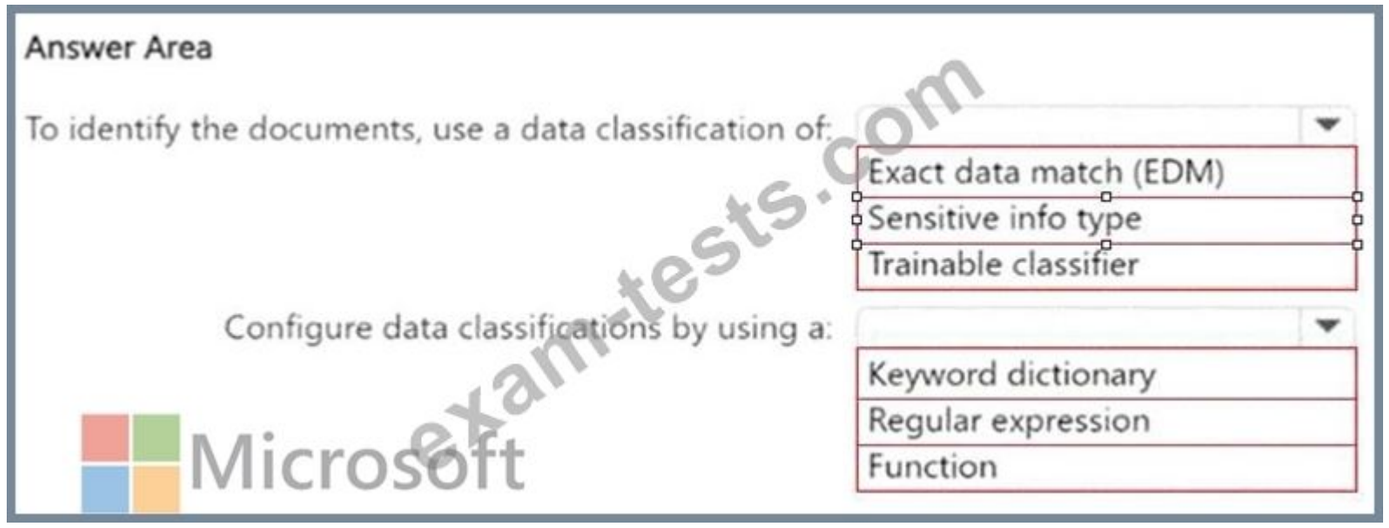
NEW QUESTION: 6

You have a Microsoft 365 E5 subscription.

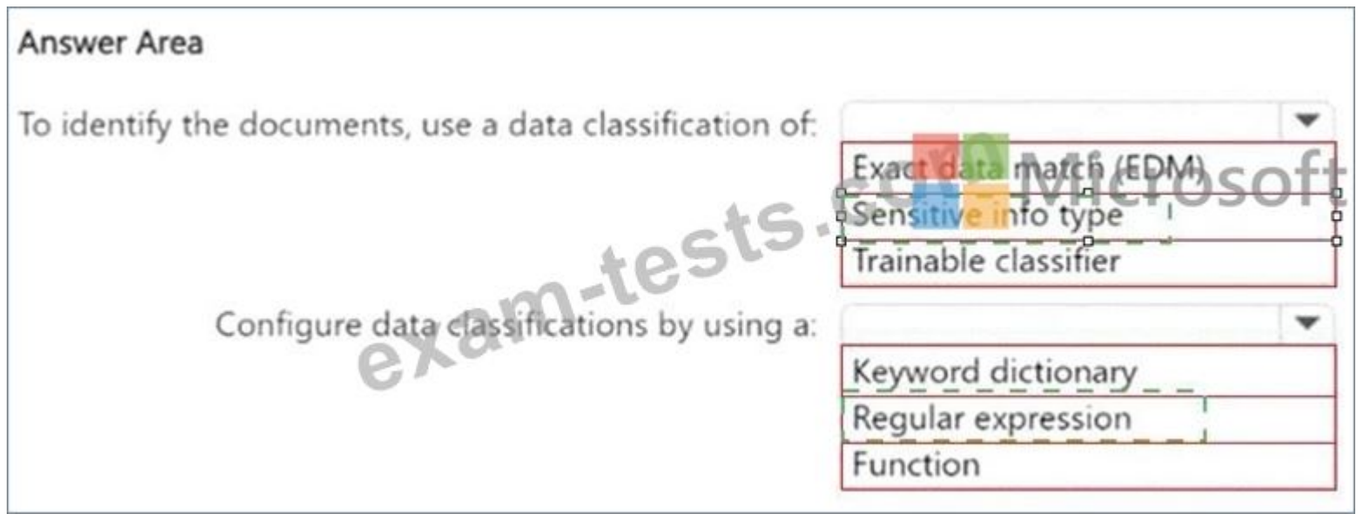
You need to identify documents that contain patent application numbers containing the letters PA followed by eight digits, for example, PA 12345678. The solution must minimize administrative effort.

What should you do? To answer, select the appropriate options in the answer area.

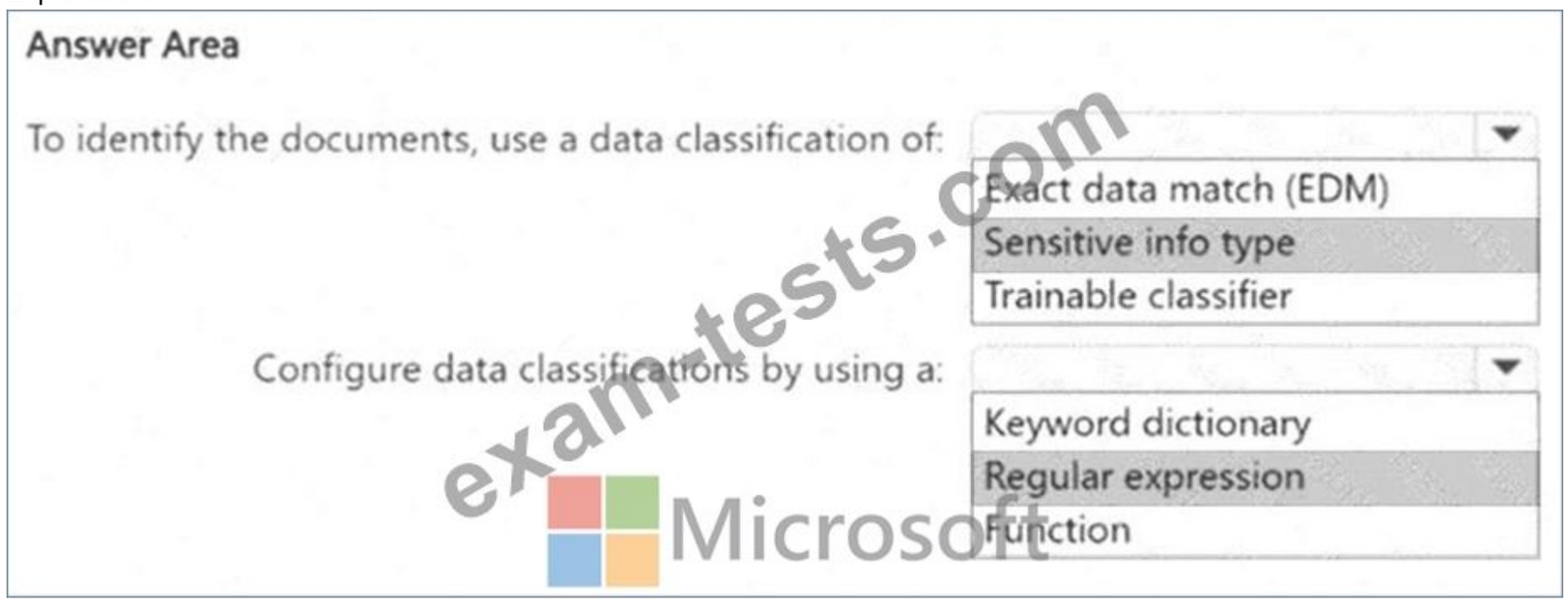
NOTE: Each correct selection is worth one point.



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: 7
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 Area

Answer:

Answer Area

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: 8
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: D (LEAVE A REPLY)
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: 9
HOTSPOT
You have a Microsoft 365 E5 subscription that contains two Microsoft 365 groups named Group1 and Group2. Both groups use the following resources:
A group mailbox
Microsoft Teams channel messages
A Microsoft SharePoint Online teams site
You create the objects shown in the following table.

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

To which resources will AutoApply1 and Retention1 be applied? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

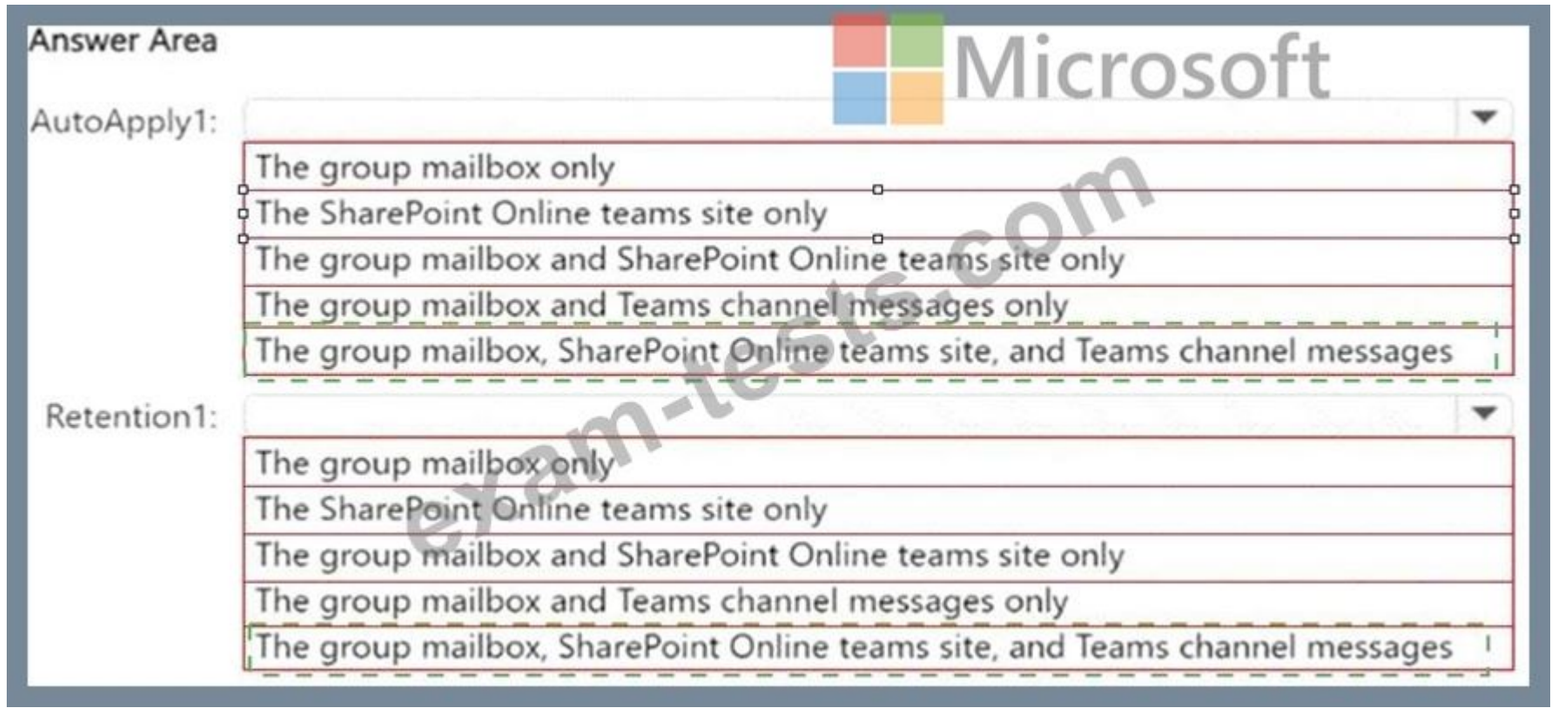
utoApply1:

- The group mailbox only
- The SharePoint Online teams site only
- The group mailbox and SharePoint Online teams site only
- The group mailbox and Teams channel messages only
- The group mailbox, SharePoint Online teams site, and Teams channel messages

Retention1:

- The group mailbox only
- The SharePoint Online teams site only
- The group mailbox and SharePoint Online teams site only
- The group mailbox and Teams channel messages only
- The group mailbox, SharePoint Online teams site, and Teams channel messages

Answer:



Explanation:

AutoApply1 is an auto-labeling policy that applies RLabel1 to Group1. Auto-labeling policies can apply retention labels across group mailboxes, SharePoint Online sites, and Teams channel messages if they are configured for group resources.

Retention1 is a retention policy applied to Group2. Retention policies for Microsoft 365 groups apply to all group resources, including group mailboxes, SharePoint Online teams sites, and Teams channel messages.
Since both AutoApply1 and Retention1 affect entire groups, they apply to all associated resources: group mailbox, SharePoint Online teams site, and Teams channel messages.

NEW QUESTION: 10
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: 11
You have a Microsoft 365 E5 subscription that contains a group named Group1.
You need to ensure that the members of Group1 can view and export alerts and cases in Microsoft Purview insider risk management. The solution must follow the principle of least privilege.
To which role group should you add to Group1?
A. Insider Risk Management Analysts
B. Insider Risk Management Admins
C. Insider Risk Management Approvers
D. Insider Risk Management Investigators

Answer: (SHOW ANSWER)
To meet the requirements using the principle of least privilege, you should add the group to the Insider Risk Management Analysts role group.
Insider Risk Management Analysts: This role group is specifically designed for users who need to perform initial triage on alerts, view alert telemetry, and export alert data. It grants fewer overall permissions than the full Insider Risk Management role group.
Incorrect:
Insider Risk Management Investigators: While this group can also view alerts and cases, it carries higher privileges. Investigators are meant to dig deeply into established cases, use the Content Explorer to view raw file content/messages, and escalate cases to eDiscovery.
By assigning the group to the Insider Risk Management Analysts role group, you ensure members can successfully perform viewing and exporting actions without granting unnecessary deeper data access.
Reference:
https://www.linkedin.com/pulse/understanding-microsoft-insider-risk-management-johana-koberov%C3%A1-yhldf

NEW QUESTION: 12
You have a Microsoft 365 E5 subscription that contains a trainable classifier named Trainable1.
You plan to create the items shown in the following table.

Name	Type
Label1	Sensitivity label
Label2	Retention label
Policy1	Retention label policy
DLP1	Data loss prevention (DLP) policy

Which items can use Trainable 1?
A. Label2 only
B. Label1 and Label2 only
C. Label1 and Policy1 only
D. Label2, Policy1, and DLP1 only
E. Label1, Label2, Policy1, and DLP1
Answer: D (LEAVE A REPLY)
A trainable classifier in Microsoft Purview is used to automatically identify and classify unstructured data based on content patterns. The classifier can be used in:
1. Retention Labels (Label2) # Supported
Trainable classifiers can be linked to retention labels to automatically classify and apply retention policies to documents.
2. Retention Label Policies (Policy1) # Supported
Retention label policies define how and where retention labels are applied, including automatically using trainable classifiers.
3. Data Loss Prevention (DLP) Policies (DLP1) # Supported
Trainable classifiers can be used in DLP policies to detect and protect sensitive content automatically.

NEW QUESTION: 13
You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3 and a file named Filetdocx.
You create a sensitivity label named Label1 as shown in the following exhibit.

You apply Label1 to File1.

For which users can Microsoft 365 Copilot summarize File1?

A. No user

B. User 1 only

C. User1 and User2 only

D. User1, User2, and User3

Answer: (SHOW ANSWER)

The sensitivity label Label1 assigns permissions (User1 = Co-Author, User2 = Reviewer, User3 = Viewer) and enables Double Key Encryption (DKE). Microsoft 365 Copilot can summarize content only when the service can access the file using the user's permissions. Content protected with Double Key Encryption is not accessible to Microsoft cloud services (including Copilot); as a result, Copilot cannot open or process DKE- protected files for any user, even if they can open the file themselves in Office apps.

Therefore, no user can use Microsoft 365 Copilot to summarize File1.

Reference: Microsoft Purview Double Key Encryption-service access limitations for Microsoft cloud services, including Copilot and search indexing.

NEW QUESTION: 14

You have a Microsoft SharePoint Online site named Site1 that has the users shown in the following table.

Name	Role
User1	Owner
User2	Member

You create the retention labels shown in the following table.

Name	Retention period	Retention action	Based on
Retention1	4 years	Retain only	When a file was labeled
Retention2	2 years	Retain and delete	When a file was labeled

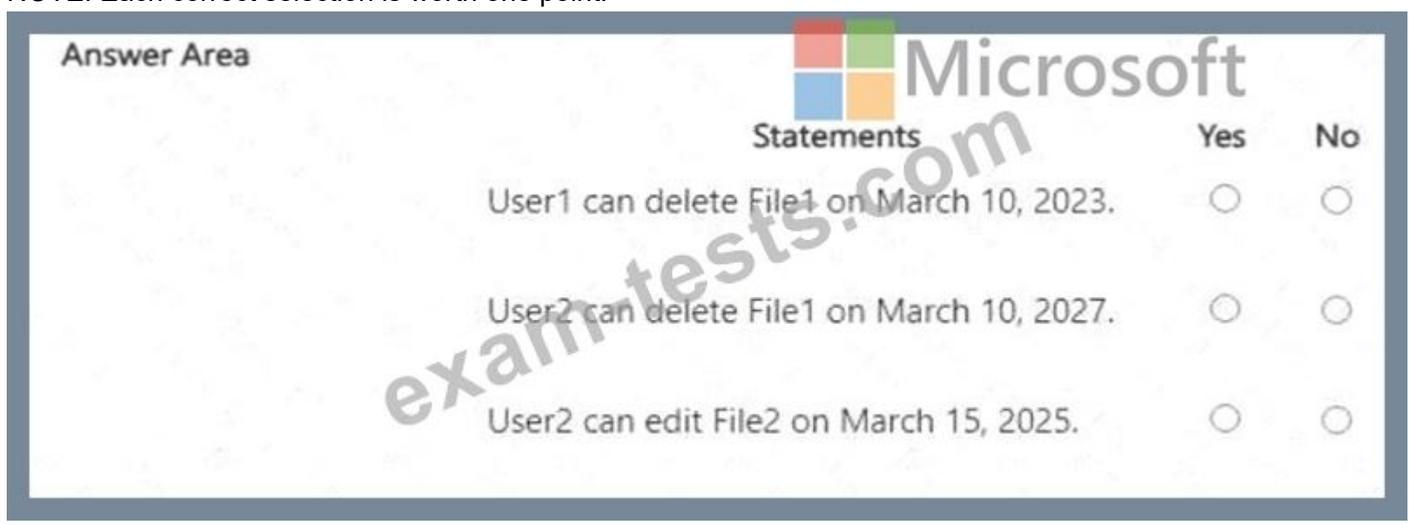
You publish the retention labels to Site1.

On March 1,2023, you assign the retention labels to the files shown in the following table.

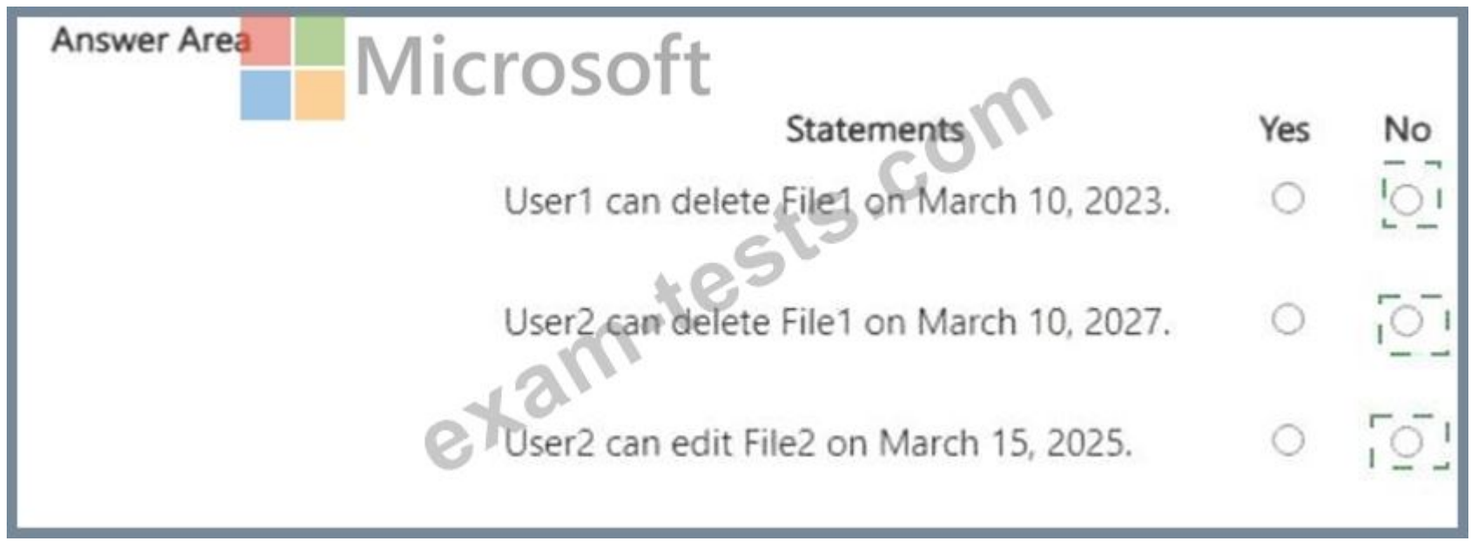
Name	Modified by	Retention label
File1	User1	Retention1
File2	User1	Retention2

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:

User1 can delete File1 on March 10, 2023.
No - File1 has Retention1 applied, which retains it for 4 years with a "Retain only" action. This means it cannot be deleted during the retention period, which ends on March 1, 2027.
User2 can delete File1 on March 10, 2027.
No - User2 is a Member and does not have the Owner role, which is required to delete files under retention policies during the retention period. Additionally, the "Retain only" action prevents deletion until the retention period ends on March 1, 2027.
User2 can edit File2 on March 15, 2025.
No - File2 has Retention2 applied, which retains it for 2 years with a "Retain and delete" action. This means the file is protected from edits or deletions during the retention period, which ends on March 1, 2025. Since March 15, 2025, is after the retention period, the file would be eligible for deletion, but the question specifies editing, which is restricted during the retention period.

NEW QUESTION: 15
You have a Microsoft 365 E5 subscription that uses Microsoft Purview.
You need to perform a content search for email messages that meet the following requirements:
* Are delivered to both user1@contoso.com and user2@contoso.com
* Are sent from a user account that has a name that starts with the word Compliance How should you complete the query in the KQL editor? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

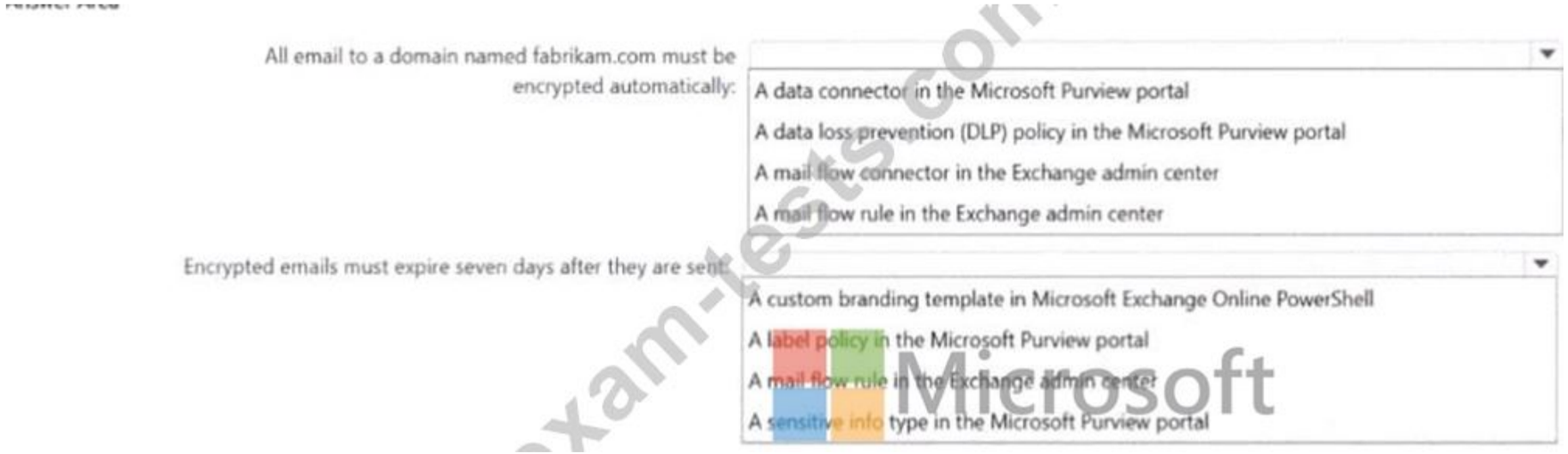
NEW QUESTION: 16
You have a Microsoft J65 subscription linked to a Microsoft Entra tenant that contains a user named User1.
You need to grant User1 permission to search Microsoft 365 audit logs. The solution must use the principle of least privilege. Which role should you assign to User1?
A. the Compliance Management role in the Exchange admin center
B. the Security Reader role in the Microsoft Entra admin center
C. the View Only Audit Logs role in the Exchange admin center
D. the Reviewer role in the Microsoft Purview portal
Answer: C (LEAVE A REPLY)

NEW QUESTION: 17
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.

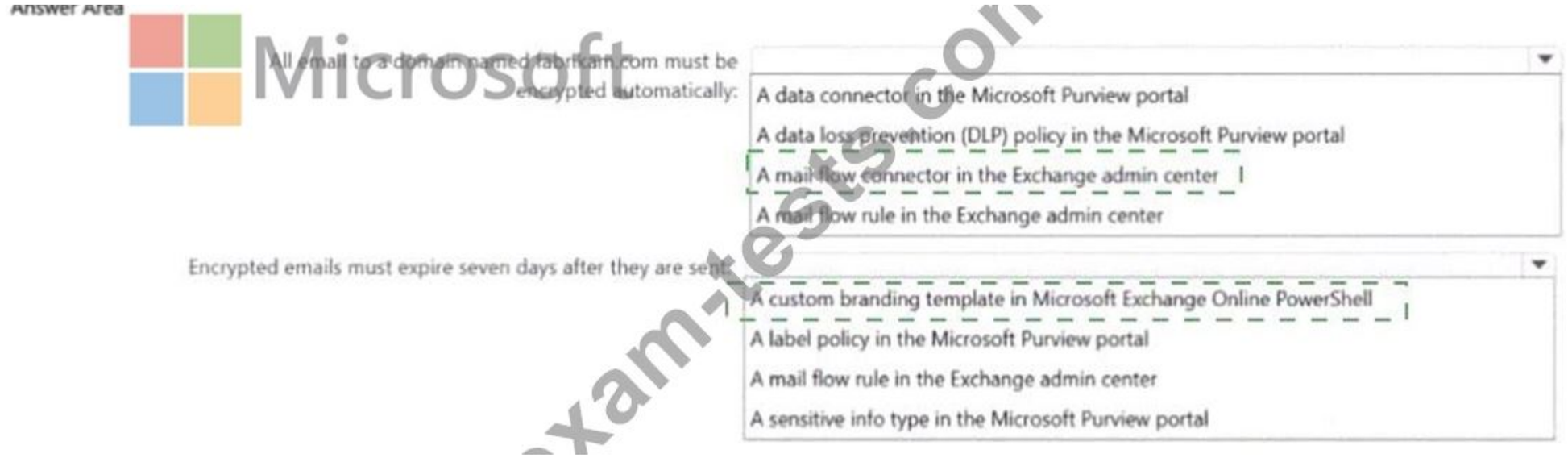
C From the Microsoft Entra admin center create a User risk policy
D From the Microsoft Purview portal create a priority user group
Answer: B (LEAVE A REPLY)
To implement insider risk management for users managing sensitive project data while minimizing the impact on other users and reducing administrative 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: 18
You have a Microsoft 365 tenant.
You have a database that stores customer details. Each customer has a unique 13-digit identifier that consists of a fixed pattern of numbers and letters.
You need to implement a data loss prevention (DLP) solution that meets the following requirements:
- Email messages that contain a single customer identifier can be sent
outside your company.
- Email messages that contain two or more customer identifiers must be
approved by the company's data privacy team.
Which two components should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. a sensitivity label
B. a sensitive information type
C. a DLP policy
D. a retention label
E. a mail flow rule
Answer: (SHOW ANSWER)
You need to define a custom sensitive information type that recognizes the unique 13-digit identifier format for customer records. Microsoft Purview DLP policies use these types to identify and protect sensitive data.
A Data Loss Prevention (DLP) policy is required to enforce the rules. It will allow emails with a single identifier but trigger an approval workflow when two or more identifiers are detected.

NEW QUESTION: 19
You are implementing Microsoft Purview Advanced Message Encryption for a Microsoft 365 tenant named contoso.com You need to meet the following requirements:
* All email to a domain named (abrikam.com must be encrypted automatically.
* Encrypted emails must expire seven days after they are sent
What should you configure for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Requirement 1 - Encrypt all email to fabrikam.com automatically

To force encryption for mail sent to a specific external domain (fabrikam.com):

You configure a mail flow rule (transport rule) in the Exchange admin center (EAC).

This rule can apply Office Message Encryption (OME) automatically when messages match conditions such as recipient domain.

Reference: Define mail flow rules to encrypt email messages

Correct choice: A mail flow rule in the Exchange admin center

Requirement 2 - Encrypted emails must expire after 7 days

To configure expiration and access control over encrypted emails:

You use Microsoft Purview sensitivity labels with encryption settings.

A label policy in the Purview portal can enforce encryption, set access rights, and define expiration (e.g., revoke access after 7 days).

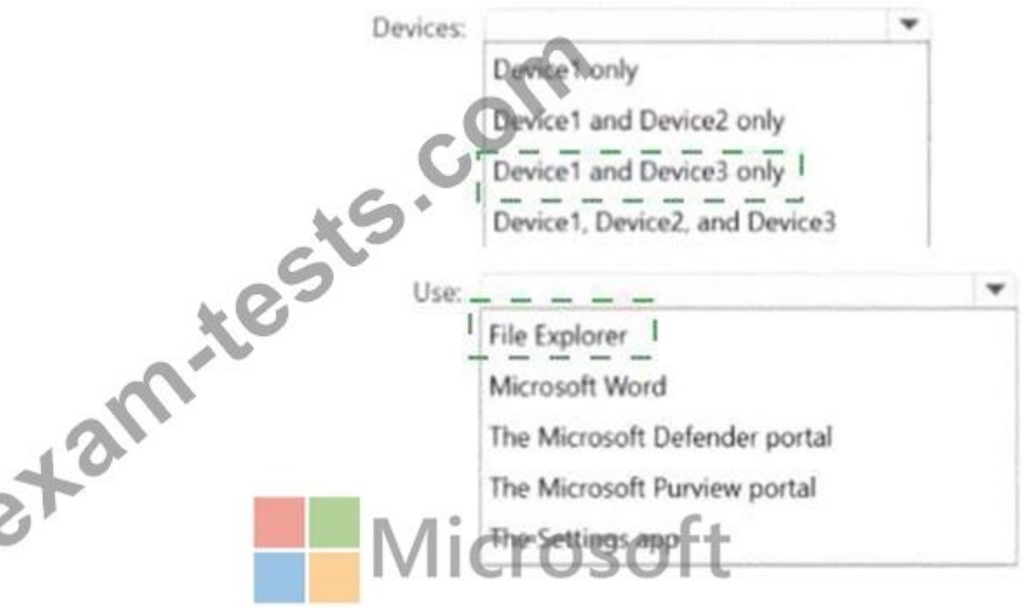
Sensitive info types or mail flow rules cannot configure expiration.
Reference: Configure encryption settings for sensitivity labels
Correct choice: A label policy in the Microsoft Purview portal

NEW QUESTION: 20
You have a Microsoft 36S ES subscription that contains the devices shown in the following table.

Name	Platform	Chipset
Device1	Windows 11	x64
Device2	Windows 11	ARM64
Device3	Windows 10	x86

You publish Microsoft Purview Information Protection sensitivity labels.
You plan to deploy the information protection client to the devices. The solution must ensure that the labels can be applied to sensitive images and documents On which devices can you install the information protection client, and what should users use to apply labels?
To answer, select the appropriate options in the answer area.

Answer:



Explanation:

NEW QUESTION: 21

You implement Microsoft 365 Endpoint data loss prevention (Endpoint DIP).

You have computers that run Windows 11 and have Microsoft 365 Apps instated. The computers are joined to a Microsoft Entra tenant You need to ensure that Endpoint DIP policies can protect content on the computers.

Solution: You deploy the Endpoint DLP configuration package to the computers.

Does this meet the goal?

A. No

B. Yes

Answer: B (LEAVE A REPLY)

NEW QUESTION: 22

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: B (LEAVE A REPLY)
To create custom trainable classifiers in Microsoft Purview, the user must have rights in the compliance portal. The Compliance Administrator role provides the necessary permissions to create and manage trainable classifiers. Security roles focus on threat management, and Global Administrator is excessive (not least privilege).
Reference: Trainable classifiers in Microsoft Purview

NEW QUESTION: 23
You have a Microsoft 365 E5 subscription that uses Microsoft Teams.
You plan to implement sensitivity labels.
You need to ensure that you can view and apply sensitivity labels to new Microsoft Teams sites.
What should you do first?
A. Create a new sensitivity label scoped to Groups & sites.
B. Configure the EnableMIPLabelssetting in Microsoft Entra ID.
C. Run the Execute-AzureAdLabelSynccmdlet.
D. Run the Set-SPOSitecmdlet.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
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: 25

You have a Microsoft 365 E5 subscription that contains a Microsoft Teams channel named Channel1.

Channel1 contains research and development documents.

You plan to implement Microsoft 365 Copilot for the subscription.

You need to prevent the contents of files stored in Channel1 from being included in answers generated by Copilot and shown to unauthorized users.

What should you use?
A. data loss prevention (DLP)
B. Microsoft Purview insider risk management
C. Microsoft Purview Information Barriers
D. sensitivity labels
Answer: D (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: 26
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 onboard the computers to Microsoft Defender for Endpoint.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
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: 27
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-MailboxFolderPermission -Identity "User1" -User User1@contoso.com -AccessRights Owner command.
Does that meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
The Set-MailboxFolderPermission -Identity "User1" -User User1@contoso.com -AccessRights Owner command is incorrect. This assigns folder permissions but does not enable auditing. It does not track who accessed the mailbox or deleted emails.

NEW QUESTION: 28
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. Information Barriers
C. Insider Risk Management
D. Information Protection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
You have a Microsoft 365 subscription that has a retention label named Retention1. The subscription contains the files shown in the following table.

Name	Stored in	Number of sensitive information types (SITs)		
		IP address	SWIFT code	Shared access signature (SAS)
File1	Microsoft Exchange Online	1	2	4
File2	Microsoft SharePoint Online	3	5	1
File3	Microsoft OneDrive	3	3	2

You create an auto-labeling policy named Policy1 that will automatically apply Retention1 as shown in the Auto-labeling policy Exhibit. (Click the Auto-labeling policy tab.) You configure Policy1 to apply Retention1 as shown in the Locations exhibit. (Click the Locations 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
Retention1 is applied to File1.	○	○
Retention1 is applied to File2.	○	○
Retention1 is applied to File3.	○	○

Answer:

Answer Area

Statements	Yes	No
Retention1 is applied to File1.	○	○
Retention1 is applied to File2.	○	○
Retention1 is applied to File3.	○	○

Explanation:

NEW QUESTION: 30

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 Area

Statements	Yes	No
User1 can access File1 on Site1.	○	○
User2 can access File1 on Site1.	○	○
Admin1 can access File1 on Site1.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can access File1 on Site1.	○	●
User2 can access File1 on Site1.	●	○
Admin1 can access File1 on Site1.	●	○

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: 31
You need to enable sensitivity labels for containers in Microsoft Purview and synchronize these labels with Microsoft Entra ID. The labels will be used to configure protection settings for groups and sites, as well as to ensure privacy and external user access settings.
What should you do?
A. Connect to Microsoft Security & Compliance PowerShell and run the Execute-AzureAdLabelSync command right
B. Enable sensitivity labels in Microsoft Entra ID without synchronizing them
C. Apply sensitivity labels to containers in Microsoft Teams
D. Use sensitivity labels to configure Office 365 apps settings

Answer: A (LEAVE A REPLY)
Sensitivity labels for containers must be synchronized to Microsoft Entra ID using the Execute- AzureAdLabelSync command after enabling them. This step ensures that labels can be used to protect groups and sites, as specified in the sensitivity labeling configuration.
Reference:
https://learn.microsoft.com/en-us/purview/sensitivity-labels-teams-groups-sites

NEW QUESTION: 32
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 activity policy
B. a sensitivity label
C. a file policy
D. an insider risk policy
Answer: (SHOW ANSWER)
Activity Policy (MCAS): Monitors and alerts on specific user actions such as uploading files, downloads, or logins to cloud apps.
Perfect for detecting "upload to third-party storage".
Sensitivity label: Used for classifying and protecting content, not generating alerts.
File policy (MCAS): Inspects and governs files already stored in sanctioned apps, not upload activity.
Insider risk policy: Focuses on risky behavior like data exfiltration or security violations, not direct activity alerts in cloud apps.
Answer: A. an activity policy
Reference: Defender for Cloud Apps activity policies

NEW QUESTION: 33
HOTSPOT
You have a Microsoft SharePoint Online site that contains the following files.

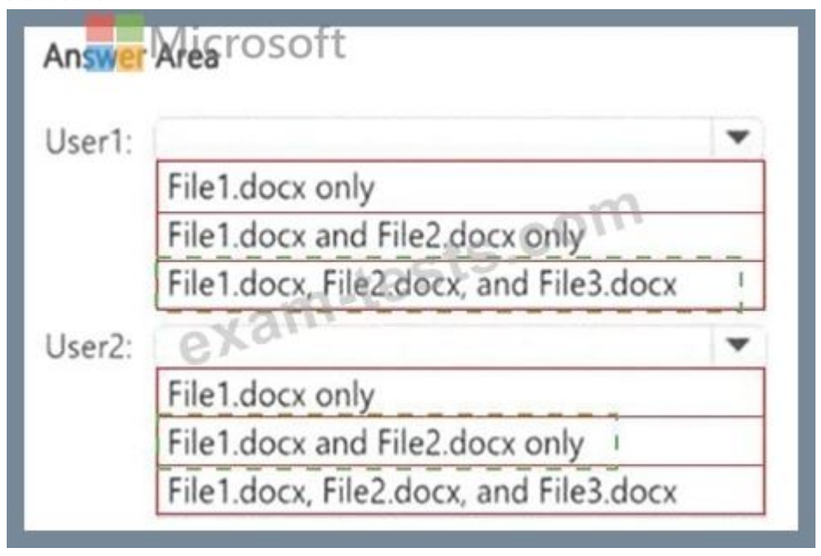
Name	Modified by	Data loss prevention (DLP) action
File1.docx	Manager1	*None*
File2.docx	Manager1	Matched by DLP
File3.docx	Manager1	Blocked by DLP

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

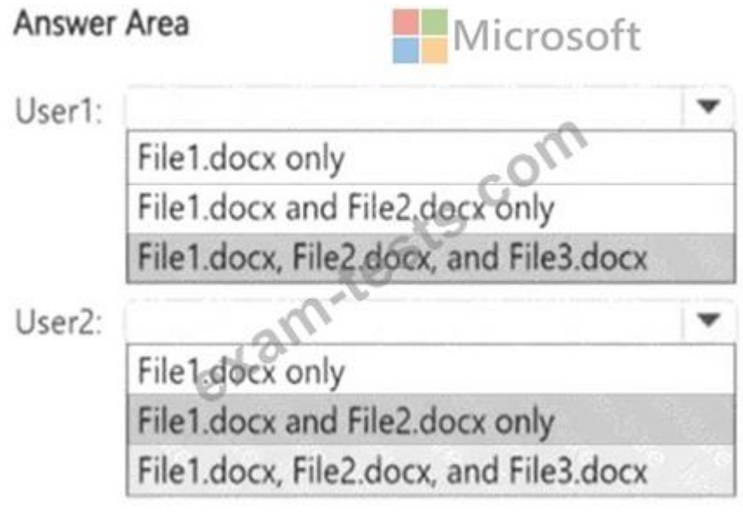
Name	Role
User1	Site owner
User2	Site member

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

Answer:



Explanation:



Let's break it down:
File1.docx # DLP action = None
No DLP restrictions, so it is fully accessible to both User1 (owner) and User2 (member).
File2.docx # DLP action = Matched by DLP
"Matched" means the DLP policy detected sensitive content but has not blocked access. Instead, it may generate an alert or policy tip.
Both User1 and User2 can still open this file.
File3.docx # DLP action = Blocked by DLP
"Blocked" means the DLP policy actively restricts access or sharing of the file.
User2 (member) cannot open this file.
However, User1 (site owner) can open it because site collection admins and owners always retain full control over content, even if a DLP rule applies.
Ref: Microsoft Purview DLP policy tips and enforcement
DLP policies do not prevent SharePoint/OneDrive site collection admins (owners) from accessing content.
Final Answer Table:
User1 (Site Owner): File1.docx, File2.docx, File3.docx
User2 (Site Member): File1.docx, File2.docx

NEW QUESTION: 34
You have a Microsoft 365 IS subscription that contains the resources shown in the following table.

Name	Type	Member of
User1	User	None
User2	User	Group1
Group1	Group	None

The subscription contains a Windows 11 device named Device 1 and has the Microsoft Purview Information Protection client installed. Device i contains the resources shown in the following table.

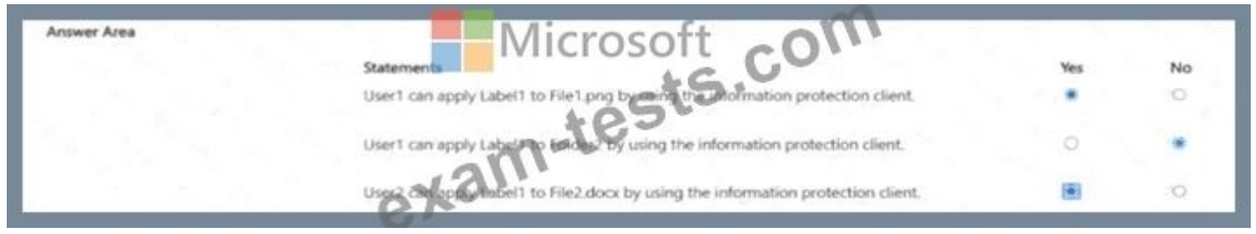
Name	Type	Path
File1.png	File	C:\Temp
File2.docx	File	D:\Folder1
Folder2	Folder	D:\

You publish a sensitivity label named Label1 to User1 and Group1.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
Answer Area

Statements	Yes	No
User1 can apply Label1 to File1.png by using the information protection client.	○	○
User1 can apply Label1 to Folder2 by using the information protection client.	○	○
User2 can apply Label1 to File2.docx by using the information protection client.	○	○

Answer:

Explanation:



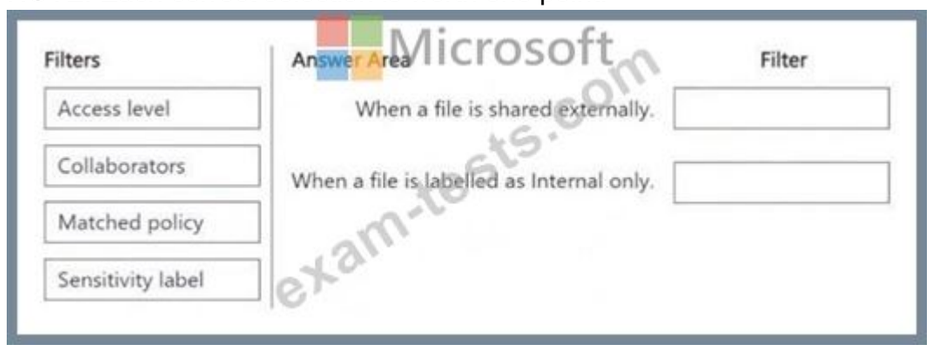
Step 1 - Label publishing and scope
The sensitivity label Label1 is published to User1 and Group1.
User1 # Directly included in label publishing.
User2 # Member of Group1, so also included indirectly.
This means both User1 and User2 are eligible to use Label1.
Step 2 - File vs Folder labeling with the Information Protection client The Microsoft Purview Information Protection (AIP unified labeling) client can apply labels to files such as .docx, .png, .pdf, etc.
It cannot label folders directly. Labels are applied to items (files and emails), not folders.
Reference: Apply sensitivity labels using the AIP client
Step 3 - Analyze each statement
User1 can apply Label1 to File1.png
File1.png is a file type supported by the Information Protection client.
User1 has Label1 published directly.
answer: Yes
User1 can apply Label1 to Folder2
Sensitivity labels cannot be applied to folders in File Explorer.
answer: No
User2 can apply Label1 to File2.docx
File2.docx is a supported file type (Word document).
User2 is a member of Group1, and Label1 is published to Group1.
answer: Yes

NEW QUESTION: 35
Drag and Drop Question
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You plan to deploy a Defender for Cloud Apps file policy that will be triggered when the following conditions are met:
- A file is shared externally.

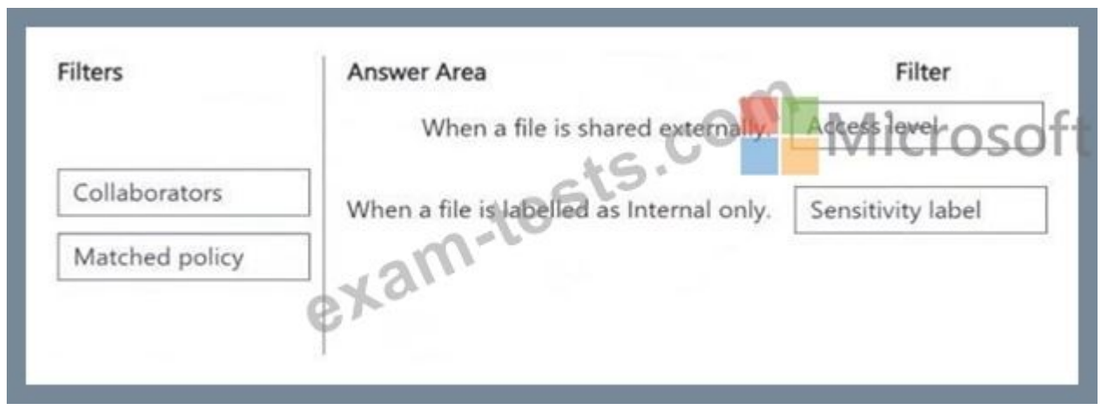
- A file is labeled as internal only.

Which filter should you use for each condition? To answer, drag the appropriate filters to the correct conditions. Each filter may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

The "Access level" filter in Microsoft Defender for Cloud Apps helps identify how a file is shared, including whether it is shared externally outside the organization.

The "Sensitivity label" filter is used to track files that have been classified with specific Microsoft Purview sensitivity labels, such as Internal only, ensuring that files with internal classifications are properly monitored and protected.

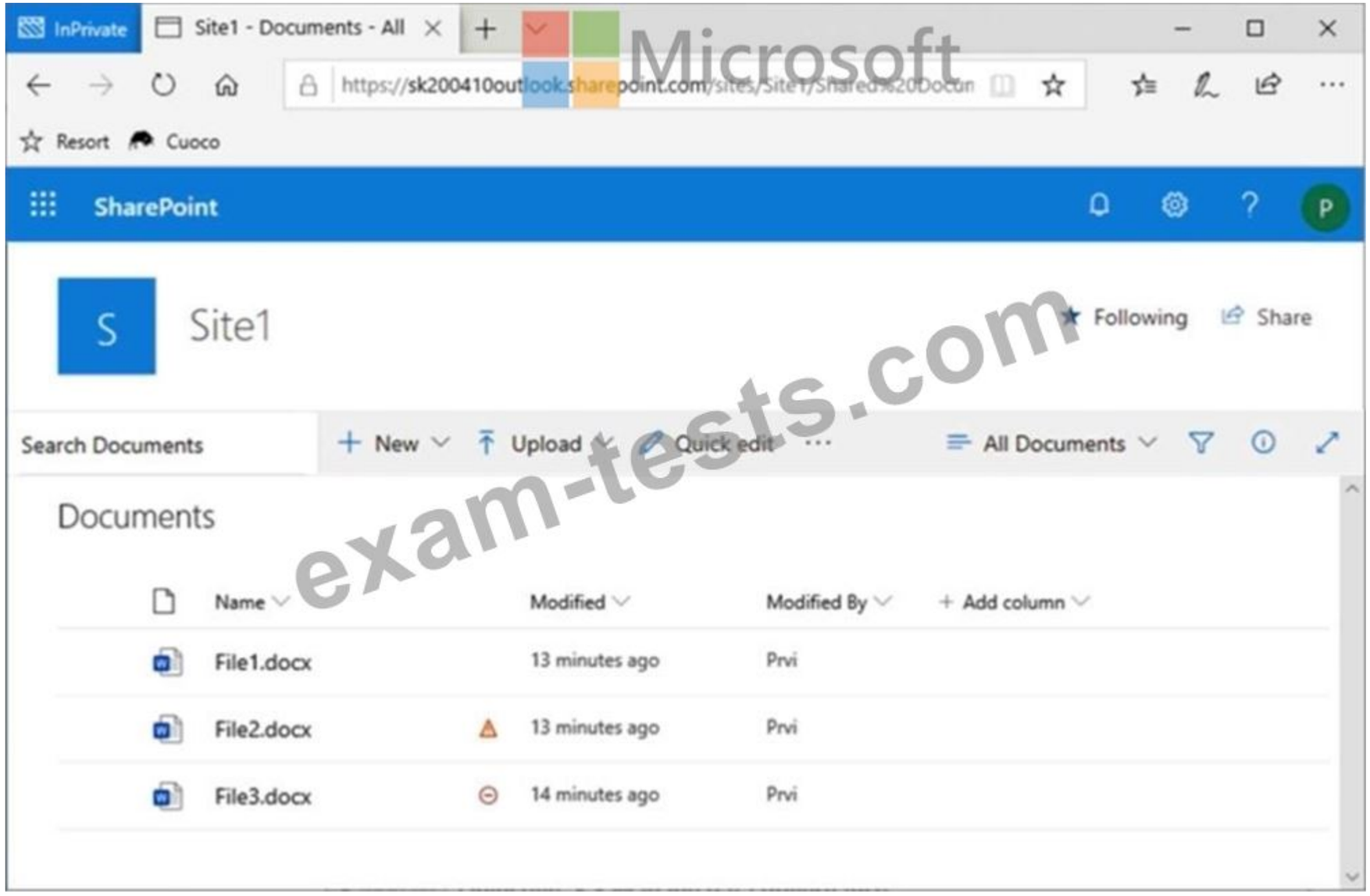
The "Collaborators" filter tracks users who have access but does not indicate external sharing.

The "Matched policy" filter identifies files based on predefined policies but does not directly filter for external sharing or sensitivity labels.

NEW QUESTION: 36

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

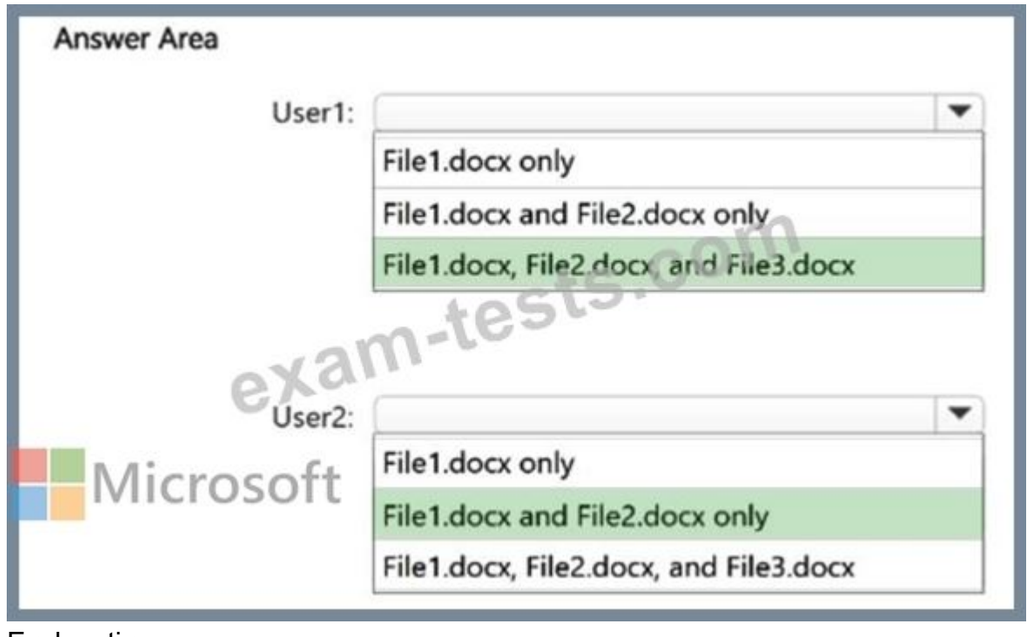
User1:

- 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:

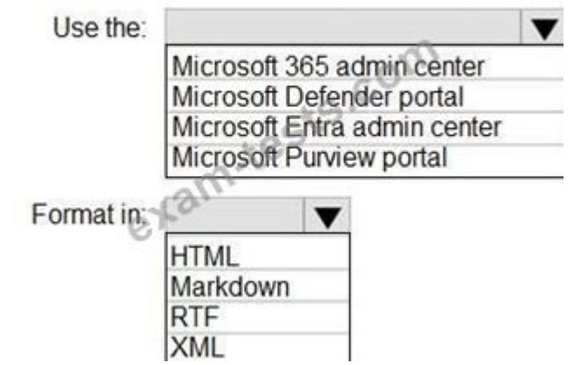
This item is protected by a policy in your organization. It can't be shared with people outside your organization.
Issues
Item contains the following sensitive information: Etc.
Box 2: File1.docx and File2.docx only
User is member and cannot access File3.
Reference:
https://answers.microsoft.com/en-us/msteams/forum/all/a-red-circle-with-a-minus-sign-after-file-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

NEW QUESTION: 37
You have a Microsoft 36S ES subscription that contains a Windows 11 device named Device 1 and three users named User 1. User2. and User3.
You plan to deploy Azure Information Protection (AIP) and the Microsoft Purview Information Protection client to Device 1.
You need to ensure that the users can perform the following actions on Device1 as part of the planned deployment
* User 1 will test the functionality of the client.
* User2 will install and configure the Microsoft Rights Management connector.
* User3 will be configured as the service account for the information protection scanner.
The solution must maximize the security of the sign-in process for the users What should you do?
A. Exclude User2 and User3 from multifactor authentication (MfA).
B. Enable User? and Usex3 for passwordless authentication.
C. Exclude User1 and User? from multifactor authentication (Mf A}
D. Enable User1. User I and User 3 for passkey (FIDO2) authentication
Answer: D (LEAVE A REPLY)
Goal: maximize sign#in security for users who will test the AIP client (User1), install/configure the Microsoft Rights Management connector (User2), and act as the AIP scanner service account (User3).
Excluding users from MFA lowers security and is not recommended.
Passwordless with FIDO2 security keys (passkeys) provides strong phishing#resistant authentication and is fully supported for Azure AD sign#ins, including admin tasks and service scenarios that require interactive sign#in during setup.
Therefore, enabling all three for FIDO2 passkey authentication best meets the "maximize security" requirement.
References:
Microsoft Entra ID - Passwordless authentication with FIDO2 security keys
https://learn.microsoft.com/azure/active-directory/authentication/concept-authentication-passwordless

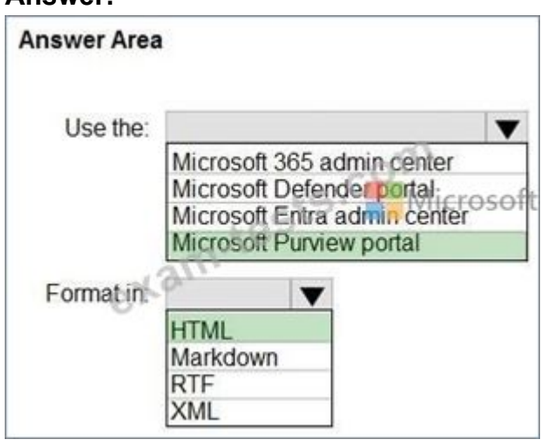
NEW QUESTION: 38
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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: (SHOW ANSWER)
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: 39
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: 40
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:

NEW QUESTION: 41
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: B (LEAVE A REPLY)
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: 42
You have 4 Microsoft 565 E5 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2. You plan to configure a retention label named Labe1 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. Start a disposition review
C. Change the label
D. Run a Power Automate flow
Answer: D (LEAVE A REPLY)
You want files in Site1 that are labeled with Label1 to automatically move to Site2 two years after creation.
In Microsoft Purview Retention Labels, under "Choose what happens after the retention period", the available options are:
Deactivate retention settings - Ends retention but does not move files.
Start a disposition review - Sends items to reviewers for approval (manual process, not auto-move).
Change the label - Applies a new retention label (but does not move files to another site).
Run a Power Automate flow - Executes an automated workflow such as moving the file to another SharePoint library or site, notifying users, or applying custom business processes.
Since the requirement is automatic movement of files from Site1 to Site2 after 2 years, the only valid choice is Run a Power Automate flow.
Reference:
Microsoft Learn: Actions after a retention period for retention labels
Quote: "For retention labels, you can choose to trigger a Power Automate flow when the retention period

NEW QUESTION: 43
You have a Microsoft 365 E5 subscription.
A security manager receives an email message every time a data loss prevention (DLP) policy match occurs.
You need to limit alert notifications to actionable DLP events.
What should you do?
A. From the Microsoft Purview portal, modify the Policy Tips settings of a DLP policy.
B. From the Microsoft Defender portal, apply a filter to the alerts.
C. From the Microsoft Purview portal, modify the matched activities threshold of an alert policy.
D. From the Microsoft Purview portal, modify the User overrides settings of a DLP policy.
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

NEW QUESTION: 44

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.
You need to meet the technical requirements for the creation of the sensitivity labels. To which user or users must you assign the Information Protection Admin role group?
A. Admin1 only
B. Admin1 and Admin4 only
C. Admin1 and Admin5 only
D. Admin1, Admin2, and Admin3 only
E. Admin1, Admin2, Admin4, and Admin5 only
Answer: B (LEAVE A REPLY)
Scenario, Technical Requirements: All administrative users must be able to create Microsoft 365 sensitivity labels.
The administrator are setup with the following roles:
Admin1 is Global Reader.
Admin2 is Compliance Data Administrator.

Admin3 is Compliance Administrator.
Admin4 is Security Operator.
Admin5 is Security Administrator.
Only Admin1 (Global Reader) and Admin4 (Security Operator) need the additional Information Protection Admin (or Sensitivity Label Administrator) role to create sensitivity labels.
Role Requirements Breakdown
To create and manage Microsoft 365 sensitivity labels in the Microsoft Purview portal, a user must be assigned a role group that explicitly contains the Sensitivity Label Administrator permission.
Microsoft Purview provides this required permission natively through several built-in role groups:
Compliance Administrator (Assigned to Admin3)
Security Administrator (Assigned to Admin5)
Compliance Data Administrator (Assigned to Admin2)
Information Protection Admins
Reference:
https://learn.microsoft.com/en-us/purview/get-started-with-sensitivity-labels

NEW QUESTION: 45
You have a Microsoft SharePoint Online site named Site! 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.

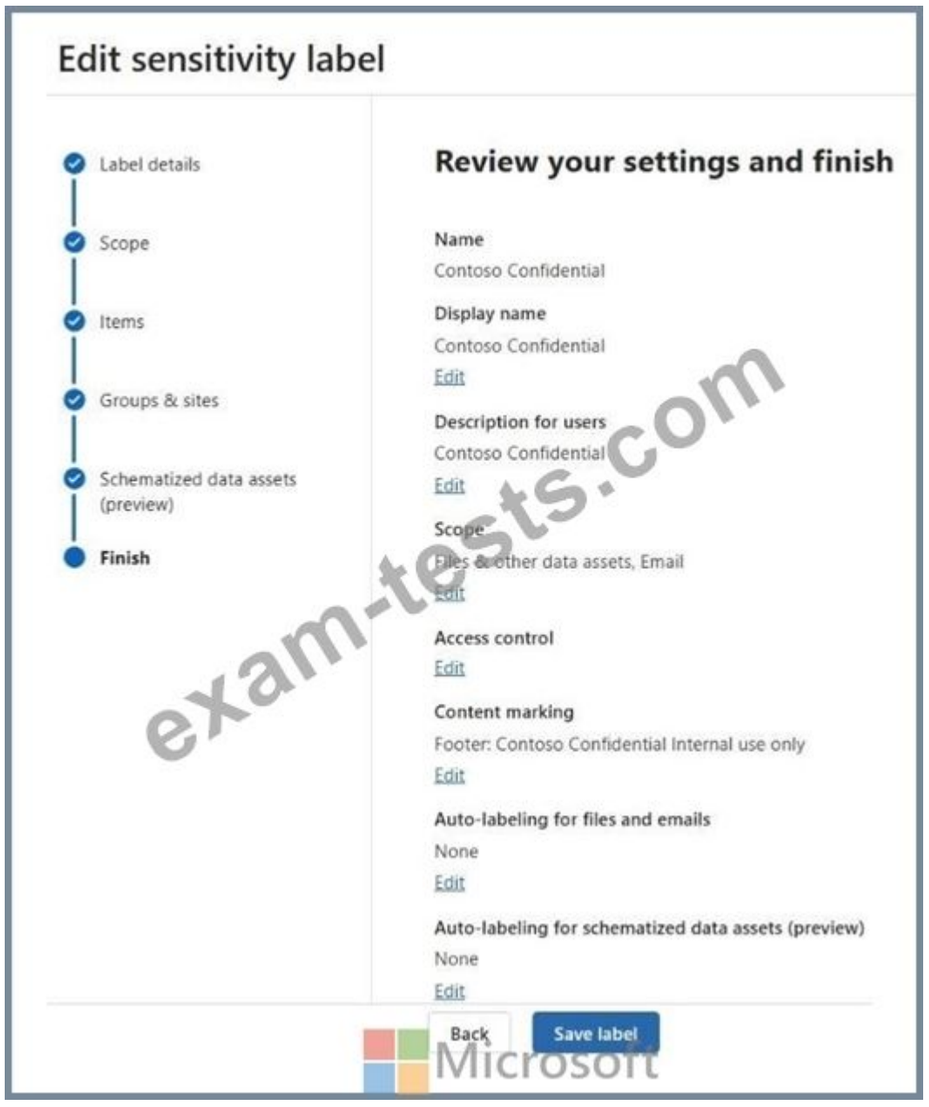
Name	Content contains	Policy tip	If match, stop processing	Priority
Rule1	1 or more IP addresses	Tip1	No	0
Rule2	3 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

You apply DLP1 toSite1.
Which policy tips will appear for File2?
A. Tip1 only
B. Tip2 only
C. Tip3 only
D. Tip1 and Tip2 only
Answer: (SHOW ANSWER)
Comprehensive Detailed Explanation with References
Step 1 - Review File2 contents
File2 contains 3 IP addresses.
Step 2 - Review DLP rules and priorities
RuleConditionPolicy TipStop Processing?Priority
Rule11 or more IP addressesTip1No0
Rule23 or more IP addressesTip2Yes1
Rule32 or more IP addressesTip3No2
Step 3 - Rule evaluation order

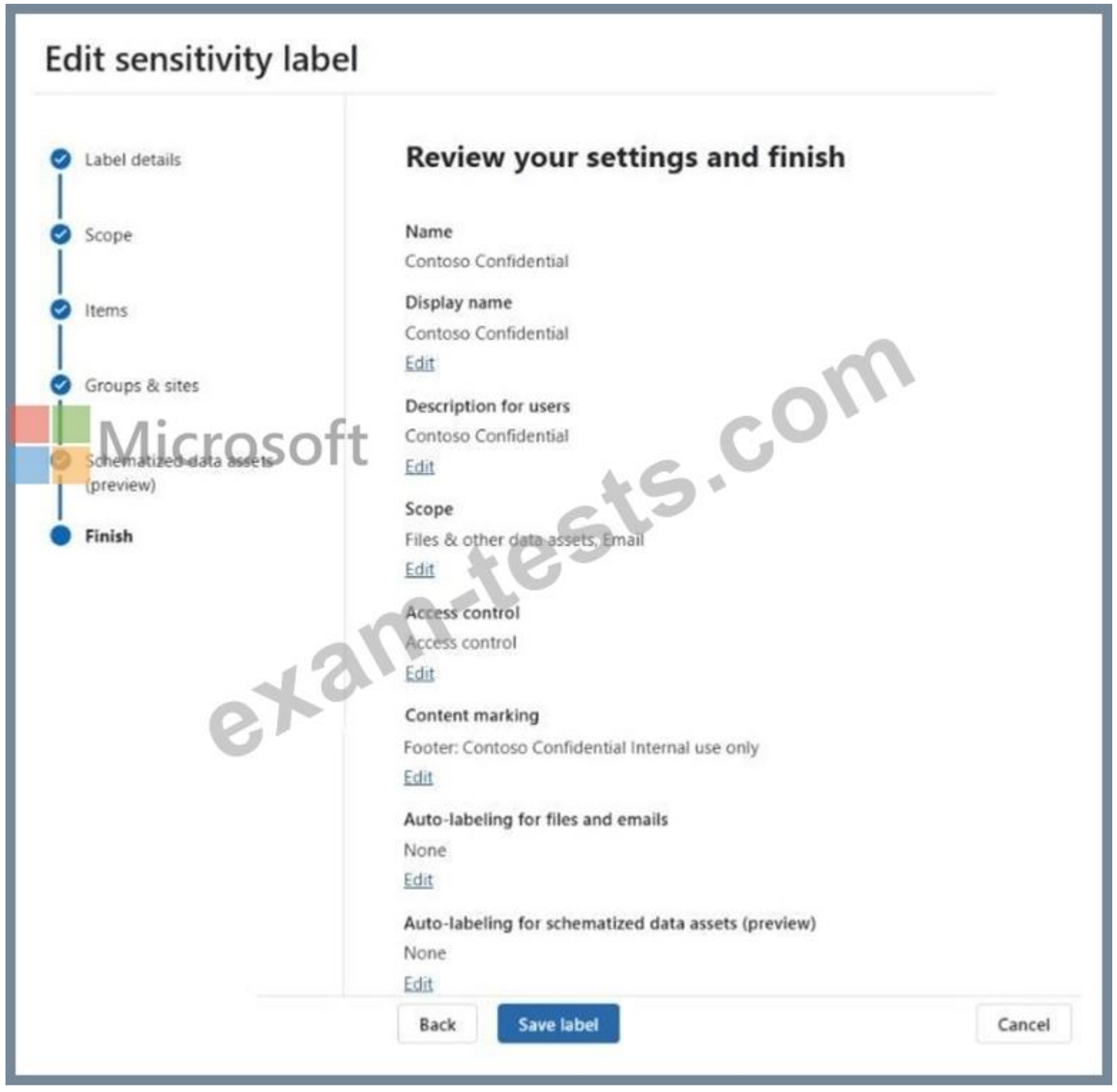
Advanced DLP rules are processed by priority order (lowest number first).
Rule1 (Priority 0) will trigger because File2 has at least 1 IP address.
This applies Tip1.
However, Rule1 has Stop Processing = No, so evaluation continues.
Rule2 (Priority 1) will also trigger because File2 has 3 IP addresses (#3).
This applies Tip2.
Rule2 has Stop Processing = Yes, so evaluation stops after this.
Rule3 (Priority 2) will not be evaluated because Rule2 stopped processing.
Step 4 - Final outcome
File2 matches Rule1 (Tip1), but since Rule2 fires afterward with Stop Processing = Yes, only Tip2 is applied.
Step 5 - Microsoft Reference
From Microsoft docs: "When a rule is configured to stop processing, subsequent rules are not evaluated and only the policy tip from the last triggered rule with stop processing applies."
Reference: Order of rule processing in DLP policies

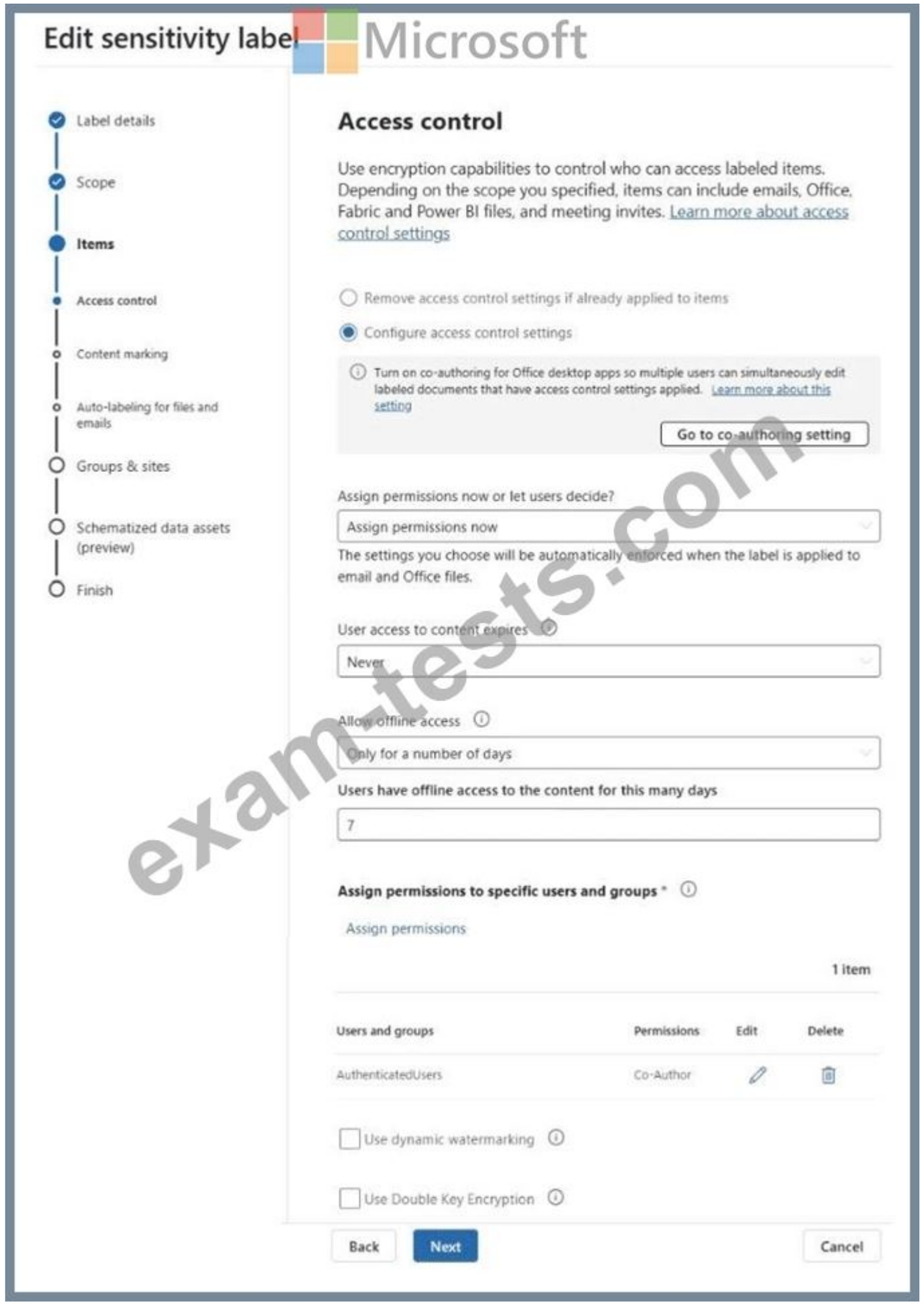
NEW QUESTION: 46
You need to provide a user with the ability to view data loss prevention (DIP) alerts in the Microsoft Purview portal. The solution must use the principle of least privilege.
Which role should you assign to the user?
A. Compliance Data Administrator
B. Security Operator
C. Security Reader
D. Compliance Administrator
Answer: (SHOW ANSWER)

NEW QUESTION: 47
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.)

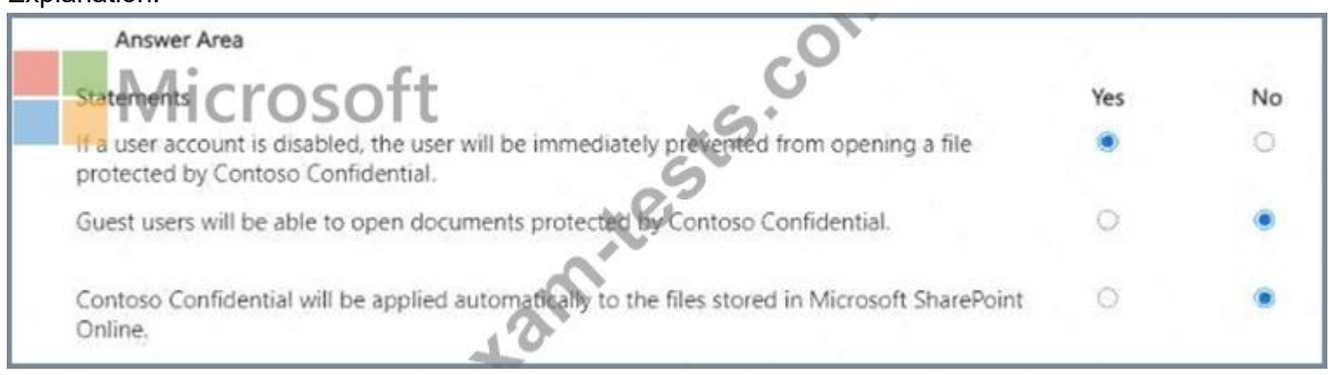




For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:



Step 1 - Review the configuration
Sensitivity label name: Contoso Confidential
Scope: Files and emails
Access control:
Encrypts documents/emails.
Permissions assigned to AuthenticatedUsers with Co-Author rights.
Offline access allowed only for 7 days.
Auto-labeling = None (not configured).
Content marking: Footer applied.
Step 2 - Analyze each statement
Statement 1: If a user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential.
Sensitivity labels with encryption enforce Azure AD authentication every time a user tries to access a file.
If the account is disabled in Azure AD, access is blocked immediately.
Statement 2: Guest users will be able to open documents protected by Contoso Confidential.
Access control was configured only for AuthenticatedUsers (internal users).

Guest or external users are not included in this group.
Therefore, guest users cannot open the protected documents.
Statement 3: Contoso Confidential will be applied automatically to the files stored in Microsoft SharePoint Online.
Auto-labeling for files and emails = None.
That means labeling must be applied manually by users, not automatically.
The answer: No
Final Verified Answers
If a user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential # Yes Guest users will be able to open documents protected by Contoso Confidential # No Contoso Confidential will be applied automatically to the files stored in Microsoft SharePoint Online # No

NEW QUESTION: 48
You have a Microsoft 365 E5 subscriptions.
You deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI).
You need to edit the default policies created as part of the deployment.
Which two Microsoft Purview solutions should you use? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Insider Risk Management
B. Information Protection
C. Compliance Manager
D. DSPMforAI
E. Information Barriers
F. Data Lifecycle Management
G. Data Loss Prevention
Answer: (SHOW ANSWER)
Step 1 - Understand the feature
The scenario is about Microsoft Purview Data Security Posture Management for AI (DSPM for AI), a capability in Microsoft Purview that helps:
* Discover sensitive data across AI environments (including Copilot for Microsoft 365).
* Assess data exposure risks.
* Apply policies for data classification and protection.
When you deploy DSPM for AI, Microsoft Purview automatically creates default policies to classify and protect sensitive content.
Step 2 - Which solutions are used to edit these policies?
* DSPM for AI (D) # This is the core solution where the default DSPM policies are deployed and visible. To edit or manage them, you must use the DSPM for AI blade in Microsoft Purview.
* Information Protection (B) # DSPM relies on Microsoft Information Protection (MIP), specifically sensitivity labels and sensitive information types. These labels and SITs are part of Purview Information Protection. Editing classification rules (e.g., sensitivity labels, sensitive info types, trainable classifiers) requires Information Protection.
# Reference:
* Microsoft Purview Data Security Posture Management for AI (DSPM for AI)
* Overview of sensitivity labels in Microsoft Purview Information Protection Step 3 - Why not the others?
* A. Insider Risk Management # Detects risky insider activities (data theft, sabotage). Not used to configure DSPM policies.
* C. Compliance Manager # Provides compliance score and assessments, but does not configure DSPM policies.
* E. Information Barriers # Used to restrict communication between groups of users. Not related to DSPM.
* F. Data Lifecycle Management # Manages retention and deletion of data. Not related to DSPM for AI policy editing.

* G. Data Loss Prevention (DLP) # Protects sensitive data from being shared in apps/services, but DSPM's default policies are not edited here.

NEW QUESTION: 49

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 Area

Statements	Yes	No
Summary1 has a sensitivity label applied.	○	○
Summary2 has a sensitivity label applied.	○	○
Summary3 has a sensitivity label applied.	○	○

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: 50

You have a Microsoft J65 E5 subscription. You plan to implement retention policies for Microsoft Teams.

Which item types can be retained?

A. voice memos from the Teams mobile client

B. embedded images

C. code snippets

Answer: (SHOW ANSWER)

The question is asking what item types can be retained when implementing Microsoft Teams retention policies in Microsoft 365 E5.

Retention policies in Teams can apply to:

Teams chat messages (1:1 or group chats)

Teams channel messages

Items within those messages, including text, links, and supported embedded objects.

Step 2 - Supported Teams retention items

According to Microsoft documentation:

Retention policies support Teams messages (chats and channel posts) and their associated attachments or in- line content such as:

Embedded images

Code snippets

Tables, links, and reactions

Retention policies do not support certain Teams items, including:

Voicemails
Calls and meetings recordings
Whiteboards
Message reactions (stored separately in Azure services)
Reference: Learn about retention for Teams in Microsoft Purview
Step 3 - Apply to options
A). Voice memos from the Teams mobile client # Not retained by retention policies.
B). Embedded images # Retained because they are part of Teams messages.
C). Code snippets # Retained because they are supported message content.

NEW QUESTION: 51
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 Conlent1 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. File1 .docx, File2.docx, and File3.docx
Answer: A (LEAVE A REPLY)
The content search uses the KQL editor with the query -Author:USER1. In eDiscovery/Content search, the minus sign denotes NOT and KQL is case-insensitive for property values.
Therefore, this query returns items whose Author is not 'User1'.
File1.docx # Author = User1 # excluded
File2.docx # Author = User2 # included
File3.docx # Author = USER1 (same as User1, case-insensitive) # excluded Result: File2.docx only.
Reference: Microsoft Search (KQL) property restrictions and case-insensitive behavior for queries in content search.

NEW QUESTION: 52
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. Compliance Administrator
B. Security Operator
C. Global Administrator
D. Security Administrator
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
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 Area

Create and manage DLP policies:

- User1
- User2
- User3

Review classified content by using Content explorer:

- User1
- User2
- User3

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: 54
You have a Microsoft 365 E5 subscription. The subscription contains a user named User1 and the sensitivity labels shown in the following table.

Name	Authenticated users: View content(VIEW)	Authenticated users: Copy and extract content(EXTRACT)	Authenticated users: Export content(EXPORT)
Label1	Granted	Not granted	Not granted
Label2	Granted	Granted	Not granted
Label3	Granted	Not granted	Granted

You publish the labels to User1.
The subscription contains the files shown in the following table.

Name	Label
File1	Label1
File2	Label2
File3	Label3

Which files can Microsoft 365 Copilot summarize for User1?
A. File2only
B. File3 only
C. File2 and File3 only
D. File1, File2. and File3
Answer: (SHOW ANSWER)
Microsoft 365 Copilot can only process (summarize, answer questions about) a labeled file when the user has the Copy and extract content (EXTRACT) usage right granted by the applied sensitivity label.
From the table of labels:
* Label1 # VIEW only (no EXTRACT) # Copilot cannot summarize.
* Label2 # VIEW and EXTRACT granted # Copilot can summarize.
* Label3 # VIEW and EXPORT (no EXTRACT) # Copilot cannot summarize.
Since File2 is labeled Label2, it's the only file for which User1 has the required EXTRACT permission, so it' s the only file Copilot can summarize.
References:
Microsoft Learn - Sensitivity labels and Copilot for Microsoft 365: Copilot requires the Copy and extract content (EXTRACT) permission to process labeled content.https://learn.microsoft.com/microsoft-365/compliance/sensitivity-labels-copilot
Microsoft Learn - Usage rights for encryption with sensitivity labels (VIEW, EXTRACT, EXPORT definitions)https://learn.microsoft.com/microsoft-365/compliance/encryption-sensitivity-labels#usage-rights- and-permissions

NEW QUESTION: 55

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

Name	Type	Member of
User1	User	*None*
User2	User	Group1
Group1	Group	*None*

The subscription contains a Windows 11 device named Device 1 and has the Microsoft Purview Information Protection client installed. Device i contains the resources shown in the following table.

Name	Type	Path
File1.png	File	C:\Temp
File2.docx	File	D:\Folder1
Folder2	Folder	D:\

You publish a sensitivity label named Label1 to User1 and Group1.

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

Answer Area

Statements	Yes	No
User1 can apply Label1 to File1.png by using the information protection client.	○	○
User1 can apply Label1 to Folder2 by using the information protection client.	○	○
User2 can apply Label1 to File2.docx by using the information protection client.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can apply Label1 to File1.png by using the information protection client.	◌	○
User1 can apply Label1 to Folder2 by using the information protection client.	○	◌
User2 can apply Label1 to File2.docx by using the information protection client.	◌	○

Explanation:

Answer Area

Statements	Yes	No
User1 can apply Label1 to File1.png by using the information protection client.	●	○
User1 can apply Label1 to Folder2 by using the information protection client.	○	●
User2 can apply Label1 to File2.docx by using the information protection client.	●	○

NEW QUESTION: 56

Hotspot Question

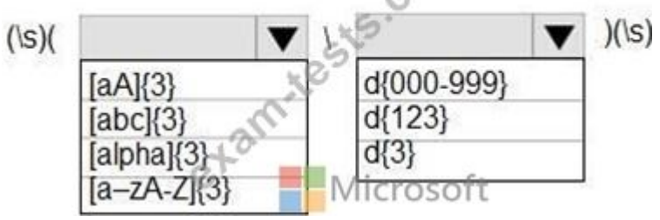
You use project codes that have a format of three alphabetical characters that represent the project type, followed by three digits, for example Abc123.

You need to create a new sensitive info type for the project codes.

How should you configure the regular expression to detect the content? To answer, select the appropriate options in the answer area.

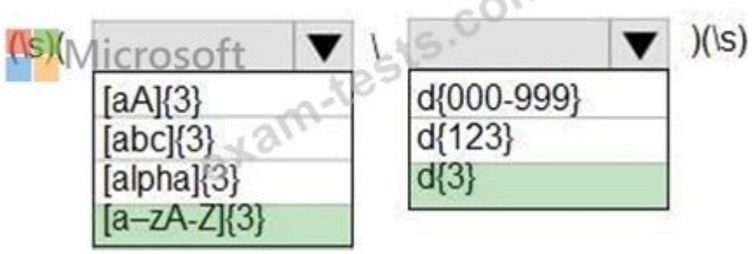
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



NEW QUESTION: 57

You have a Microsoft J65 E5 subscription that contains a user named User1.

All users are assigned Microsoft 365 Copilot licenses.

You deploy Microsoft Purview Data Security Posture Management for Al (DSPM for Al).

You need to ensure that User1 can analyze prompts and responses for Al interaction events. The solution must follow the principle of least privilege.

To which two role groups should you add User1? Each correct answer presents part of the solution.

NOTE; Each correct selection is worth one point.

A. Information Protection Analysts

B. Security Reader

C. Content Explorer Content Viewer

D. Insider Risk Management Investigators

E. Content Explorer list Viewer

Answer: A,E (LEAVE A REPLY)

The requirement is that User1 must be able to analyze prompts and responses for AI interaction events in Microsoft Purview DSPM for AI, while following the principle of least privilege.

Information Protection Analysts role group:

Members can review and analyze sensitive data activity, including AI interaction events collected by Purview DSPM. This role is specifically intended for analysts monitoring sensitive information and is therefore necessary for User1.

Content Explorer List Viewer role group:

Members can see metadata about items with sensitive information, such as file names, locations, sensitivity labels, and policy matches, without accessing the actual file content. This provides the required visibility for AI-related data classification and interaction analysis while adhering to the least privilege principle.

Roles not required:

Content Explorer Content Viewer would give the ability to view the actual content of files, which is more access than needed.

Security Reader is intended for reviewing alerts and incidents but not for analyzing AI prompts and responses.
Insider Risk Management Investigators focus on insider risk investigations, not AI event analysis.
References:
Microsoft Learn: Microsoft Purview compliance portal permissions
Microsoft Learn: Use Content Explorer in data classification

NEW QUESTION: 58
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 Sensitivity! as shown in the exhibit. (Click the Exhibit tab) 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:

Statements	Yes	No
User1 can edit rights for File1.	○	○
User2 can edit rights for File3.	○	○
User3 can print File2.	○	○

Explanation:
Yes , Yes, No
To determine whether each statement is true or false, let's analyze the provided information step by step based on the sensitivity label settings and the user permissions associated with the files.
Given Information:
Users and Subscriptions:
User1: Contoso subscription, email: user1@contoso.com

User2: Contoso subscription, email: user2@contoso.com
User3: Fabrikam subscription, email: user3@fabrikam.com
User4: Fabrikam subscription, email: user4@fabrikam.com
Files and Sensitivity Label Application:
File1: Automatically applied Sensitivity1 using an auto-labeling policy File2: Applied by User2 File3: Applied by User1 Sensitivity Label (Sensitivity1) Assumptions: Since the exhibit for the sensitivity label is not fully detailed, we need to make reasonable assumptions based on typical Microsoft 365 sensitivity label behavior.
Sensitivity labels can restrict access based on user permissions, subscription boundaries, or specific configurations (e.g., allowing only users within the same organization to edit or view).
Given the context of two separate subscriptions (Contoso and Fabrikam), it's likely that Sensitivity1 restricts access to users within the same subscription unless explicitly configured otherwise. A common default for such labels is to allow editing and other rights only to users within the applying user's organization, with possible restrictions for cross-subscription access.
Key Assumptions:
Sensitivity1 likely encrypts the files and restricts editing rights to users within the same subscription as the user who applied the label or where the auto-labeling policy is configured.
File1 (auto-applied) would inherit permissions based on the policy, likely restricting access to Contoso users if the policy is set up within the Contoso subscription.
File2 (applied by User2 from Contoso) would restrict access to Contoso users.
File3 (applied by User1 from Contoso) would also restrict access to Contoso users.
Users from Fabrikam (User3, User4) would not have edit rights unless explicitly granted, which is unlikely given the separation of subscriptions.
Statement Analysis:
User1 can edit rights for File1.
File1 was automatically applied with Sensitivity1 using an auto-labeling policy. Since the policy is likely configured within the Contoso subscription (where User1 resides), User1, as a Contoso user, should have edit rights unless the policy explicitly restricts this. Given User1's affiliation with Contoso, this is typically allowed.
The answer: Yes
User2 can edit rights for File3.
File3 was applied by User1, who is from the Contoso subscription. Since User2 is also from the Contoso subscription, they should have edit rights unless the label configuration explicitly denies this for other users within the same subscription. Typically, users within the same organization can edit files labeled by another user from the same organization.
The answer: Yes
User3 can print File2.
File2 was applied by User2, who is from the Contoso subscription. Sensitivity1 likely restricts access to Contoso users only. User3 is from the Fabrikam subscription, which is a separate entity. Unless cross-sub Answer : No

NEW QUESTION: 59
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: 60
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft Purview insider risk management.
You implement the HR data connector.
You need to prepare the data that will be imported by the data connector.
In which format should you prepare the data?
A. JSON
B. CSV
C. TSV
D. XML
E. PRN
Answer: B (LEAVE A REPLY)
When implementing Microsoft Purview Insider Risk Management and using the HR data connector, you must prepare HR data in CSV (Comma-Separated Values) format. This format is required because Microsoft Purview supports CSV files for importing user employment details, termination dates, role changes, and other HR-related attributes.

NEW QUESTION: 61
Hotspot Question
You have Microsoft 365 E5 tenant that has a domain name of 86s40q.onmicrosoft.com.
The tenant contains the users shown in the following table.

Name	User type
User1	Member
User2	Guest

You have a published sensitivity label.
The Access control settings for the sensitivity label are configured 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

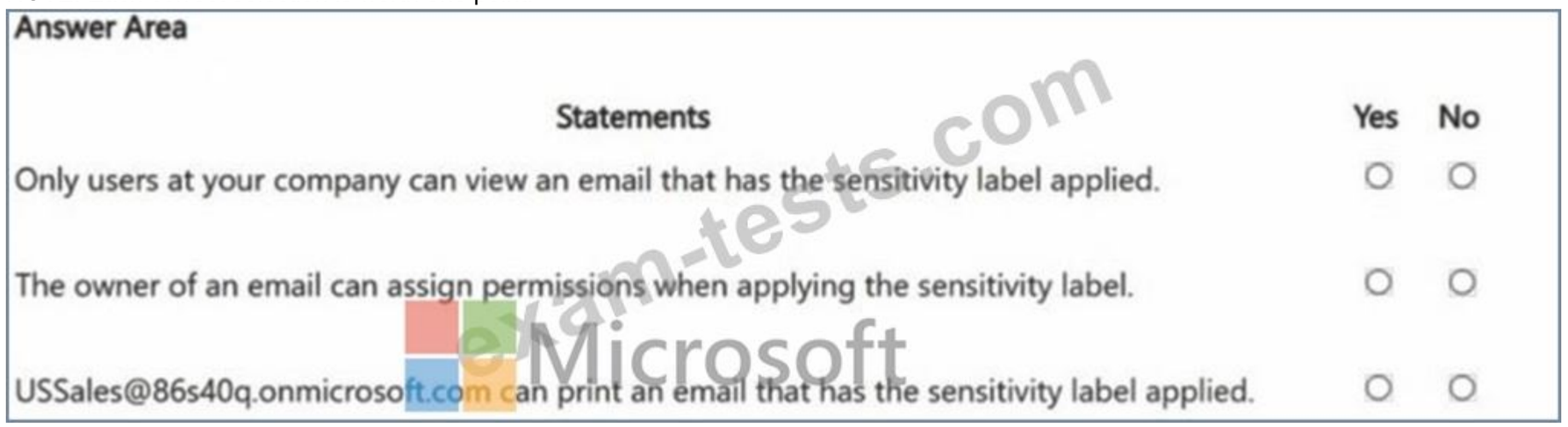
Users and groups	Permissions	Edit	Delete
LegalTeam@86s40q.onmicrosoft.com	Co-Author		
USSales@86s40q.onmicrosoft.com	Reviewer		

☐ Use dynamic watermarking ⓘ

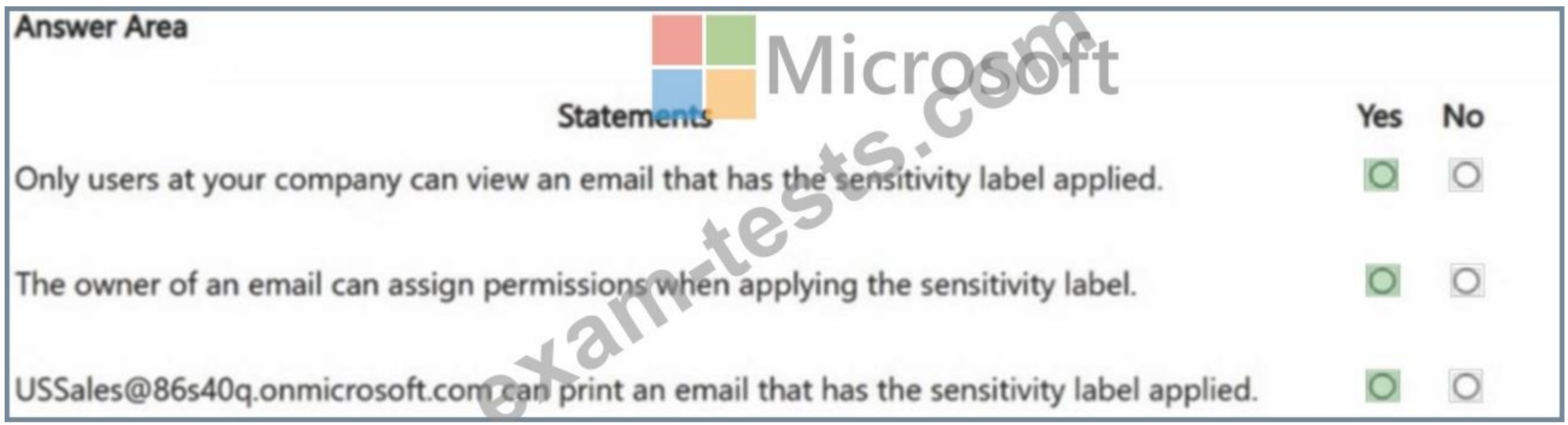
☐ Use Double Key Encryption ⓘ

Back | Next | Cancel

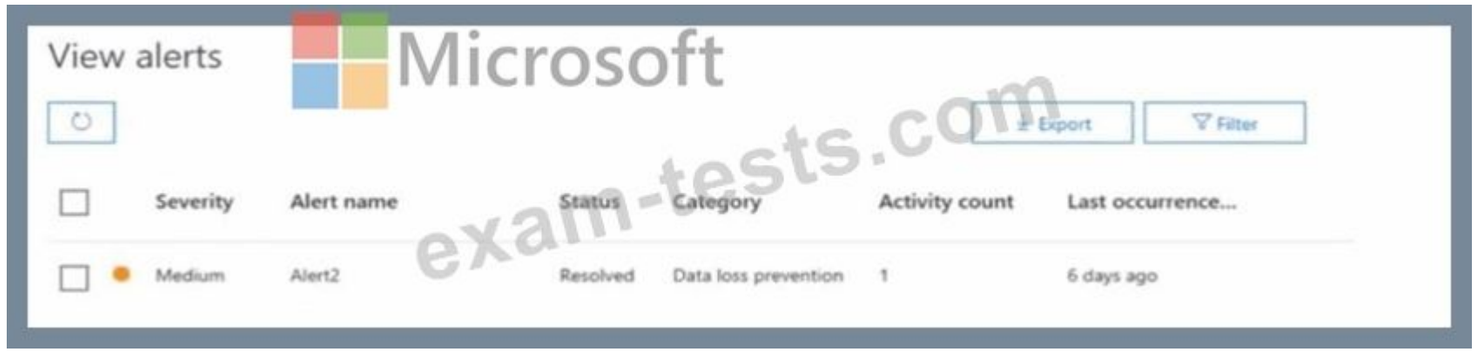
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 62
You have a Microsoft 365 alert named Alert2 as shown in the following exhibit.



You need to manage the status of Alert? To which status can you change Alette?

A. The status cannot be changed.

B. Dismissed only

C. Investigating only

D. Active or Investigating only

E. Investigating. Active, or Dismissed

Answer: E (LEAVE A REPLY)

Step 1 - Scenario

The alert in the exhibit is named Alert2.

Current status = Resolved.

The task is to identify which statuses you can change the alert to.

Step 2 - Microsoft 365 Alert Lifecycle

In Microsoft 365 compliance and security alerts, an alert can move between multiple statuses depending on investigation and remediation. The available statuses are:

Active - The alert is new and not yet acted upon.

Investigating - The alert is under review.

Resolved - The alert has been addressed.

Dismissed - The alert is ignored or deemed not relevant.

Step 3 - Status changes from "Resolved"

If an alert is in the Resolved state, administrators can reopen or reclassify it. According to Microsoft documentation, from Resolved, you can change it to:

Active

Investigating

Dismissed

This allows flexibility in continuing investigations if needed or dismissing false positives.

Step 4 - Microsoft Reference

From Microsoft Docs: "You can change the status of an alert between Active, Investigating, Resolved, and Dismissed to reflect its current stage in the triage process." Reference: Manage alerts in the Microsoft 365 security and compliance center

NEW QUESTION: 63

SIMULATION

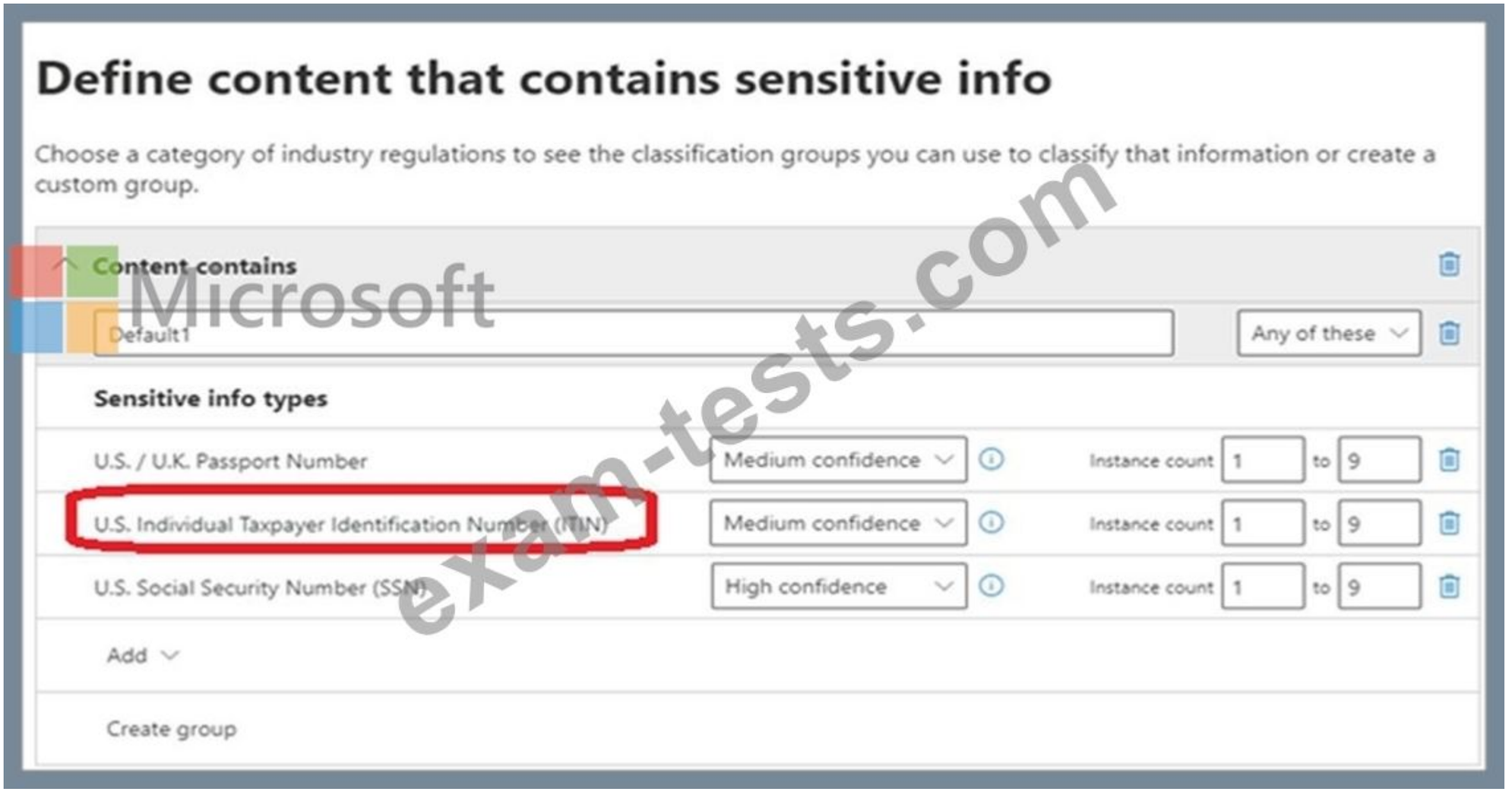
Username and password

Use the following login credentials as needed:

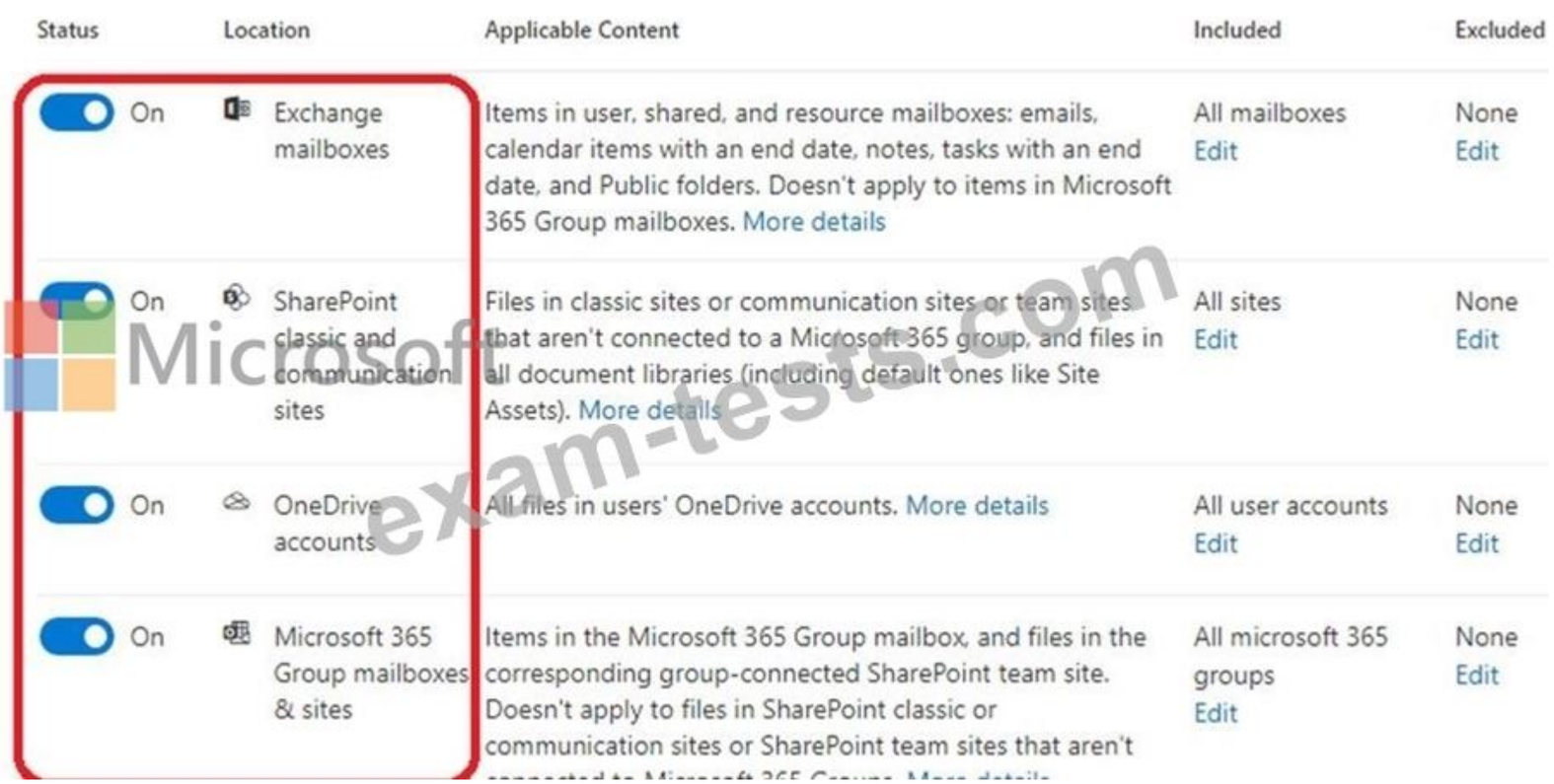
To enter your username, place your cursor in the Sign in box and select the username below.

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 8
You need to ensure that the Employee Records retention label is applied automatically to content that meets the following requirements:
- Contains only the U.K. Unique Taxpayer Reference Number sensitive info type
- Is located in any Exchange email, SharePoint sites, OneDrive accounts or Microsoft 365 groups
Answer:
See explanation below.
Explanation:
To configure a retention label to use a specific sensitive information type, you need to create an auto-labeling policy in the Microsoft Purview portal that applies a label to content containing that sensitive information type. First, create the retention label itself with its retention settings, and then create the auto-labeling policy, select "Apply label to content that contains sensitive info," choose the desired sensitive info type, specify the locations to apply it, and select your retention label.
Step 1: Sign in to the Microsoft Purview portal.
Step 2: If you're using records management [Yes!]: Solutions > Records Management > Policies > Label policies > Auto-apply a label Step 3: Enter a name and description for this auto-labeling policy, and then select Next.
Step 4: For Choose the type of content you want to apply this label to, select one of the available conditions.
Auto-apply labels to content with specific types of sensitive information Step 5: Select U.K. Unique Taxpayer Reference Number sensitive info type in the U.K Personally Identifiable Information (PII) Data template.
When you create auto-apply retention label policies for sensitive information, you see the same list of policy templates as when you create a Microsoft Purview Data Loss Prevention (DLP) policy. Each template is preconfigured to look for specific types of sensitive information. In the following example, the sensitive info types are from the Privacy category, and U.S Personally Identifiable Information (PII) Data template:



Step 6: For the Assign admin units page, keep the default of Full directory. Currently, admin units aren't supported for this policy.
Step 7: For the Choose the type of retention policy to create page, select Adaptive or Static.
[Select Static]
Step 8: If you chose Static: On the Choose locations page, toggle on or off any of the locations.
Select:
Exchange email
SharePoint sites
OneDrive accounts
Microsoft 365 groups



Step 9: Follow the prompts to select a retention label, whether to run the policy in simulation mode or turn it on (if applicable for your chosen condition), and then review and submit your configuration choices.

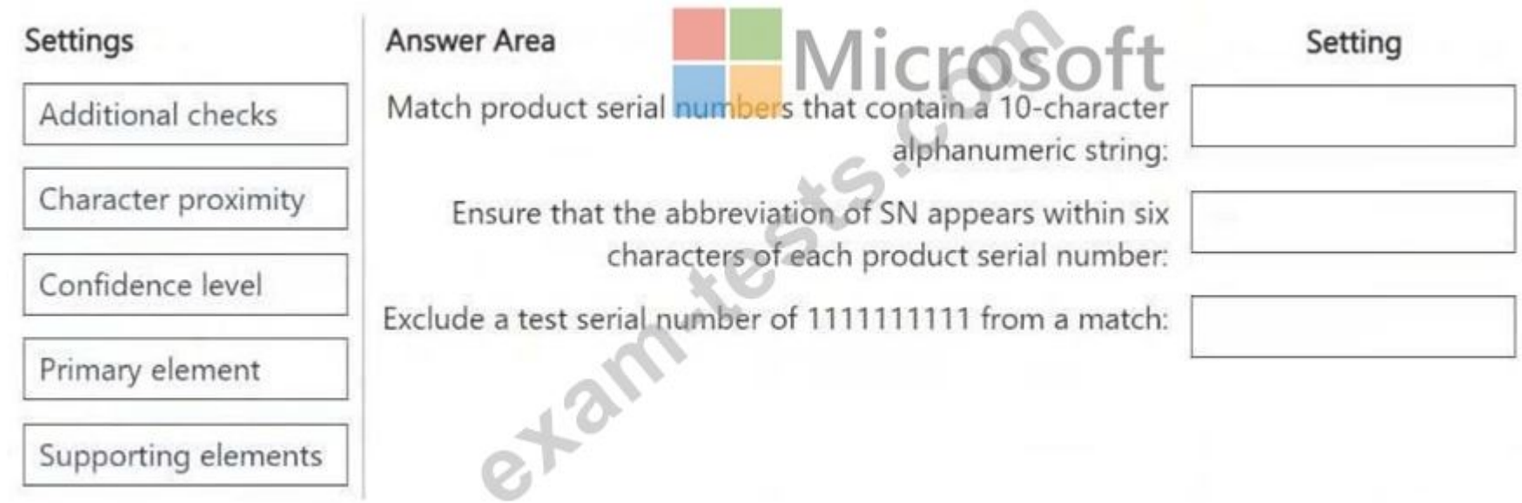
Reference:
https://learn.microsoft.com/en-us/purview/apply-retention-labels-automatically
https://learn.microsoft.com/en-us/purview/retention-settings#locations

NEW QUESTION: 64
You need to meet the technical requirements for the creation of the sensitivity labels.
To which user or users must you assign the Sensitivity Label Administrator role?
A. Admin1 only
B. Admin1 and Admin4 only
C. Admin1 and Admin5 only
D. Admin1, Admin2, and Admin3 only
E. Admin1, Admin2, Admin4, and Admin5 only
Answer: D (LEAVE A REPLY)
To meet the requirement that all administrative users must be able to create Microsoft 365 sensitivity labels, we need to assign the Sensitivity Label Administrator role to the correct users.
Sensitivity Label Administrator Role Responsibilities
This role allows users to:
*Create and manage sensitivity labels in Microsoft Purview.
*Publish and configure auto-labeling policies.
*Modify label encryption and content marking settings.
Review of Admin Roles from the Table:

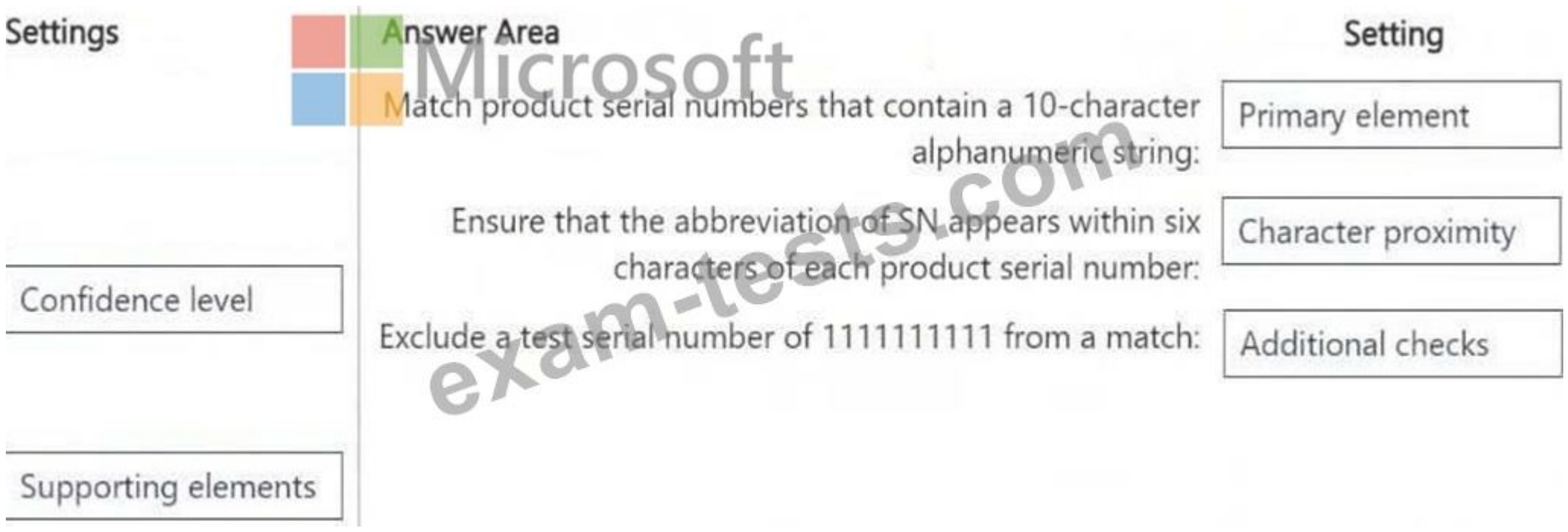
Admin	Role Assigned	Can Create Sensitivity Labels?
Admin1	Global Reader	☐ No, read-only permissions.
Admin2	Compliance Data Administrator	☐ Yes, can manage compliance data, including labels.
Admin3	Compliance Administrator	☐ Yes, has full compliance management, including labels.
Admin4	Security Operator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

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

NEW QUESTION: 65
Drag and Drop Question
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.
You need to create a custom sensitive info type. The solution must meet the following requirements:
- Match product serial numbers that contain a 10-character alphanumeric string.
- Ensure that the abbreviation of SN appears within six characters of
each product serial number.
- Exclude a test serial number of 1111111111 from a match.
Which pattern settings should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
Microsoft custom sensitive info types use pattern settings to refine detection accuracy for data loss prevention (DLP) policies.
The Primary element defines the main pattern that must be detected. Since we need to match a
10-character alphanumeric string, this should be defined in the primary element.
Character proximity determines how close a supporting keyword (e.g., "SN") must be to the detected data. Since "SN" must be within six characters of the product serial number, this setting ensures a valid match.
Additional checks allow for exceptions and exclusions in the detection logic. This ensures that
1111111111 (a test serial number) is excluded from triggering a match.

NEW QUESTION: 66
You have a Microsoft 365 E5 tenant that contains a user named User1. User1 is assigned the Compliance Administrator role. User1 cannot view the regular expression in the IP Address sensitive info type. You need to ensure that User! can view the regular expression. What should you do?
A. Assign User1 the Global Reader role.

B. Assign Used to the Reviewer role group
C. Instruct User1 to use the Test function on the sensitive info type.
D. Create a copy of the IP Address sensitive info type and instruct User1 to edit the copy.
Answer: (SHOW ANSWER)

NEW QUESTION: 67
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 ate 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:

Explanation:

Step 1 - Review what's configured

Labels: Public, General, Confidential, Internal, External.

Also shown in policy: Confidential/Internal and Confidential/External.

Policy setting: Users must provide justification to remove a label or lower its classification.

Confidential/External # encrypts content when applied.

Step 2 - Analyze each statement

Statement 1: The Internal sensitivity label inherits all the settings from the Confidential label.

Sub-labels (e.g., Confidential/Internal, Confidential/External) do not inherit settings from the parent.

They are independent labels grouped under a parent for organization, but each sub-label must have its own protection settings defined.

Statement 2: Users must provide justification if they change the label of content from Confidential/Internal to Confidential/External.

The policy requires justification only when removing a label or downgrading classification (lowering).

Changing between two sub-labels of the same parent (Confidential/Internal # Confidential/External) is considered a lateral move (not a downgrade).

Statement 3: Content that has the Confidential/External label applied will retain the encryption settings if the sensitivity label is removed from the label policy.

If a label is removed from a published policy, content already labeled retains its protection settings (such as encryption).

The label metadata stays applied to the file/email, even if unpublished.

Reference: What happens when you delete or edit a sensitivity label

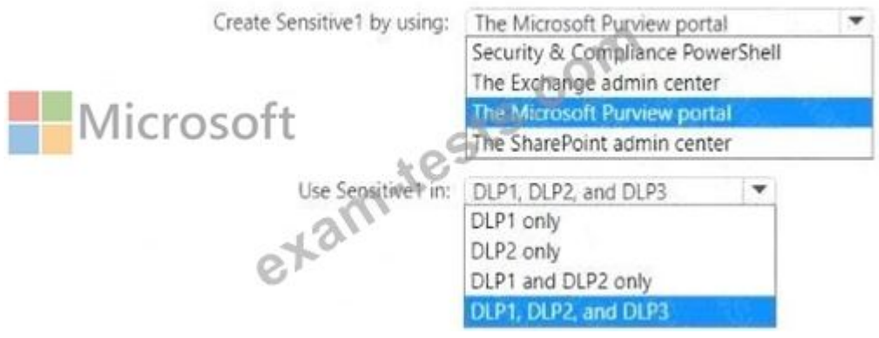
NEW QUESTION: 68

You create a retention label that has a retention period of seven years.
You need to ensure that documents containing a credit card number are retained for seven years. Other documents must not be retained.
What should you create?
A. a retention policy that retains files automatically
B. a retention policy that deletes files automatically
C. a retention label policy of type auto-apply
D. a retention label policy of type publish
Answer: C (LEAVE A REPLY)

NEW QUESTION: 69
You have a Microsoft 365 E5 subscription that contains the data loss prevention (DLP) policies shown in the following table.

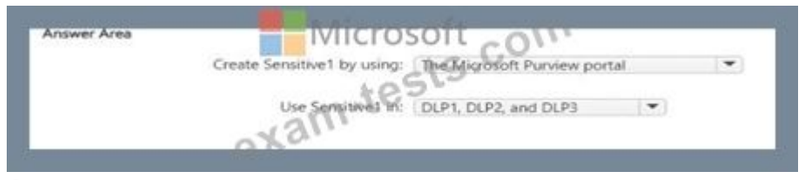
Name	Applied to
DLP1	Microsoft Exchange Online email
DLP2	Microsoft SharePoint Online sites
DLP3	Microsoft Teams chat and channel messages

You have a custom employee information form named Template1 .docx.
You plan to create a sensitive info type named Sensitive! 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.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Step 1 - Requirement
You want to create a custom sensitive info type named Sensitive1.
This SIT will be created from a document fingerprint of Template1.docx.
You then want to use Sensitive1 in DLP policies.
Step 2 - Where do you create custom Sensitive Info Types?
Custom SITs (including document fingerprinting) can only be created in the Microsoft Purview compliance portal.
They cannot be created in the Exchange admin center, SharePoint admin center, or directly in PowerShell.
Answer for creation: The Microsoft Purview portal
Reference: Create a custom sensitive information type with document fingerprinting Step 3 - Where can custom Sensitive Info Types be used?
Once created, custom SITs are tenant-wide and can be used across all workloads that support DLP:
Exchange email
SharePoint Online sites
OneDrive
Teams chat and channel messages
In the table, the DLP policies are:
DLP1 # Exchange Online email
DLP2 # SharePoint Online sites
DLP3 # Teams chat and channel messages
Since Sensitive1 is a custom SIT, it can be used in all three policies.
Answer for usage: DLP1, DLP2, and DLP3

NEW QUESTION: 70
You have a Microsoft 365 E5 subscription.
You need to ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days.
What should you configure first?
A. a custom branding template
B. a mail flow rule
C. a sensitivity label
D. a Conditional Access policy
Answer: A (LEAVE A REPLY)
To ensure that encrypted email messages sent to external recipients can be revoked or expire within seven days, you need to configure a sensitivity label with encryption settings in Microsoft Purview Information Protection. A sensitivity label allows you to encrypt emails and documents, set expiration policies (e.g., emails expire after 7 days), and enable email revocation How to configure it?
Go to Microsoft Purview compliance portal # Information Protection
Create a sensitivity label
Enable encryption and configure the content expiration policy
Publish the label to users

NEW QUESTION: 71
You have a Microsoft 365 subscription.
You plan to retain the following audit log record types and activities for the next three years:
- CopilotInteraction: All activities selected (1/1)
- Interacted with Copilot
- ComplianceDLPEndpoint: All activities selected (2/2)
- Matched DLP rule
- Removed DLP rule from document
- AzureActiveDirectory: 2 of 25 activities selected (2/25)
- Reset user password
- Changed user password
What is the minimum number of audit retention policies you should create to retain only the selected record types and activities?
A. 1
B. 2
C. 3
D. 5
Answer: A (LEAVE A REPLY)
You only need one Microsoft 365 audit retention policy to cover CopilotInteraction, ComplianceDLPEndpoint, and AzureActiveDirectory for three years, as a single policy can be configured with a three-year duration to apply to all specified record types. However, this requires having a Microsoft 365 Enterprise E5 subscription and a 10-Year Audit Log Retention add-on license to meet the three-year retention requirement.
Reference:
https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

NEW QUESTION: 72
You have a Microsoft 365 E5 subscription.
Microsoft Purview Compliance Manager has the improvement actions shown in the following table.

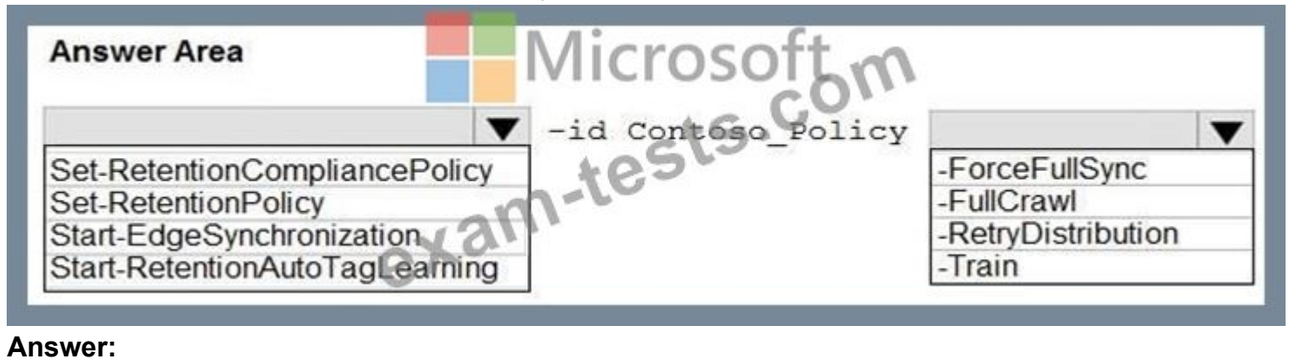
Name	Improvement action	Implementation status
Action1	Enable' Consistent MIME Handling'	Not implemented
Action2	Configure external sharing links to expire	Implemented
Action3	Update antivirus definitions	Alternative implementation
Action4	Enable self-service password reset	Planned

Automatic testing is disabled for all improvement actions.
For which improvement actions can you update the Test status?
A. Action1 only
B. Action2 only
C. Action2 and Action3 only
D. Action1 and Action4 only
E. Action1, Action2, Action3 and Action4
Answer: C (LEAVE A REPLY)

When "Automatic Testing" is disabled for all improvement actions, you can update the Test status for actions that are either implemented or have an alternative implementation.
* Action2 (Configure external sharing links to expire) - Implemented
* Action3 (Update antivirus definitions) - Alternative implementation

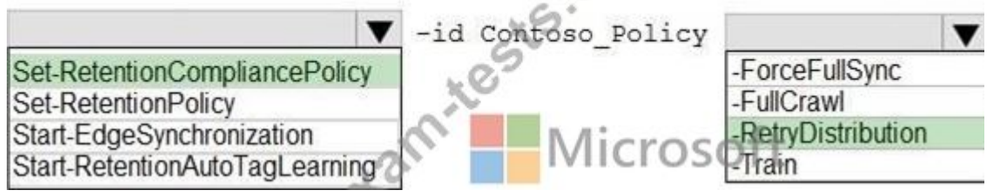
NEW QUESTION: 73
You have a Microsoft 365 E5 subscription. Microsoft Priva Privacy Risk Management licenses are assigned to all users.
You need to review and delete all the personal data that relates to a former employee. The solution must minimize administrative effort.
What should you do first?
A. Create a retention policy.
B. From Data matching, add a personal data schema for the data profile.
C. Purchase a Microsoft Priva Subject Rights Requests license.
D. Create an eDiscovery (Standard) case.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 74
Hotspot Question
You create a retention label policy named Contoso Policy that contains the following labels:
10 years then delete
5 years then delete
Do not retain
Contoso_Policy is applied to content in Microsoft SharePoint Online sites.
After a couple of days, you discover the following messages on the Properties page of the label policy:
- Status: Off (Error)
- It's taking longer than expected to deploy the policy
You need to reinitiate the policy.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Answer Area



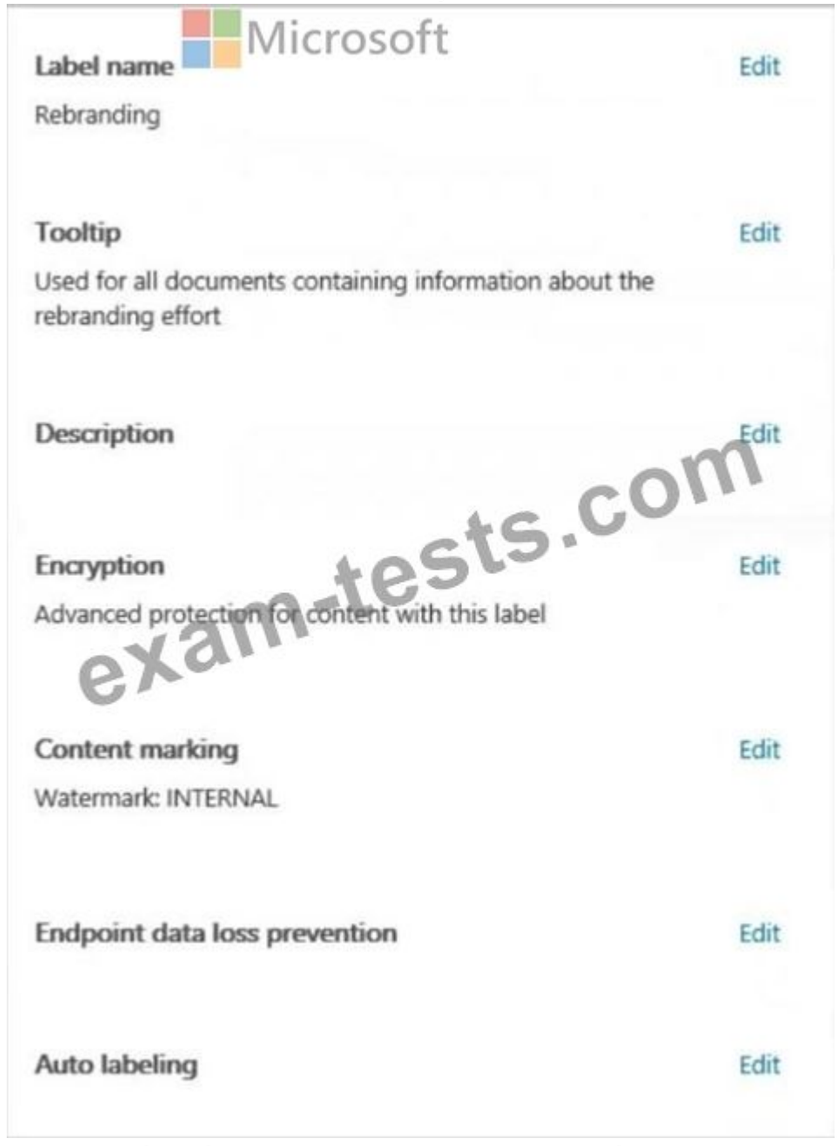
Explanation:

https://docs.microsoft.com/en-us/powershell/module/exchange/set-retentioncompliancepolicy

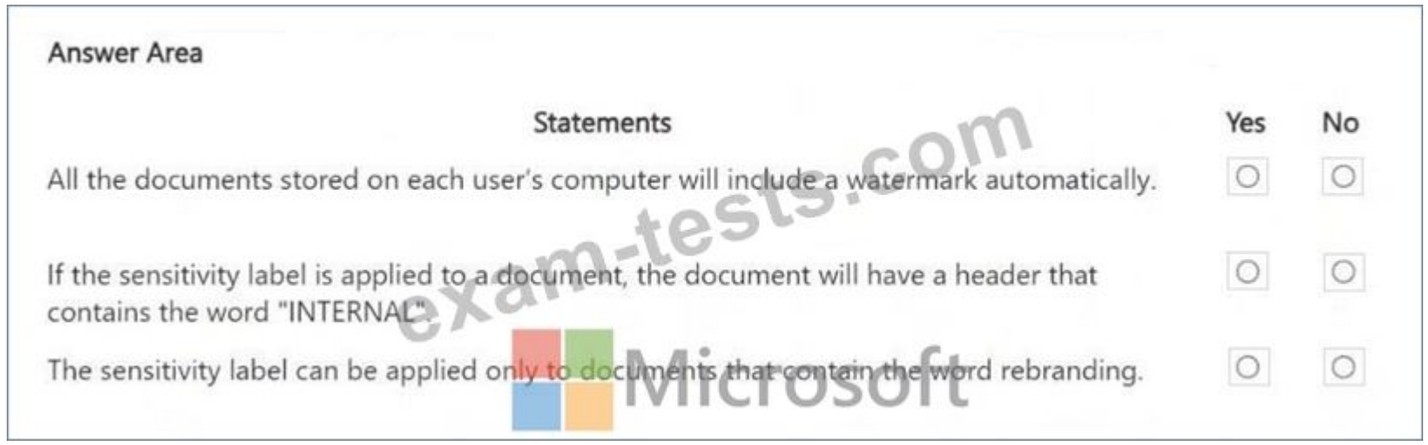
NEW QUESTION: 75

Hotspot Question

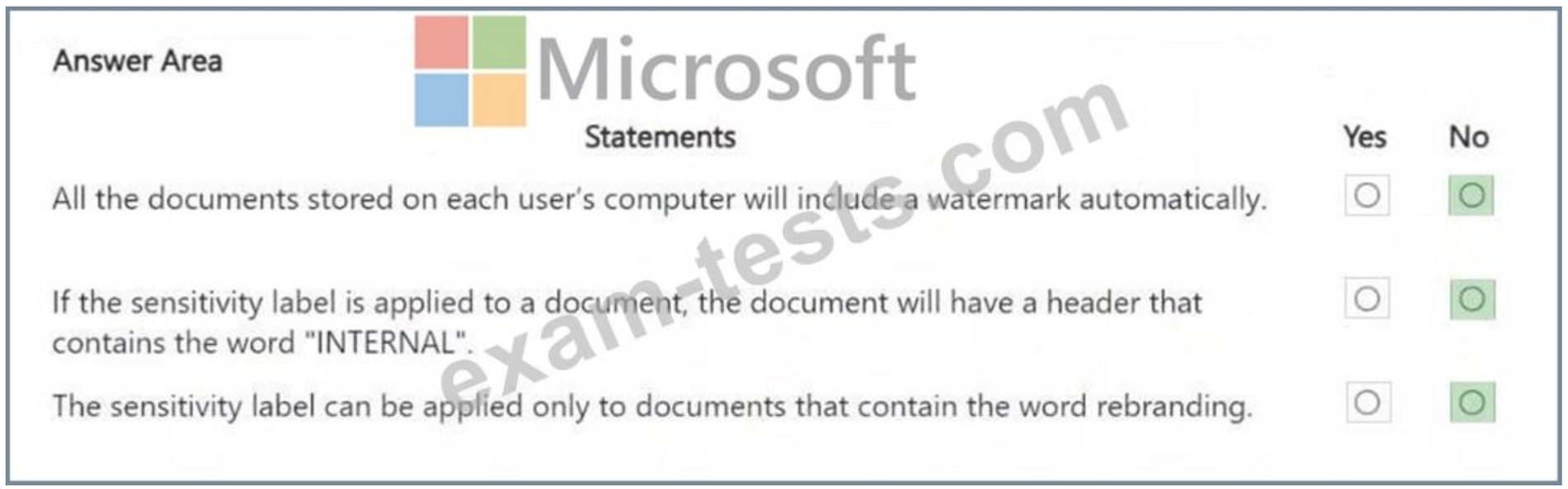
You have a Microsoft 365 sensitivity label that is published to all the users in your Microsoft Entra tenant as shown in the following exhibit.



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.

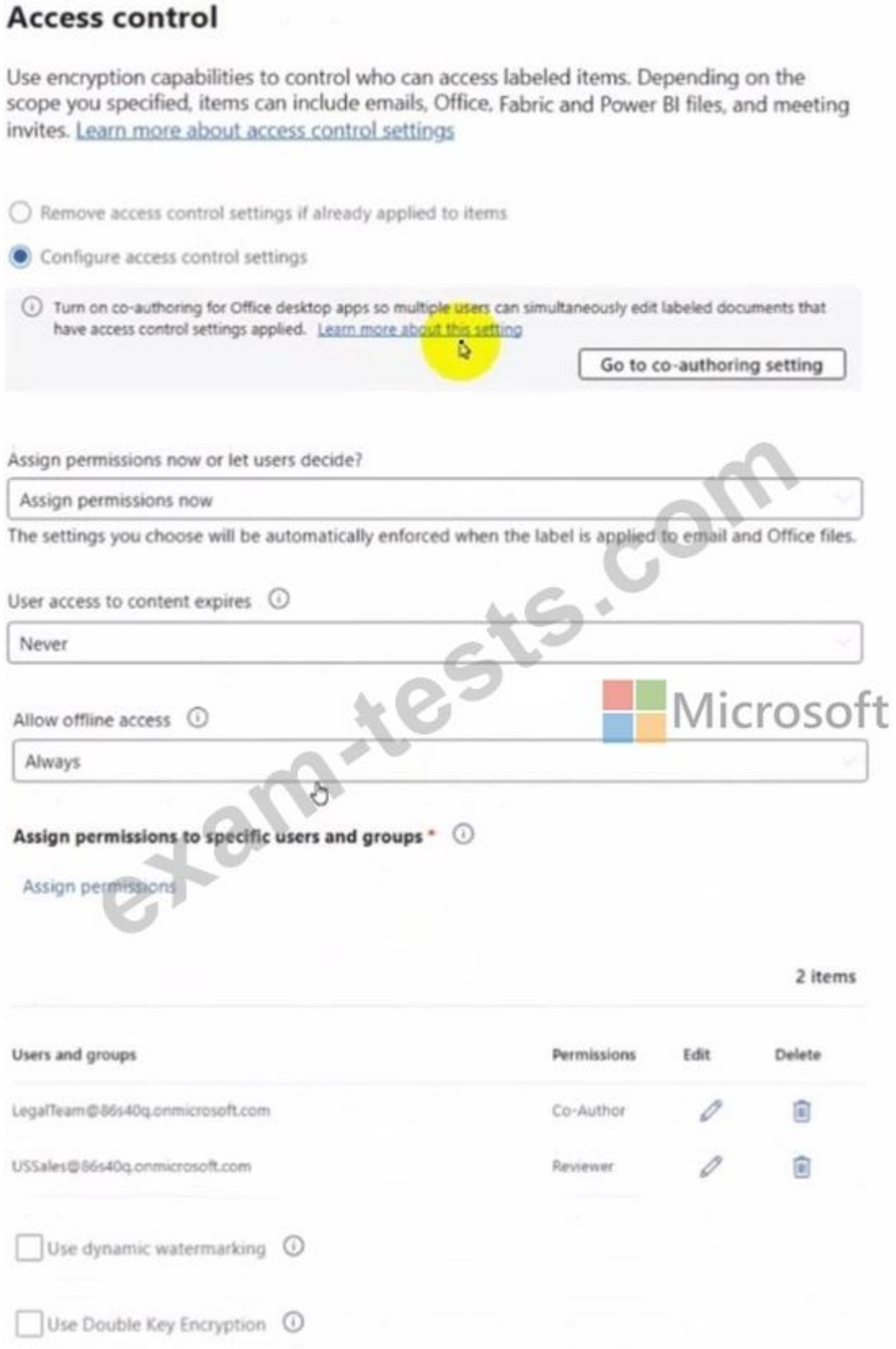
NEW QUESTION: 76
You have a Microsoft 365 E5 subscription.
You need to ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days.
What should you configure first?
A. a sensitivity label
B. a custom branding template
C. a Conditional Access policy
D. a mail flow rule

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

NEW QUESTION: 77
You have Microsoft 365 E5 tenant that has a domain name of 86s40q.ofimicrosoft.com. The tenant contains the users shown in the following table.

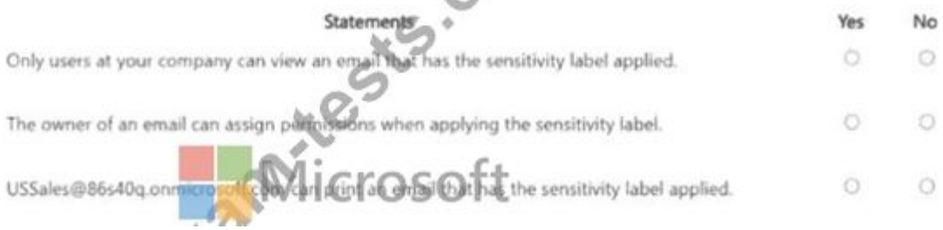
Name	User type
User1	Member
User2	Guest

You have a published sensitivity label.
The Access control settings for the sensitivity label are configured as shown in the exhibit (Click the Exhibit tab.)

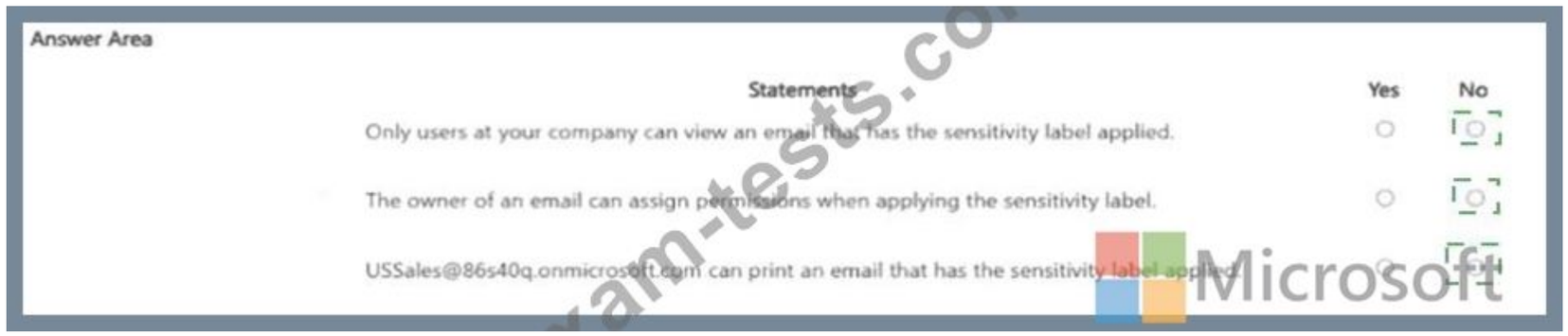


For each of the following statements, select Yes if the statement is true. Otherwise, select No.

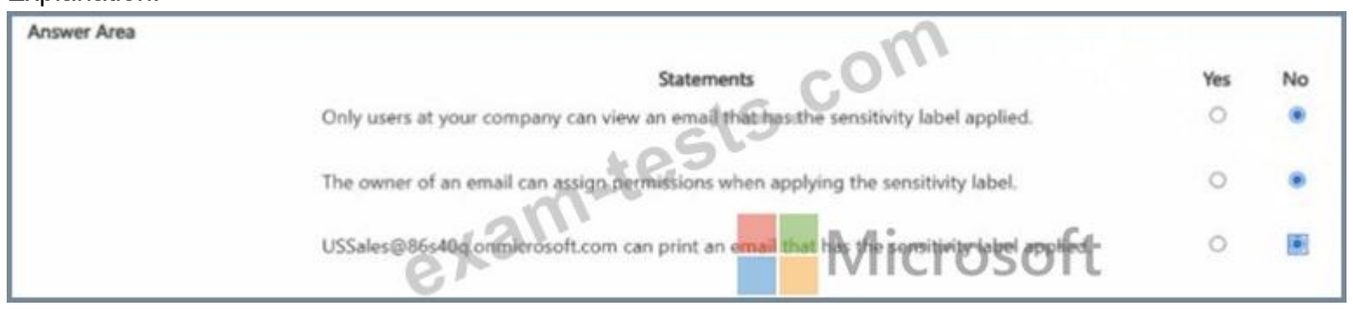
Answer Area



Answer:



Explanation:



NEW QUESTION: 78

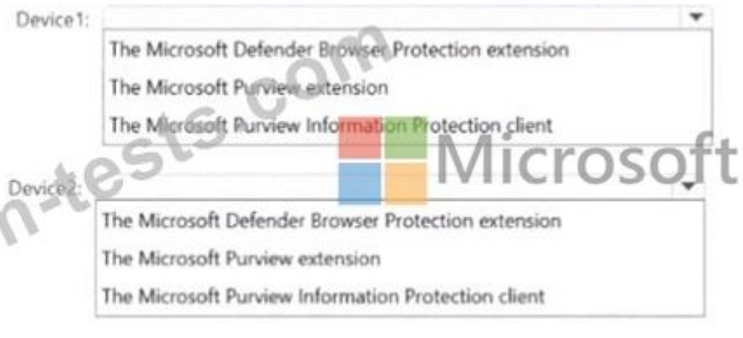
You have a Microsoft 36S ES subscription that contains two Windows devices named Devicel1and Device2 Device1 has the default browser set to Microsoft Edge. Devke2 has the default browser set to Google Chrome.

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.

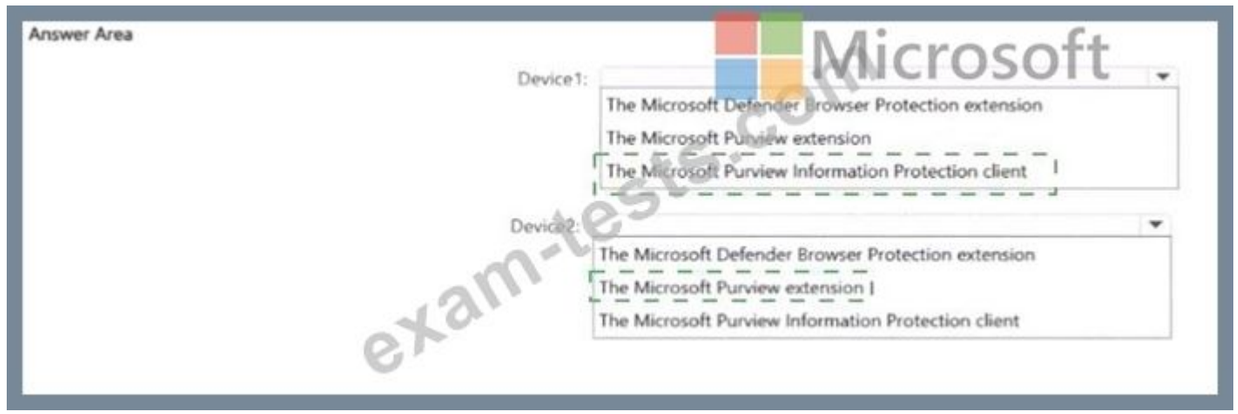
What should you deploy to each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:



Explanation:

NEW QUESTION: 79

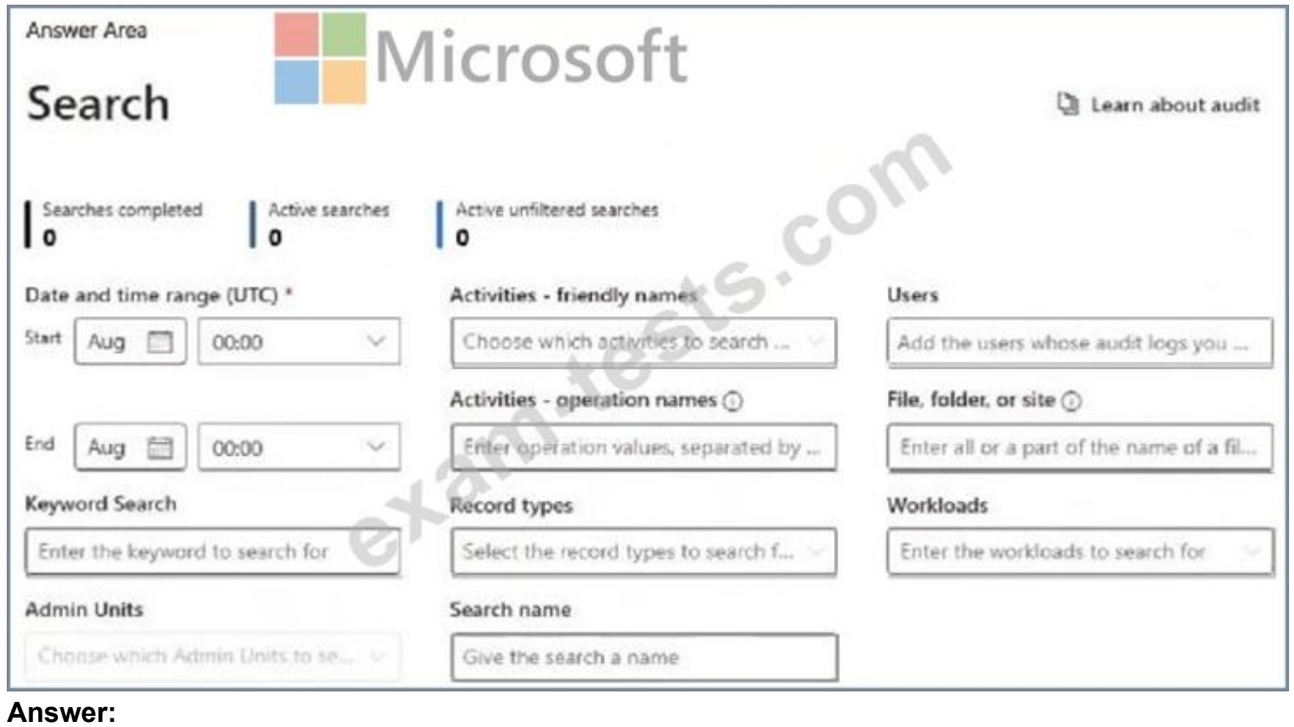
You have a Microsoft 365 subscription.

You plan to deploy an audit log retention policy.

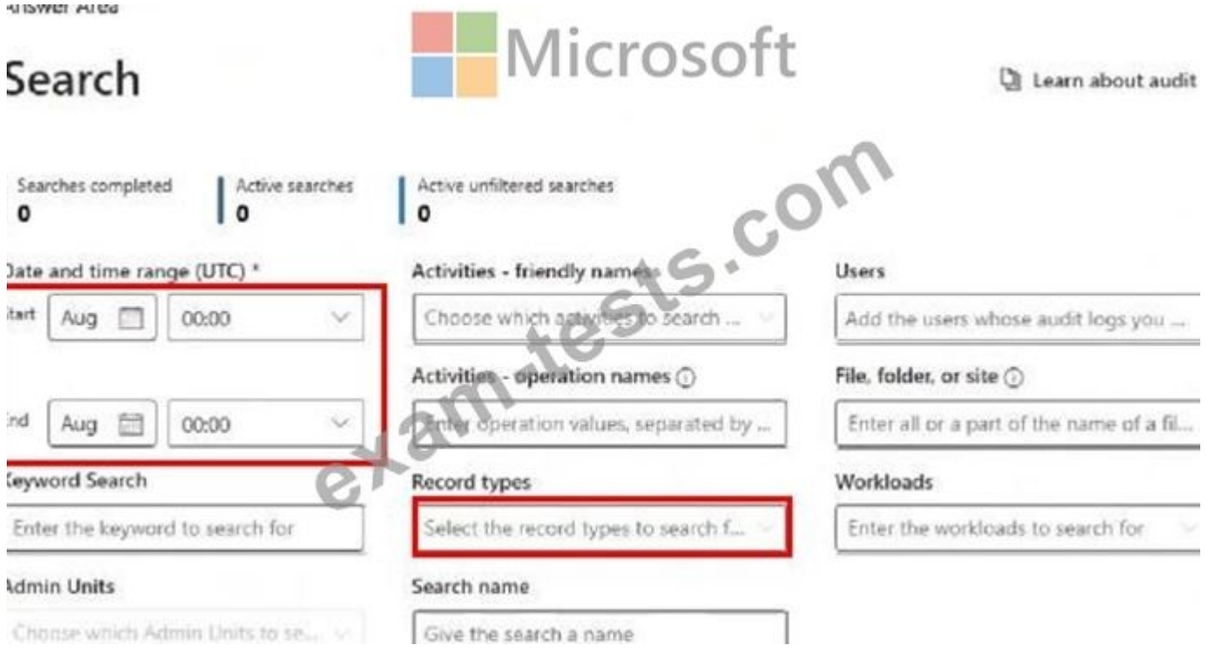
You need to perform a search to validate whether the policy will be applied to the intended entries.

Which two fields should you configure for the search? To answer, select the appropriate fields in the answer area.

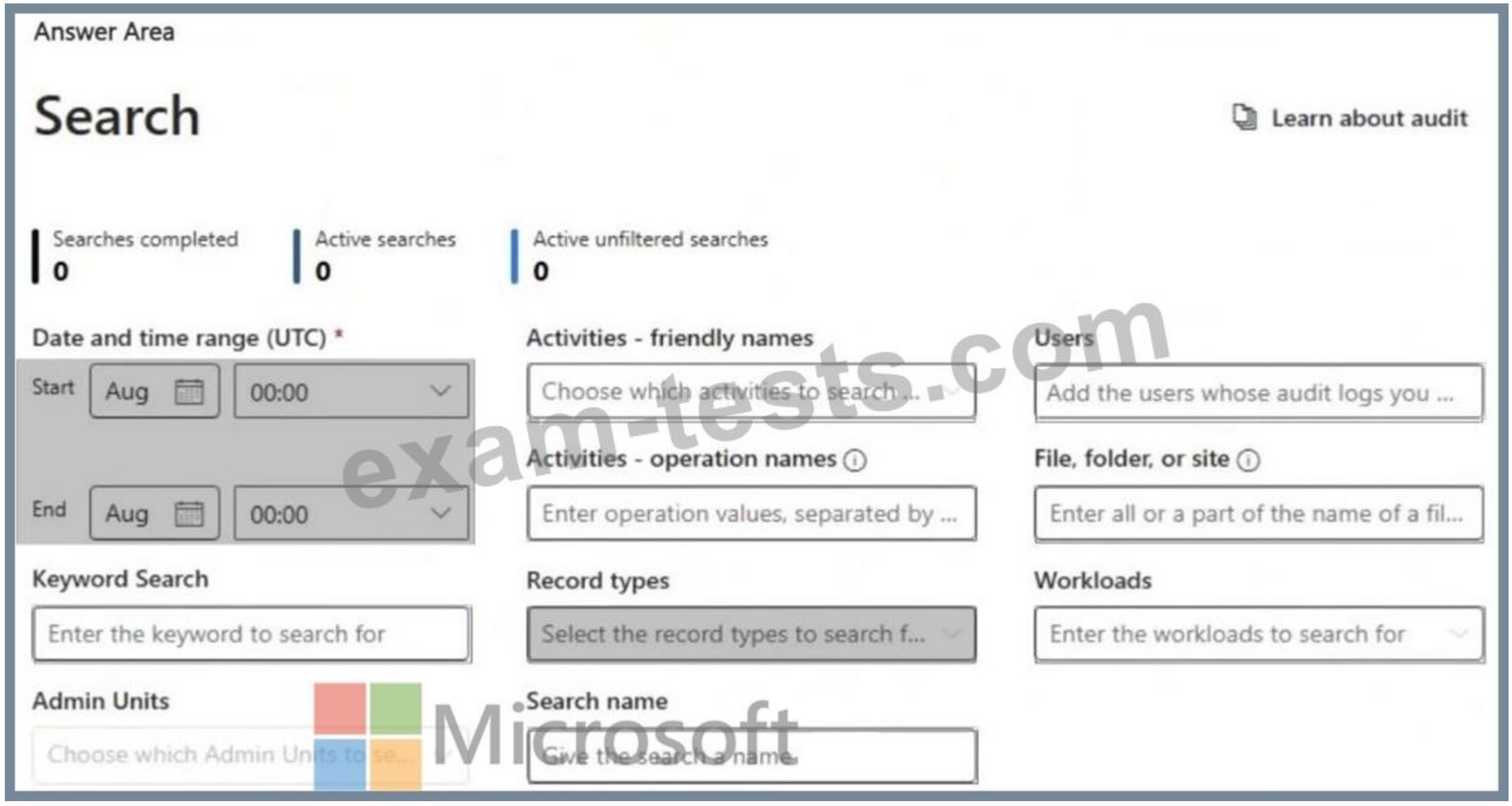
NOTE: Each correct selection is worth one point.



Answer:



Answer Area



NEW QUESTION: 80

You have a Microsoft 365 E5 tenant that contains a user named User1. User1 is assigned the Compliance Administrator role. User1 cannot view the regular expression in the IP Address sensitive info type. You need to ensure that User! can view the regular expression. What should you do?

A. Assign Used to the Reviewer role group

B. Create a copy of the IP Address sensitive info type and instruct User1 to edit the copy.

C. Instruct User1 to use the Test function on the sensitive info type.

D. Assign User1 the Global Reader role.

Answer: (SHOW ANSWER)

Step 1 - Problem statement

User1 has the Compliance Administrator role but cannot view the regular expression in the built-in IP Address sensitive info type.

This is expected because:

Microsoft provides a large set of built-in sensitive info types (SITs).

For these built-in SITs, the underlying regular expressions, keywords, or detection logic are not exposed to administrators for security reasons.

As a result, even with Compliance Administrator privileges, User1 cannot directly see or modify the regex in the built-in IP Address SIT.
Step 2 - Microsoft solution
To view or modify the regex:
You must create a copy of the built-in SIT.
Once copied, the new custom SIT allows you to edit and view the regex and supporting elements.
This is the only supported way to customize or examine the detection logic.
Reference: Create a custom sensitive information type
"You can't directly modify the definitions of built-in sensitive information types, but you can create a copy of an existing SIT and then edit it." Step 3 - Why not the other options?
A). Reviewer role group # Reviewers are for records management/discovery, not SIT regex visibility.
C). Test function # Allows you to test SIT detection but does not reveal the regex.
D). Global Reader role # Read-only access, does not expose regex definitions either.

NEW QUESTION: 81
You have a Microsoft J65 E5 subscription. You plan to implement retention policies for Microsoft Teams.
Which item types can be retained?
A. embedded images
B. voice memos from the Teams mobile client
C. code snippets
Answer: (SHOW ANSWER)

NEW QUESTION: 82
You have a Microsoft 365 E5 tenant that contains a sensitivity label named label1.
You plan to enable co-authoring for encrypted files.
You need to ensure that files that have label1 applied support co-authoring.
Which two settings should you modify? To answer, select the settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

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 ⓘ

A number of days after label is applied

Access expires this many days after the label is applied

90

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

Assign permissions

0 items

Users and groups	Permissions	Edit	Delete

No data available

☑ Use dynamic watermarking ⓘ

Customize text (optional)

☑ Use Double Key Encryption ⓘ

https://sts.contoso.com

Answer:

Answer Area

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 ⓘ

A number of days after label is applied

Access expires this many days after the label is applied

90

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

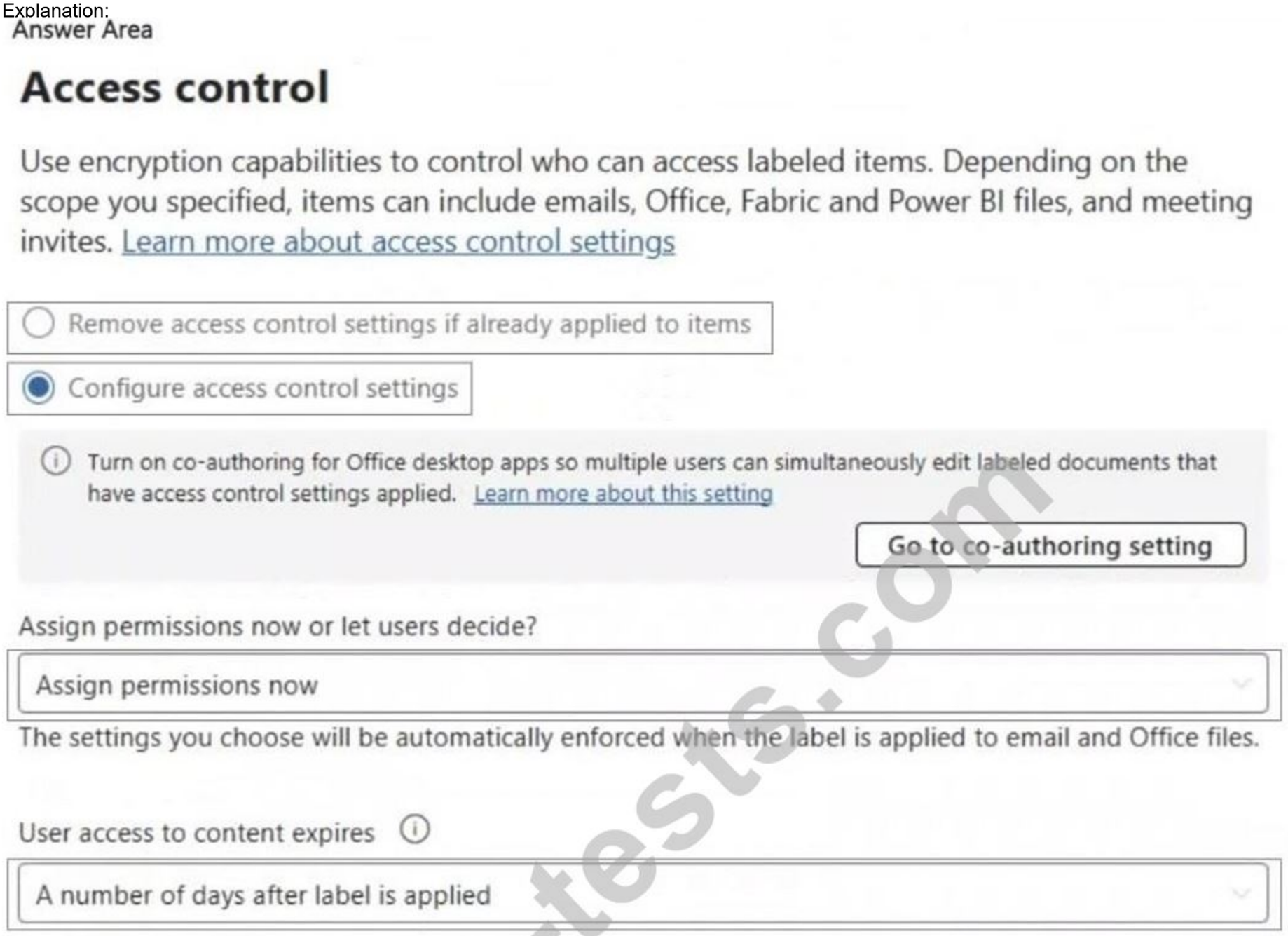
Assign permissions

0 items

Users and groups	Permissions	Edit	Delete
No data available			

Explanation:

Answer Area



Access expires this many days after the label is applied

90

Allow offline access

Always

Assign permissions to specific users and groups *

Assign permissions

0 items

Users and groups	Permissions	Edit	Delete

No data available

NEW QUESTION: 83

You have a Microsoft 365 subscription.

You are evaluating whether to use the Microsoft Purview auditing solutions shown in the following table.

Name	Description
Solution1	Control auditing by using audit log retention policies.
Solution2	Export audit records to a CSV file.
Solution3	Retain audit logs for one year.

You plan to implement Microsoft Purview Audit (Standard).

Which solutions can you use?

A. Solution1, Solution2, and Solution3

B. Solution1 and Solution2 only

C. Solution3 only

D. Solution2 and Solution3 only

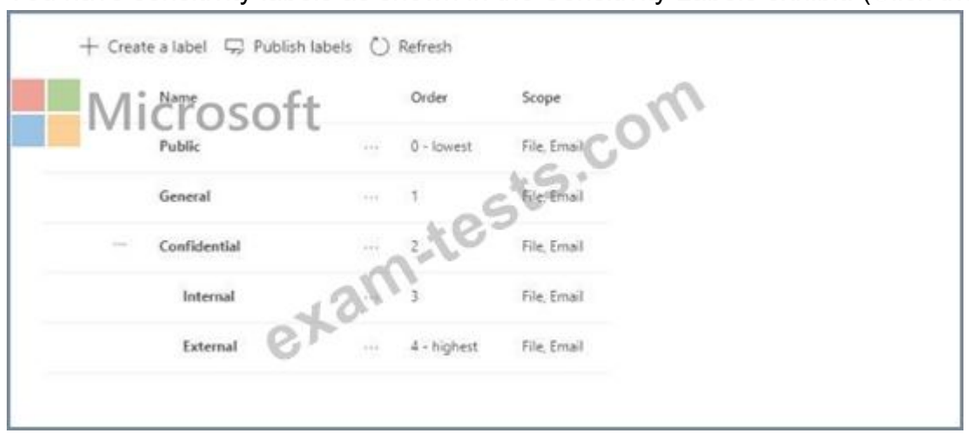
E. Solution2 only

Answer: E (LEAVE A REPLY)

NEW QUESTION: 84

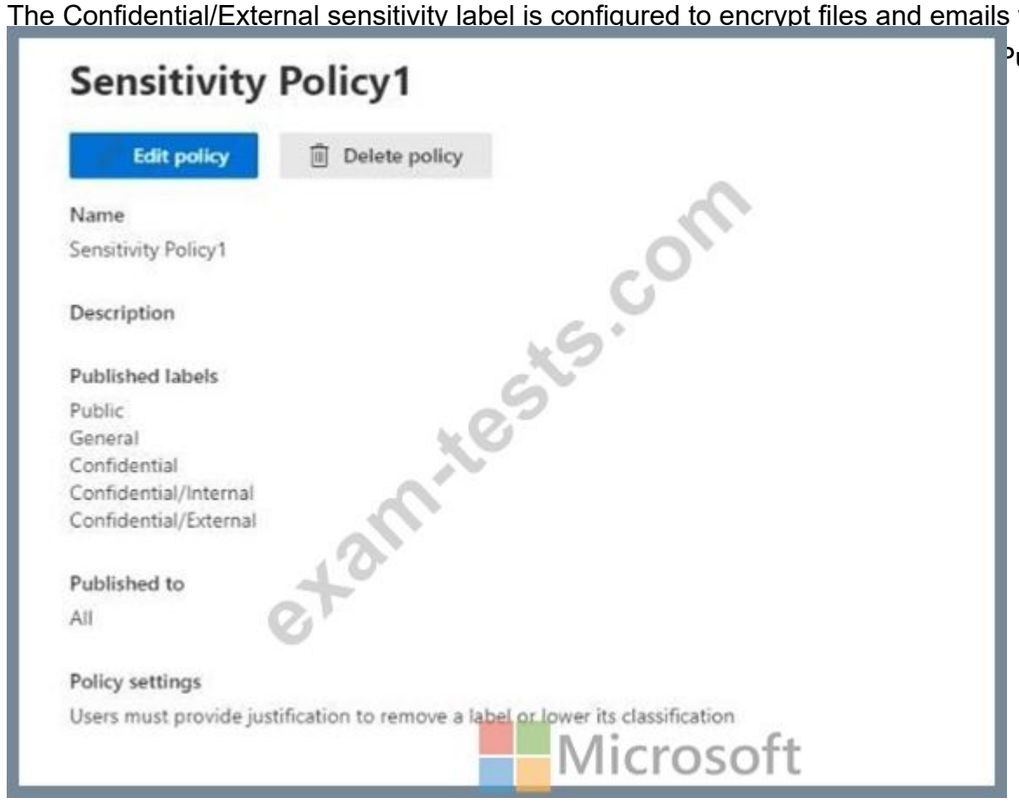
You have a Microsoft 365 E5 tenant.

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.

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:

Explanation:

NEW QUESTION: 85

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 Area

Search

Learn about audit

Searches completed
0

Active searches
0

Active unfiltered searches
0

Date and time range (UTC) *

Start Aug 00:00

End Aug 00:00

Activities - friendly names
Choose which activities to search ...

Activities - operation names
Enter operation values, separated by ...

Users
Add the users whose audit logs you ...

File, folder, or site
Enter all or a part of the name of a fil...

Keyword Search
Enter the keyword to search for

Record types
Select the record types to search f...

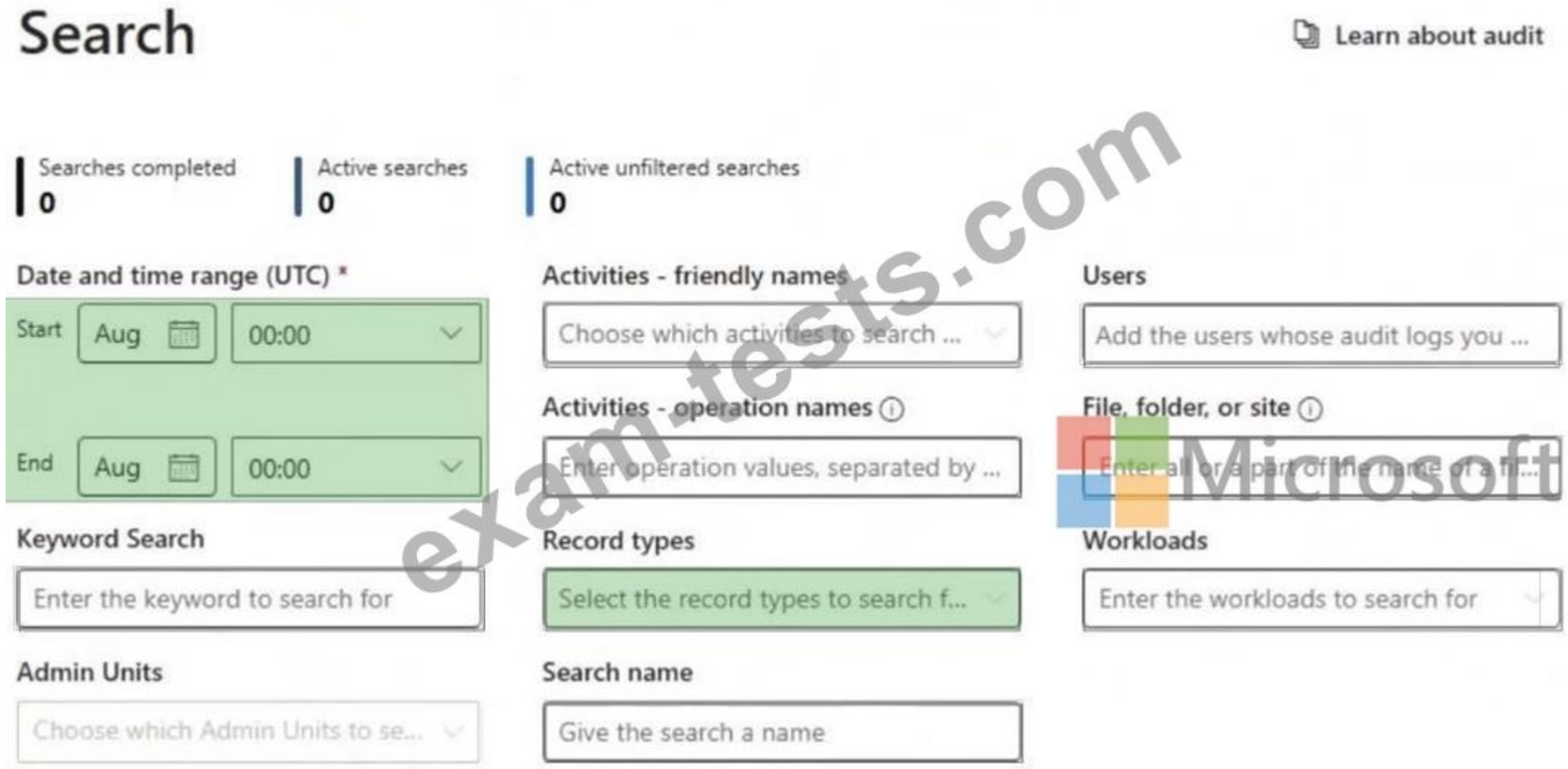
Workloads
Enter the workloads to search for

Admin Units
Choose which Admin Units to se...

Search name
Give the search a name

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: 86

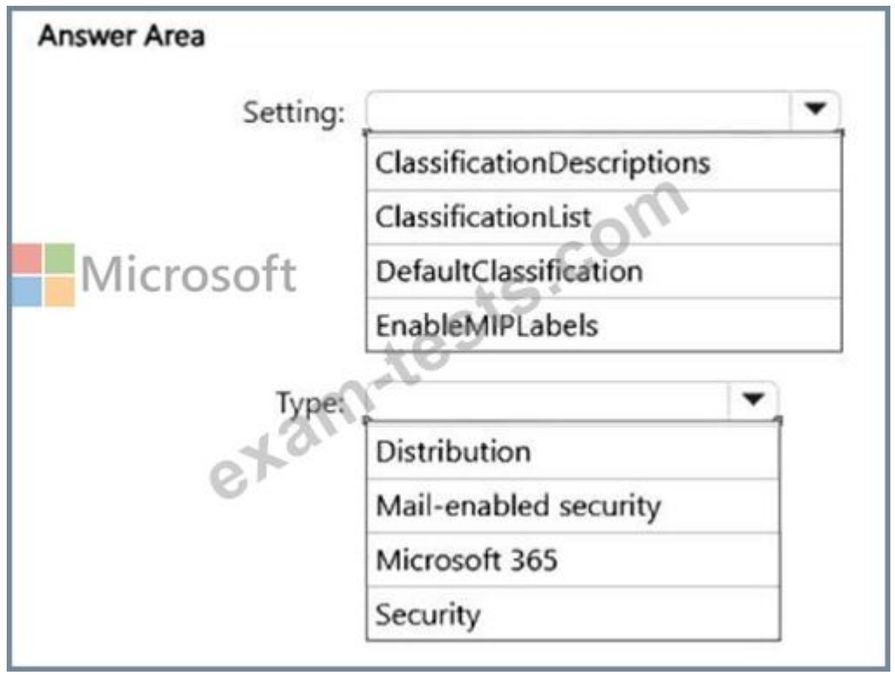
Hotspot Question

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

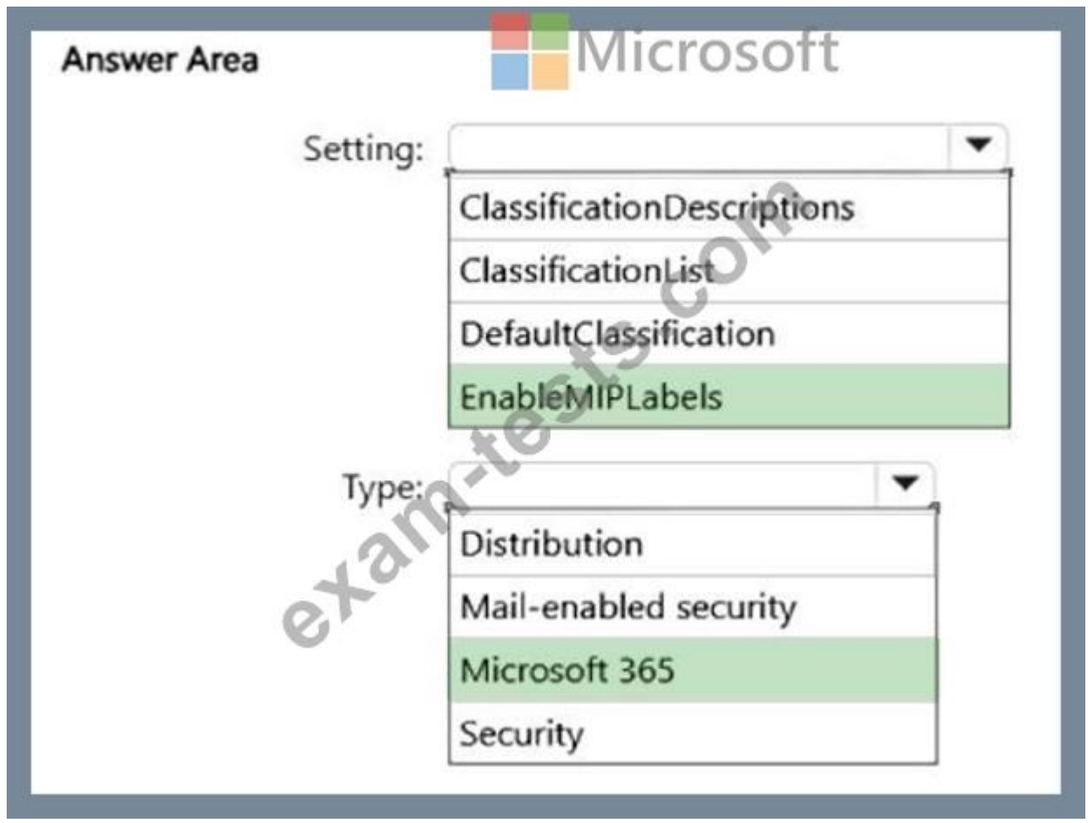
You plan to create a Microsoft Entra group named Group1 and assign Sensitivity1 to Group1.

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

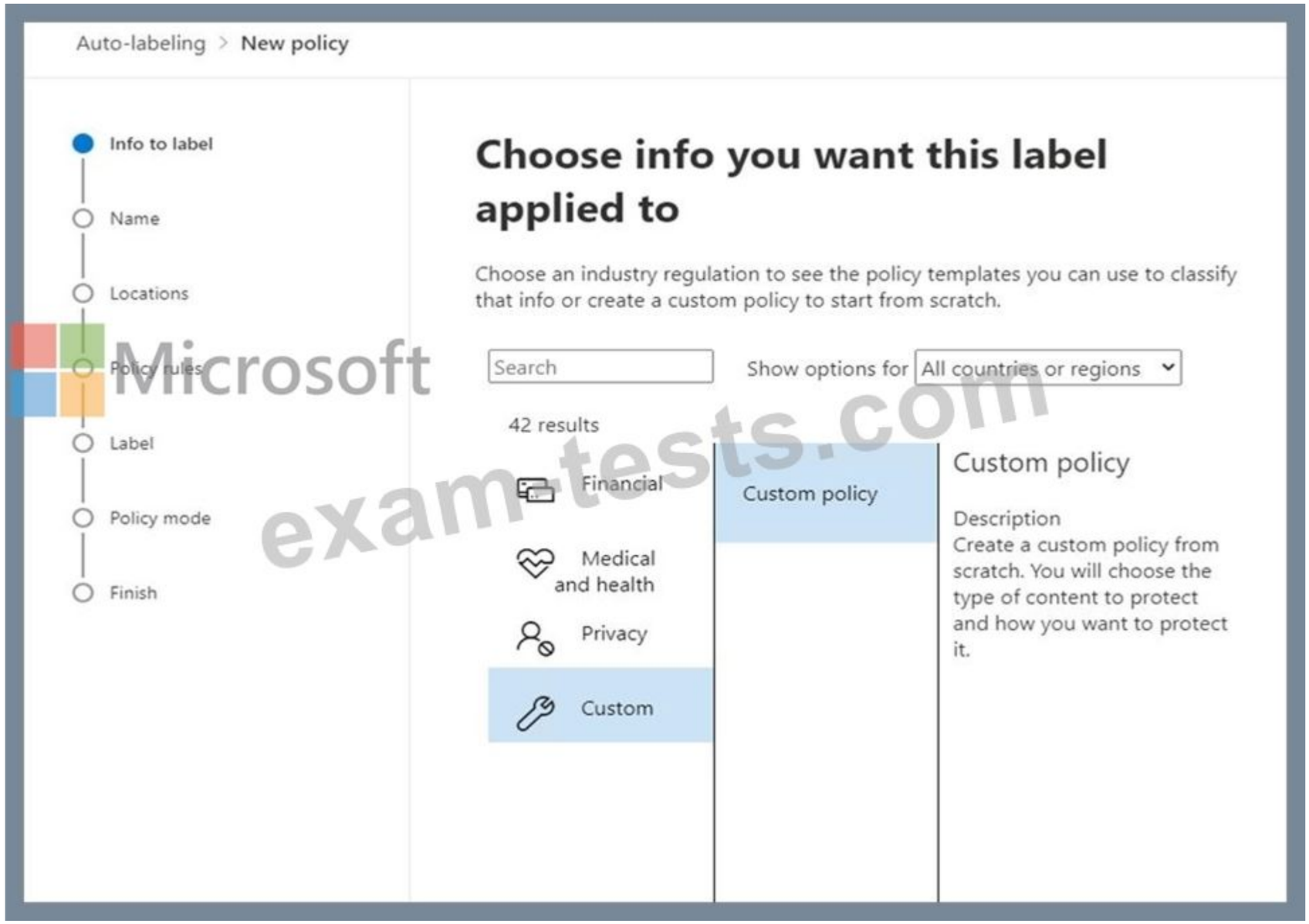
NEW QUESTION: 87
You have a Microsoft 36S ES subscription.
From the Microsoft Purview Data Security Posture Management for Al portal, you review the recommendations for Al data security You plan to create a one-click policy to block elevated risk users from pasting or uploading sensitive data to Al websites How will the policy be configured? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.
Answer Area

Answer:

Explanation:

Answer Area

NEW QUESTION: 88
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 5
You need to simulate applying the Confidential - Finance label to all the content in the Exchange emails, the SharePoint sites, and the OneDrive accounts that contain the Credit Card Number sensitive info type.
Answer:
Simulation mode is supported for auto-labeling policies and woven into the workflow. You can't automatically label documents and emails until your policy has run at least one simulation.
Workflow for an auto-labeling policy:
1. Create and configure an auto-labeling policy.
2. Run the policy in simulation mode, which can take 12 hours to complete. The completed simulation triggers an email notification that's sent to the user configured to receive activity alerts.
3. Review the results, and if necessary, refine your policy.
4. Repeat step 3 as needed.
5. Deploy in production.
Creating an auto-labeling policy
Step 1: Sign in to the Microsoft Purview portal > Solutions > Information Protection > Policies > Auto-labeling policies.
Step 2: Select + Create auto-labeling policy. This starts the New policy configuration:



Step 3: For the Choose a label to auto-apply page: Select + Choose a label, select a label from the Choose a sensitivity label pane, and then select Next.

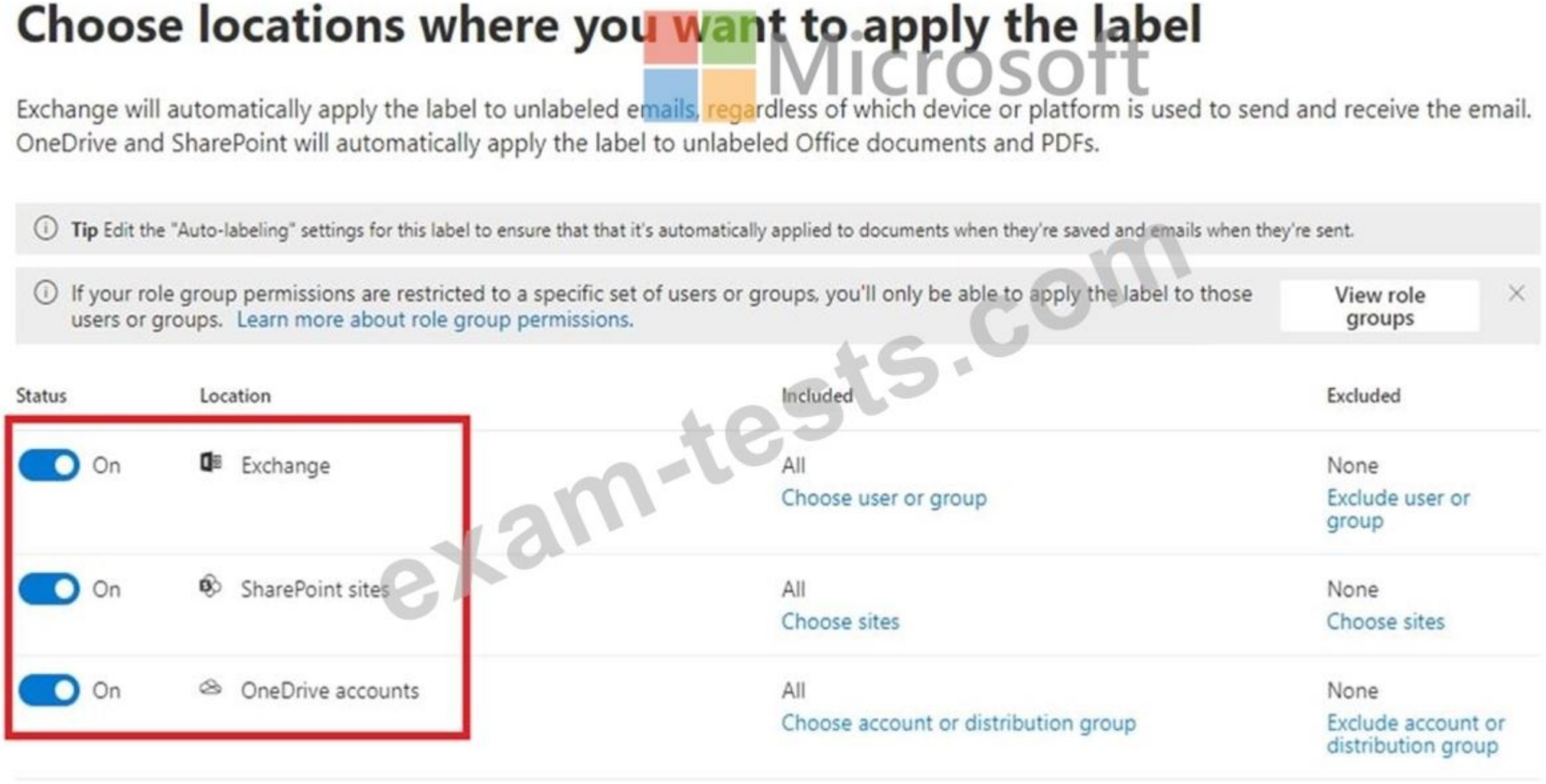
Step 4: For the page Choose info you want this label applied to: Select one of the templates, such as Financial or Privacy [Select Confidential - Finance label]. You can refine your search by using the search or dropdown box for countries or regions. Or, select Custom policy if the templates don't meet your requirements. Select Next.

Step 5: For the page Name your auto-labeling policy: Provide a unique name, and optionally a description to help identify the automatically applied label, locations, and conditions that identify the content to label.

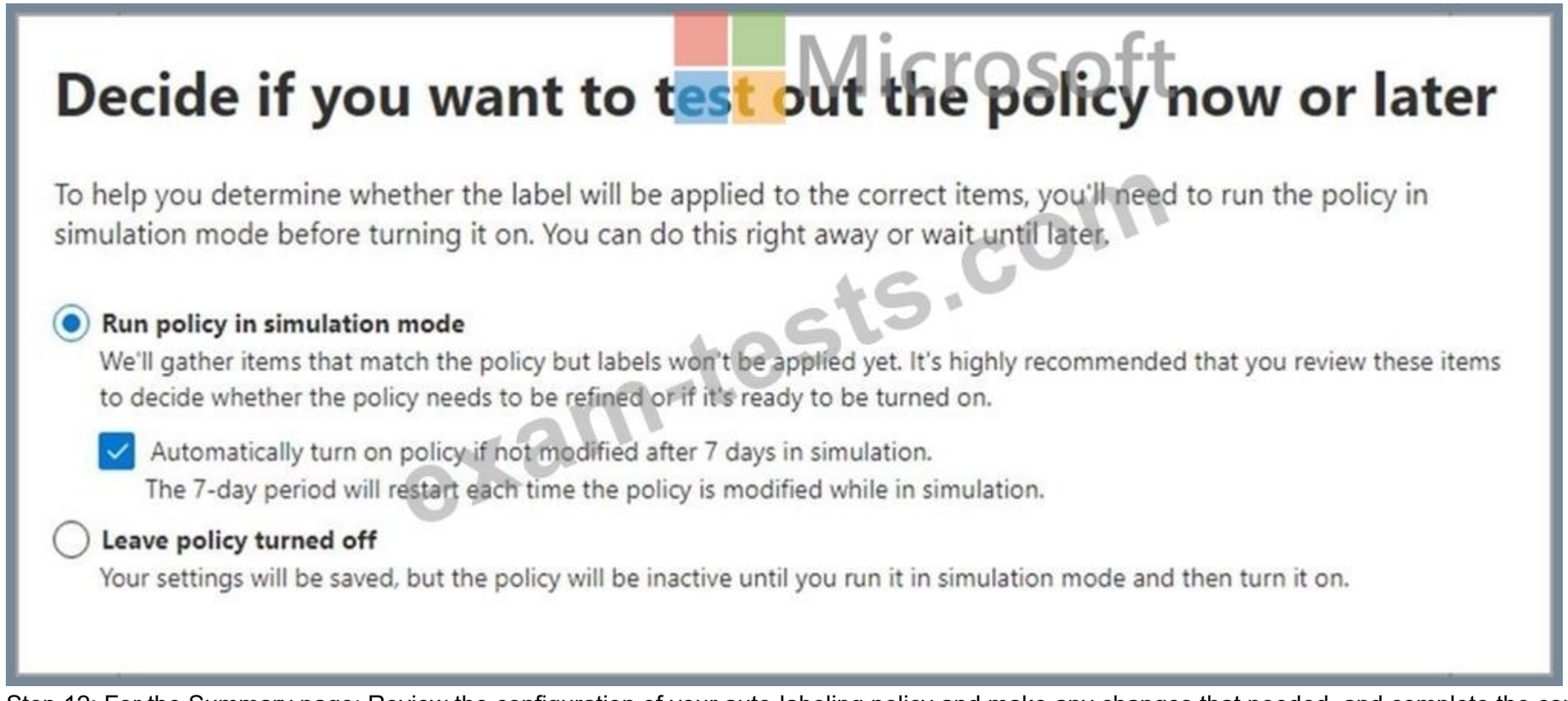
Step 6: For the page Assign admin units: [Keep default]

If you don't want to restrict the policy by using administrative units, or your organization hasn't configured administrative units, keep the default of Full directory.

Step 7: For the page Choose locations where you want to apply the label: Select and specify locations for Exchange, SharePoint, and OneDrive.



Step 8: For the Set up common or advanced rules page: Keep the default of Common rules to define rules that identify content to label across all your selected locations. If you need different rules per location, including some rules that are only available for Exchange, or SharePoint sites and OneDrive accounts, select Advanced rules. Then select Next. [select Advanced rules. Then select Next]
8a. To select a sensitive information type or trainable classifier as a condition, under Content contains, select Add, and then choose Sensitive info types or Trainable classifiers.
8b. Select the the Credit Card Number sensitive info type.
Step 9: Depending on your previous choices, you'll now have an opportunity to create new rules by using conditions and exceptions. [Skip] Step 10: If your policy includes the Exchange location: Specify optional configurations [Skip] Step 11: For the Decide if you want to test out the policy now or later page: Select Run policy in simulation mode if you're ready to run the auto-labeling policy now, in simulation mode.



Step 12: For the Summary page: Review the configuration of your auto-labeling policy and make any changes that needed, and complete the configuration.

Reference:

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

NEW QUESTION: 89

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: 90

Hotspot Question

You have a Microsoft 365 E5 subscription that contains four users named User1, User2, User3, and User4 and a file named File1.docx.

To File1, you apply a sensitivity label that has the permissions 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

Microsoft 365 Copilot can summarize File1 for **[answer choice]**.

- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3 and User4

For **[answer choice]**, Microsoft 365 Copilot can reference File1 by using a link.

- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3 and User4

Answer:

Answer Area

Microsoft 365 Copilot can summarize File1 for **[answer choice]**.

- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3 and User4

For **[answer choice]**, Microsoft 365 Copilot can reference File1 by using a link.

- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3 and User4

Explanation:
Box 1: User1 and User2 only
For File1:
User1 is Co-Owner. User1 - Yes
User2 is Co-Author. User2 - Yes.
User3 is Reviewer. User3 - No.
A user with "Reviewer" permissions on a document, folder, or site does not have extract permissions.
User4 is Viewer. User4 - No.
A user with "Vewer" permissions on a document, folder, or site does not have extract permissions.
Note: For Microsoft 365 Copilot to summarize data within a file, the user must have both the EXTRACT and VIEW usage rights on the sensitivity label applied to that file, according to Microsoft Learn. This ensures that Copilot can access and process the file's content for summarization purposes. If a file is encrypted using Azure Rights Management without a sensitivity label, the same permissions (EXTRACT and VIEW) are still required for Copilot to function.
Box 2: User1, User2, User3 and User4.
User1 is Co-Owner. User1 - Yes
User2 is Co-Author. User2 - Yes.
User3 is Reviewer. User3 - Yes.
In Microsoft 365, a Reviewer of a file can reference that file, and potentially other files, within their comments or suggestions. Reviewers can use @mentions to tag individuals, including the file's author or other reviewers, to draw attention to specific points or sections within the document.
Additionally, Microsoft 365 Copilot allows reviewers to reference files, emails, and meetings when creating, reviewing, or finalizing documents.
User4 is Viewer. User4 - Yes.
In Microsoft 365, a user with Viewer permissions for a file can indeed reference that file in various ways, including using it as a source for Microsoft Copilot, or simply copying and pasting the link to share with others.
Reference:
https://techcommunity.microsoft.com/blog/microsoft365insiderblog/expanding-reference-capabilities-with-microsoft-365-copilot-in-word/4406054

NEW QUESTION: 91
You have a Microsoft 36S ES subscription that contains the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	macOS
Device4	Android

You plan to implement inside' risk management and capture forensic evidence Which devices support the collection of forensic evidence, and what should you do lo prepare each supported device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

The question is about Insider Risk Management forensic evidence collection in Microsoft 365 E5 (Microsoft Purview).

Step 1 - Which devices are supported?

According to Microsoft documentation, forensic evidence collection for insider risk investigations is supported only on:

Windows 10
Windows 11
It is not supported on:
macOS
Android
iOS
Reference: Forensic evidence collection in Microsoft Purview Insider Risk Management
So, only Device1 (Windows 11) and Device2 (Windows 10) qualify.
Step 2 - What preparation is needed?
For forensic evidence to be collected, supported devices must:
Be onboarded to Microsoft Purview (via Microsoft Defender for Endpoint integration).
Have the Microsoft Purview client installed.
This enables capture of user actions such as file copies, USB transfers, printing, etc., to provide forensic evidence for insider risk alerts.
Correct option: Onboard the devices to Microsoft Purview and install the Microsoft Purview client

NEW QUESTION: 92
You need to meet the technical requirements for the creation of the sensitivity labels.
To which user or users must you assign the Sensitivity Label Administrator role?
A. Admin1 only
B. Admin1 and Admin4 only
C. Admin1 and Admin5 only
D. Admin1, Admin2, and Admin3 only
E. Admin1, Admin2, Admin4, and Admin5 only
Answer: D (LEAVE A REPLY)
To meet the requirement that all administrative users must be able to create Microsoft 365 sensitivity labels, we need to assign the Sensitivity Label Administrator role to the correct users.
Sensitivity Label Administrator Role Responsibilities
This role allows users to:
Create and manage sensitivity labels in Microsoft Purview.
Publish and configure auto-labeling policies.
Modify label encryption and content marking settings.
Review of Admin Roles from the Table:

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

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

NEW QUESTION: 93
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 of Site1
Admin1	SharePoint Administrator role

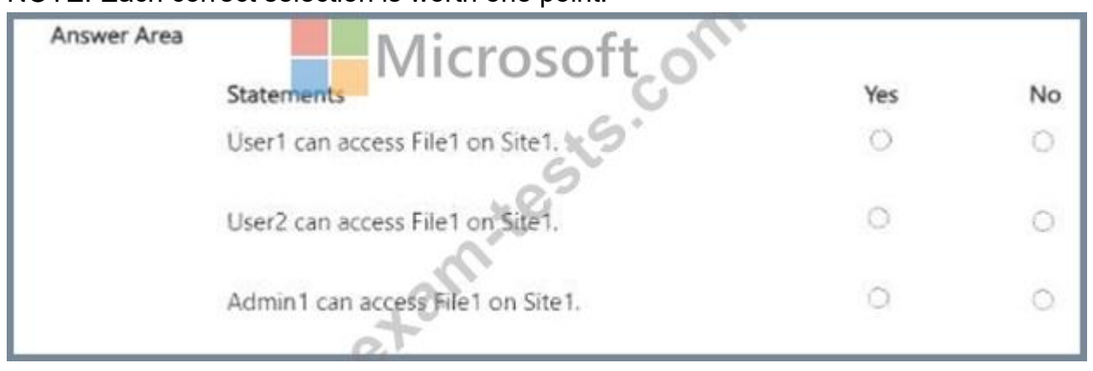
You have a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.

You apply DLP1 to Site1.

User1 uploads a file named File1 to Site1. File1 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:

Answer Area

Statements	Yes	No
User1 can access File1 on Site1.	○	●
User2 can access File1 on Site1.	○	○
Admin1 can access File1 on Site1.	●	○

NEW QUESTION: 94

You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1. Site1 has a document library that contains the files shown in the following table.

Name	File type	Created on
File1	DOCX	December 1, 2023
File2	XLSX	February 5, 2024
File3	PNG	May 4, 2023

From the Microsoft Purview compliance portal, for Site1 you create a content search named Search1 that has the date in the YYYY-MM-DD format as 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 Area

Statements	Yes	No
File1 is included in the Search1 results.	○	○
File2 is included in the Search1 results.	○	○
File3 is included in the Search1 results.	○	○

Answer:

Explanation:

NEW QUESTION: 95

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 and Device2 only
B. Device only
C. Device2 and Device3 only
D. Device2 only
E. Device1, Device2 and Device3
Answer: (SHOW ANSWER)

NEW QUESTION: 96

You create a retention label policy named Contoso_Policy that contains the following labels:
* 10 years then delete
* 5 years then delete
* Do not retain
Contoso.Policy is applied to content in Microsoft SharePoint Online sites.
After a couple of days, you discover the following messages on the Properties page of the label policy:
* Status: Off (Error)
* It's taking longer than expected to deploy the policy
You need to reinitiate the policy.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Step 1 - Review scenario

You created a retention label policy Contoso_Policy.

Status shows Off (Error) with message: "It's taking longer than expected to deploy the policy." Requirement: Reinitiate the policy.

Step 2 - Correct PowerShell cmdlet

To manage retention label policies in Microsoft Purview (compliance), the cmdlet is:

Set-RetentionCompliancePolicy

Other cmdlets:

Set-RetentionPolicy # Legacy Exchange Online retention policies, not Purview label policies.

Start-EdgeSynchronization # Sync for Edge Transport servers, not retention.

Start-RetentionAutoTagLearning # Used for auto-tagging learning, not relevant here.

Step 3 - Correct parameter

To force redistribution of a retention label policy when deployment fails, the parameter is:

-RetryDistribution

Other options:

-ForceFullSync and -FullCrawl # Apply to search/crawl, not retention.

-Train # Related to auto-tagging learning models, not retention.

Final Verified Answer

Set-RetentionCompliancePolicy -id Contoso_Policy -RetryDistribution

Reference:

Set-RetentionCompliancePolicy (Microsoft Purview PowerShell)

NEW QUESTION: 97

HOTSPOT

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

Name	Platform
Config1	Windows 11
Config2	macOS
Config3	Android

Each configuration uses either Google Chrome or Firefox as a default browser.

You need to implement Microsoft Purview and deploy the Microsoft Purview browser extension to the configurations.

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

NOTE: Each correct selection is worth one point.

Answer Area

Google Chrome:

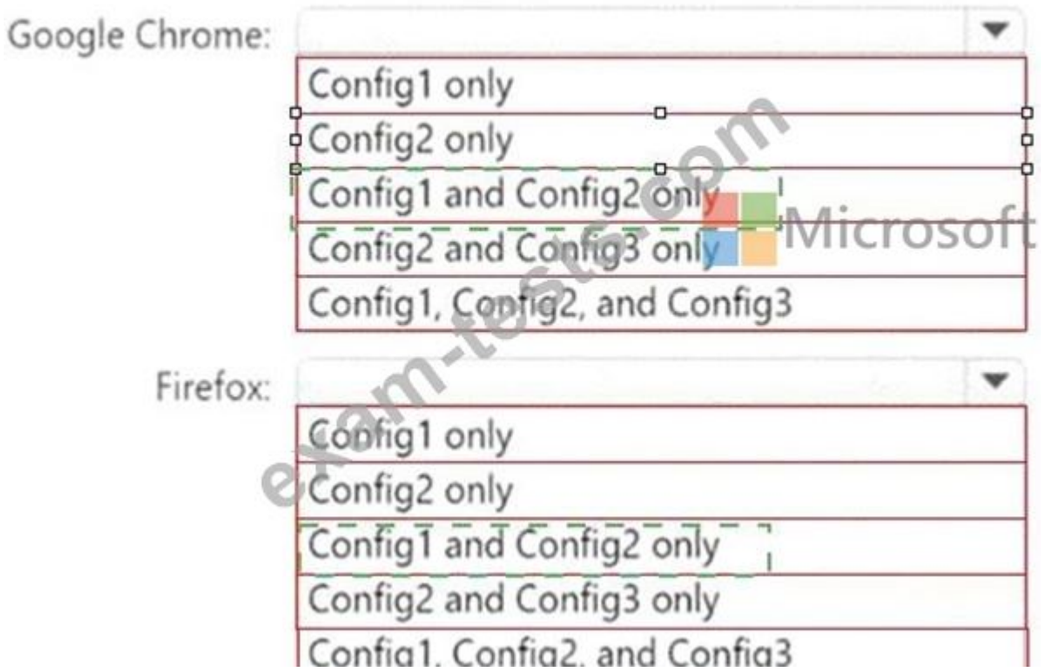
- Config1 only
- Config2 only
- Config1 and Config2 only
- Config2 and Config3 only
- Config1, Config2, and Config3

Firefox:

- Config1 only
- Config2 only
- Config1 and Config2 only
- Config2 and Config3 only
- Config1, Config2, and Config3

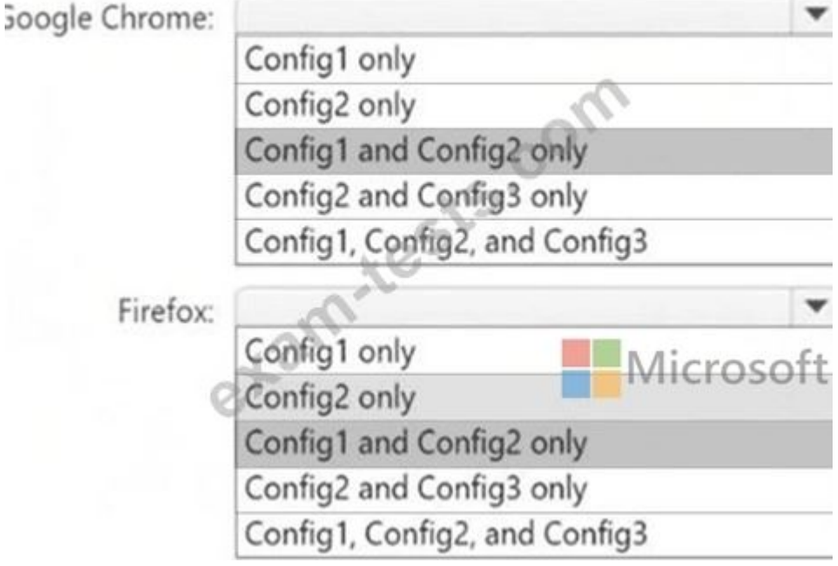
Answer:

Answer Area



Explanation:

Answer Area



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: 98

DRAG DROP

You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.

You need to create a custom sensitive info type. The solution must meet the following requirements:

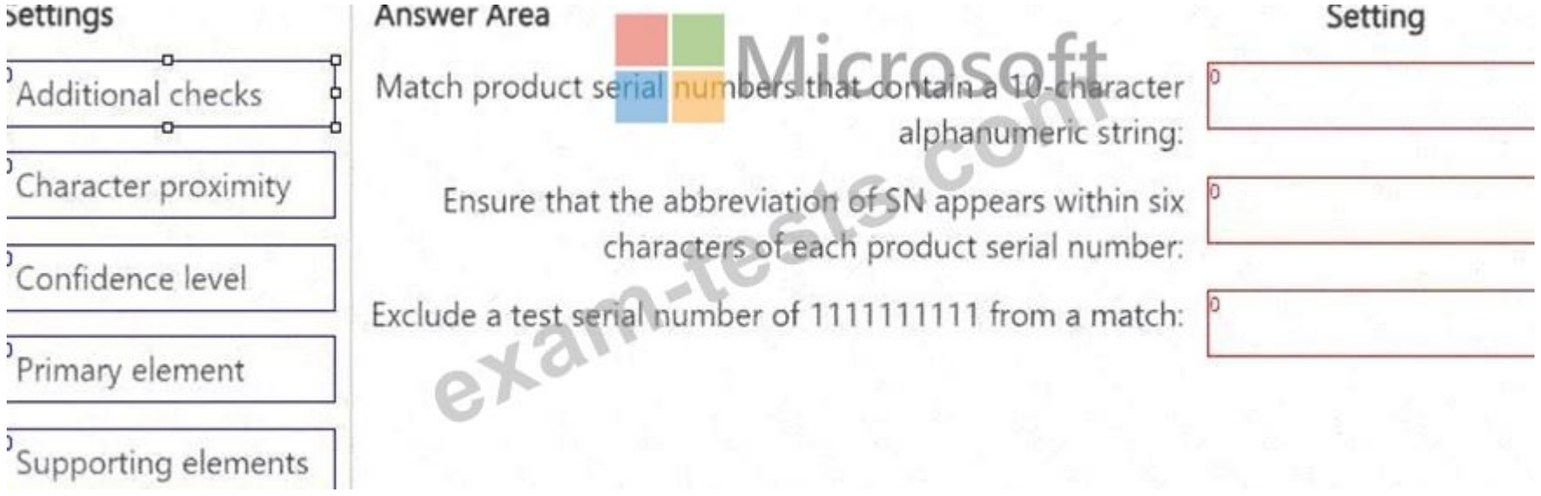
Match product serial numbers that contain a 10-character alphanumeric string.

Ensure that the abbreviation of SN appears within six characters of each product serial number.

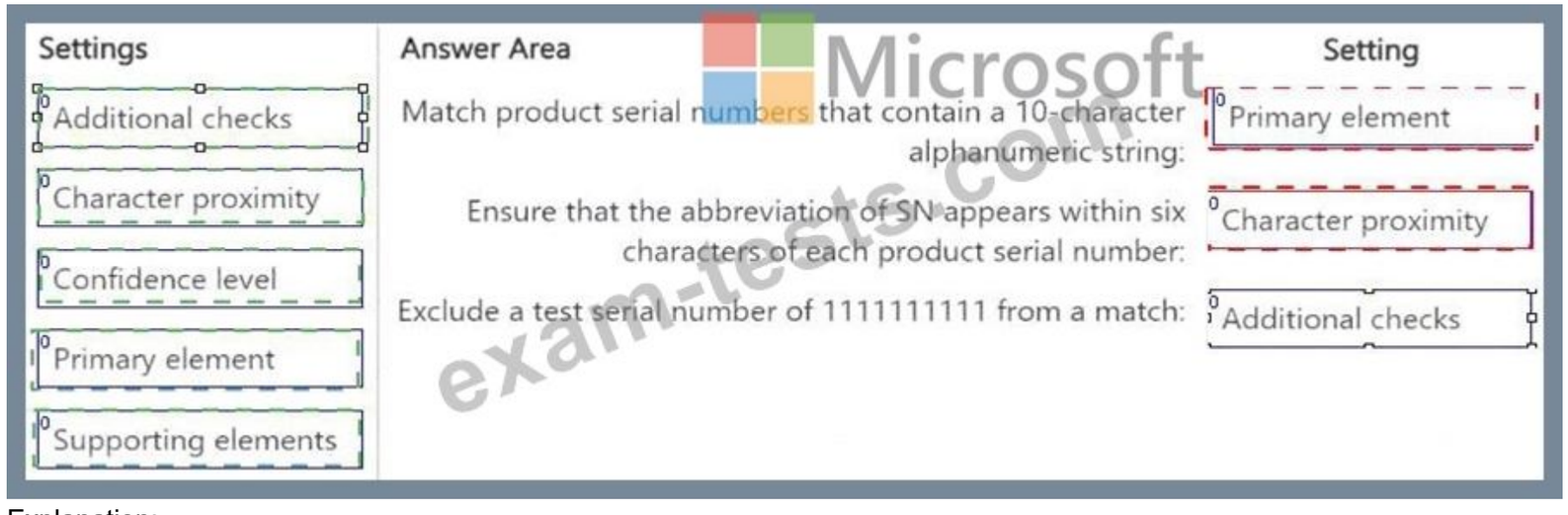
Exclude a test serial number of 1111111111 from a match.

Which pattern settings should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

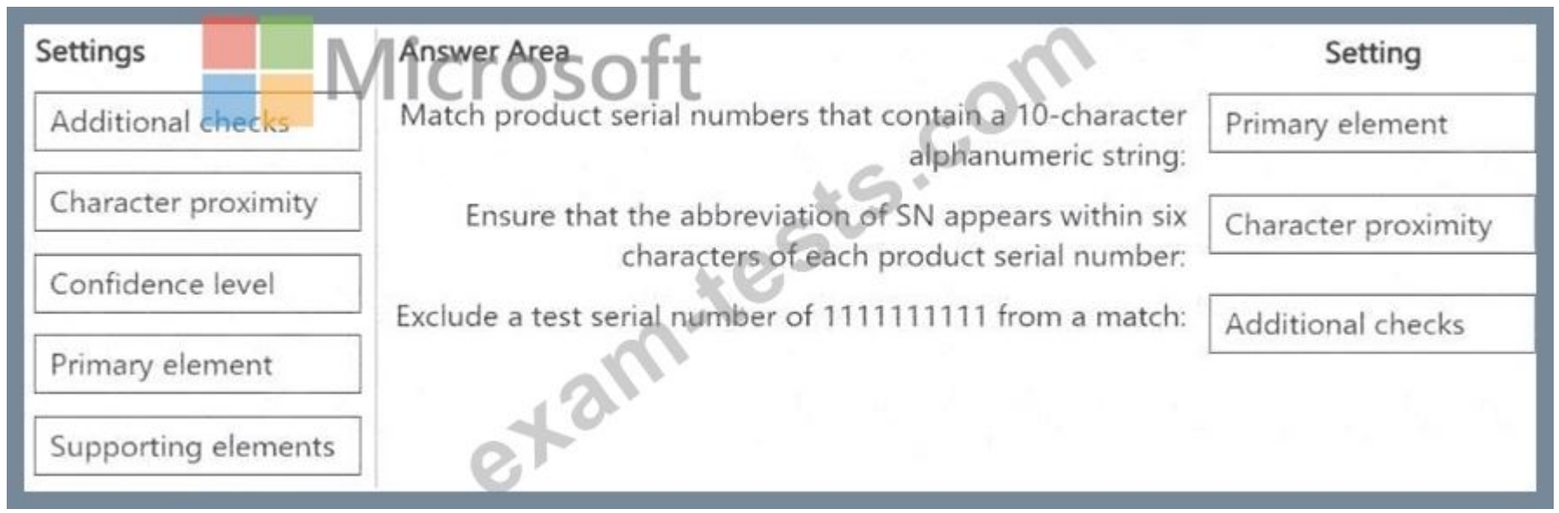
NOTE: Each correct selection is worth one point.



Answer:



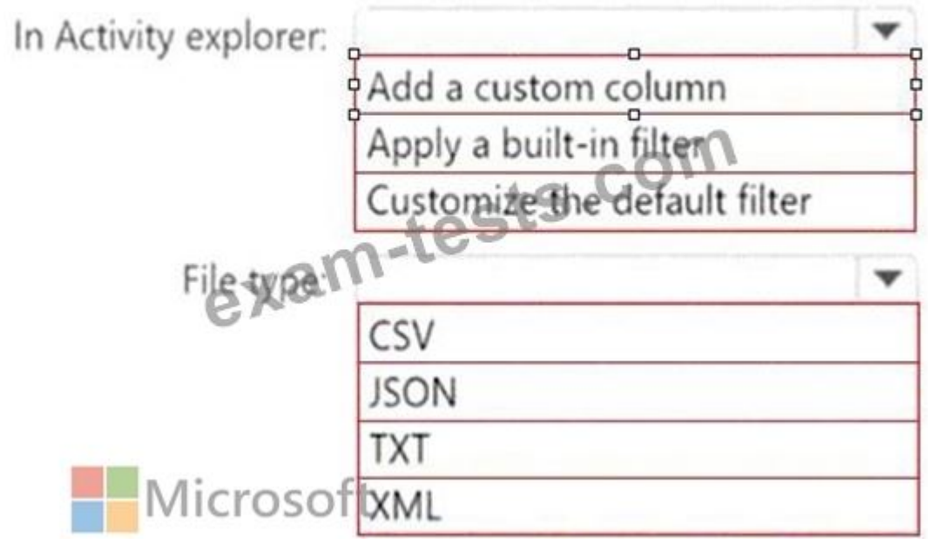
Explanation:



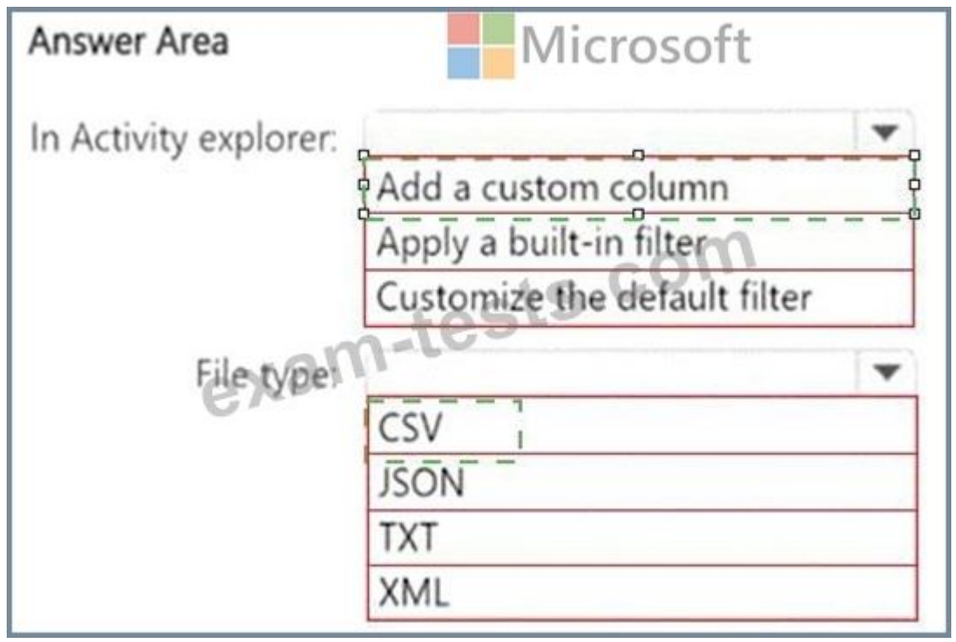
NEW QUESTION: 99
You have a Microsoft 365 subscription that uses Microsoft Purview Insider Risk Management.
The subscription has a policy named Policy1 that detects potential insider risks based on exfiltration activities.
You discover multiple high-severity alerts for Policy1.
When you review the alerts, you discover that the activities that triggered alerts have a low-risk score.
You need to ensure that you only receive high-severity alerts for activities that have a high-risk score.
What should you modify in Policy1?
A. the time range
B. the triggers
C. the indicators
D. the notification settings
Answer: C (LEAVE A REPLY)
To ensure that you receive high-severity alerts only for activities that carry a high-risk score, you need to change the indicators setting.
In Microsoft Purview Insider Risk Management, indicators define the specific risky activities being tracked (e.g., downloading large volumes of files or printing sensitive documents). Within the policy's indicator settings, you can adjust the thresholds from "default" to "custom". This allows you to fine-tune and elevate the volume or frequency required for an activity to trigger an alert, directly linking the overall policy risk score and severity to high-risk activities instead of low-risk, everyday behaviors.
Reference:
https://learn.microsoft.com/en-us/purview/insider-risk-management-policies

NEW QUESTION: 100
HOTSPOT
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.
You plan to export DLP activity by using Activity explorer.
The exported file needs to display the sensitive info type detected for each DLP rule match.
What should you do in Activity explorer before exporting the data, and in which file format is the file exported? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:



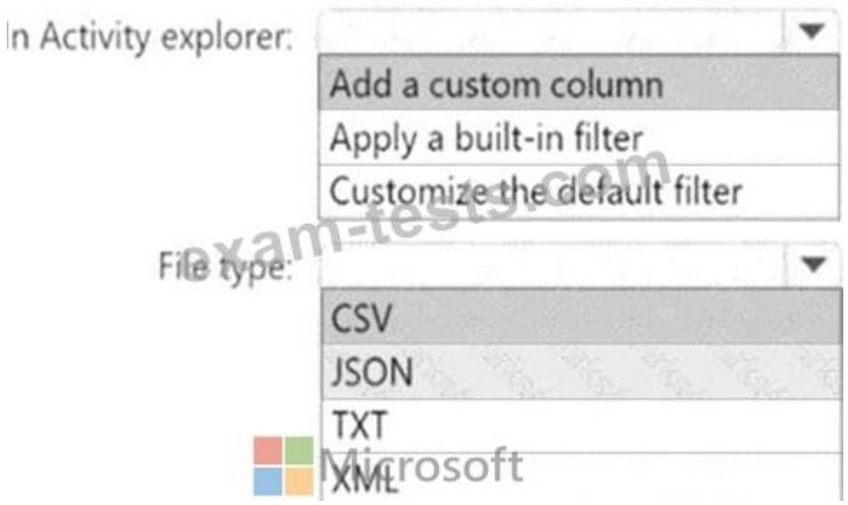
Explanation:

Box 1: To include the sensitive info type detected for each DLP rule match, you need to add a custom column in Activity Explorer. This ensures that the exported file contains specific details about the detected sensitive information types.

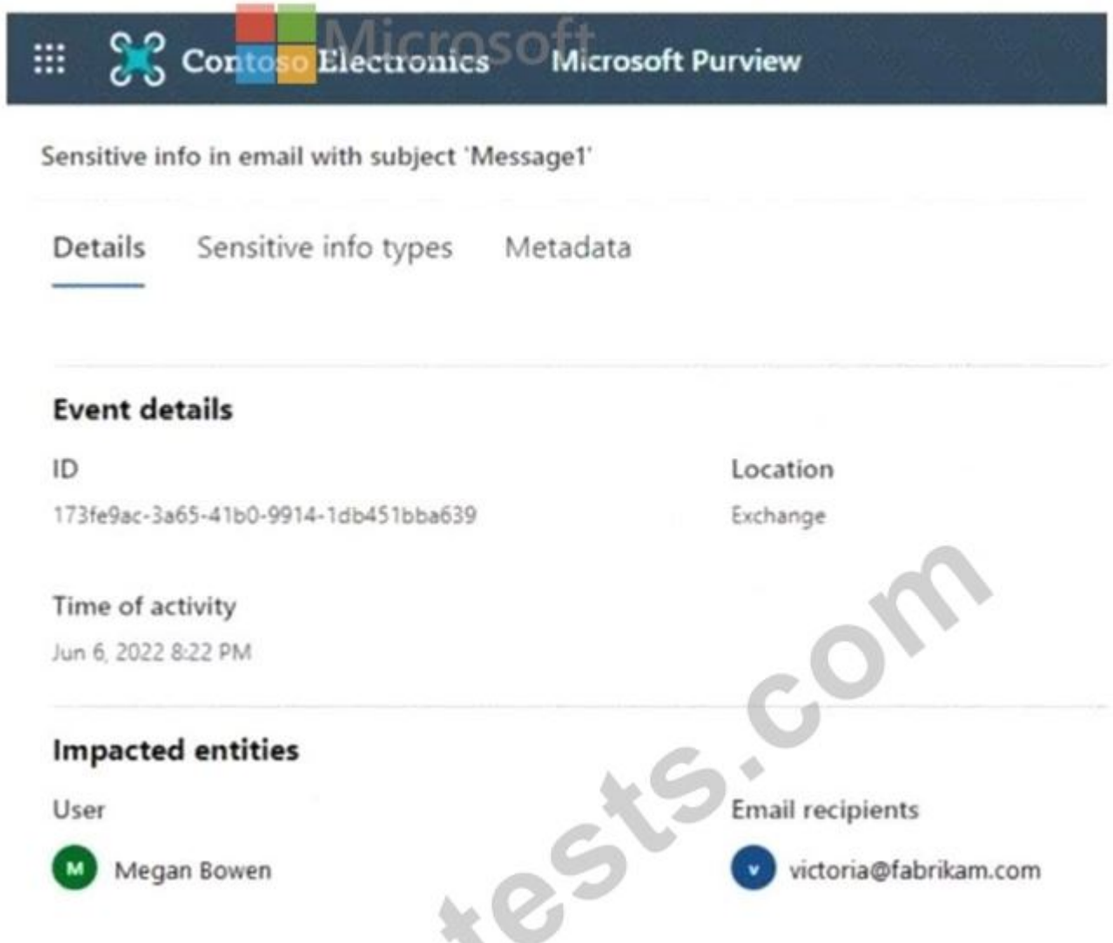
Box 2: DLP activity exports from Activity Explorer are always in CSV (Comma-Separated Values) format.

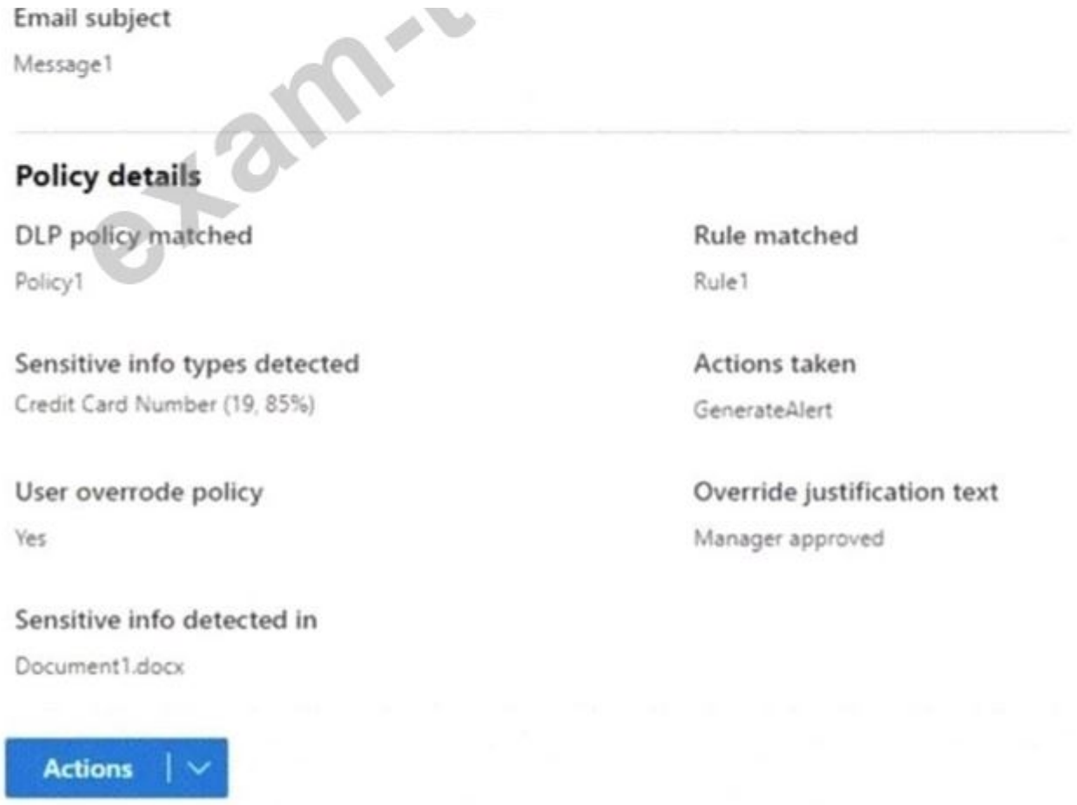
This format allows for easy data analysis and reporting in Excel or other data-processing tools.

Answer Area



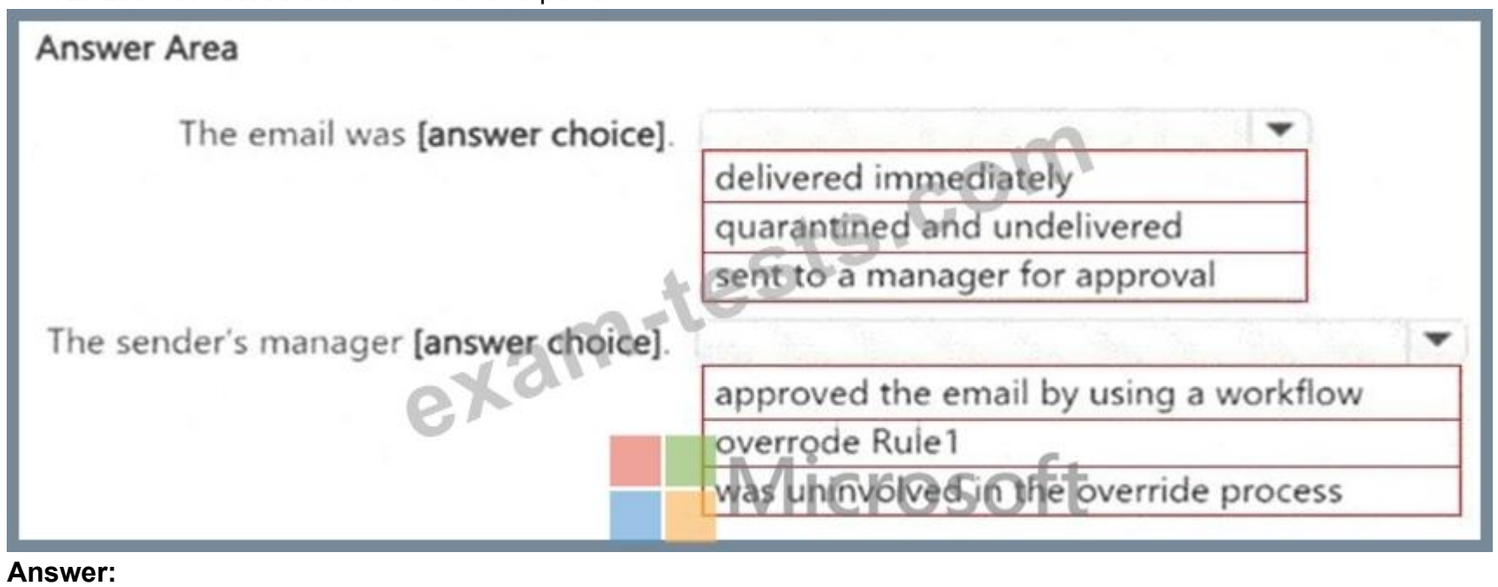
NEW QUESTION: 101
HOTSPOT
You have a Microsoft 365 E5 subscription.
You receive the data loss prevention (DLP) alert shown in the following exhibit.





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

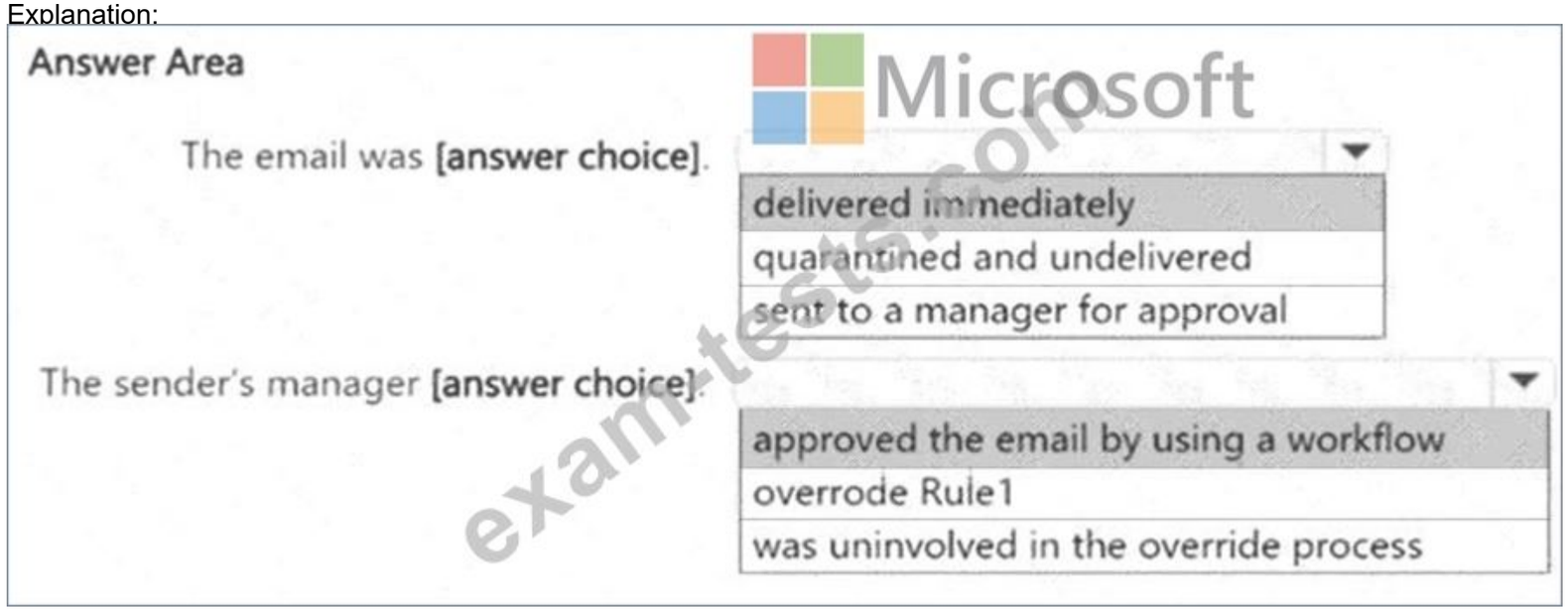
NOTE: Each correct selection is worth one point.



Answer:

Answer Area

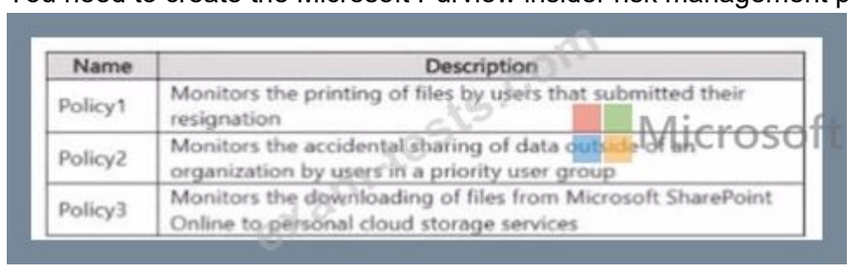
Explanation:



NEW QUESTION: 102

You have a Microsoft 36S ES 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 polices 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..

Answer:

Explanation:

NEW QUESTION: 103

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to implement Microsoft Purview data lifecycle management.

What should you create first?

A. a sensitivity label policy

B. a data loss prevention (DLP) policy

C. an auto-labeling policy

D. a retention label

Answer: D (LEAVE A REPLY)

To implement Microsoft Purview Data Lifecycle Management for SharePoint Online (Site1), you need to create a retention label first. Retention labels define how long content should be retained or deleted based on compliance requirements. Once a retention label is created, it can be manually or automatically applied to content in SharePoint Online, Exchange, OneDrive, and Teams. After creating a retention label, you can configure label policies to apply them to Site1 and other locations.

NEW QUESTION: 104
You have a Microsoft 365 E5 subscription. The subscription contains a user named User1 and the sensitivity labels shown in the following table.

Name	Authenticated users: View content(VIEW)	Authenticated users: Copy and extract content(EXTRACT)	Authenticated users: Export content(EXPORT)
Label1	Granted	Not granted	Not granted
Label2	Granted	Granted	Not granted
Label3	Granted	Not granted	Granted

You publish the labels to User1.
The subscription contains the files shown in the following table.

Name	Label
File1	Label1
File2	Label2
File3	Label3

Which files can Microsoft 365 Copilot summarize for User1?
A. File2only
B. File3 only
C. File2 and File3 only
D. File1, File2. and File3
Answer: (SHOW ANSWER)
Microsoft 365 Copilot can only process (summarize, answer questions about) a labeled file when the user has the Copy and extract content (EXTRACT) usage right granted by the applied sensitivity label.
From the table of labels:
* Label1 # VIEW only (no EXTRACT) # Copilot cannot summarize.
* Label2 # VIEW and EXTRACT granted # Copilot can summarize.
* Label3 # VIEW and EXPORT (no EXTRACT) # Copilot cannot summarize.
Since File2 is labeled Label2, it's the only file for which User1 has the required EXTRACT permission, so it' s the only file Copilot can summarize.
References:
Microsoft Learn - Sensitivity labels and Copilot for Microsoft 365: Copilot requires the Copy and extract content (EXTRACT) permission to process labeled content.https://learn.microsoft.com/microsoft-365/compliance/sensitivity-labels-copilot
Microsoft Learn - Usage rights for encryption with sensitivity labels (VIEW, EXTRACT, EXPORT definitions)https://learn.microsoft.com/microsoft-365/compliance/encryption-sensitivity-labels#usage-rights- and-permissions

NEW QUESTION: 105
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 Conlent1 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. File1 .docx, File2.docx, and File3.docx

Answer: (SHOW ANSWER)

The content search uses the KQL editor with the query -Author:USER1. In eDiscovery/Content search, the minus sign denotes NOT and KQL is case-insensitive for property values. Therefore, this query returns items whose Author is not 'User1'.

File1.docx # Author = User1 # excluded

File2.docx # Author = User2 # included

File3.docx # Author = USER1 (same as User1, case-insensitive) # excluded Result: File2.docx only.

Reference: Microsoft Search (KQL) property restrictions and case-insensitive behavior for queries in content search.

NEW QUESTION: 106

Hotspot Question

You have a Microsoft 365 tenant that uses Microsoft Teams.

You create a data loss prevention (DLP) policy to prevent Microsoft Teams users from sharing sensitive information, You need to identify which locations must be selected to meet the following requirements:

- Documents that contain sensitive information must not be shared inappropriately in Microsoft Teams.
- If a user attempts to share sensitive information during a Microsoft Teams chat session, the message must be deleted immediately.

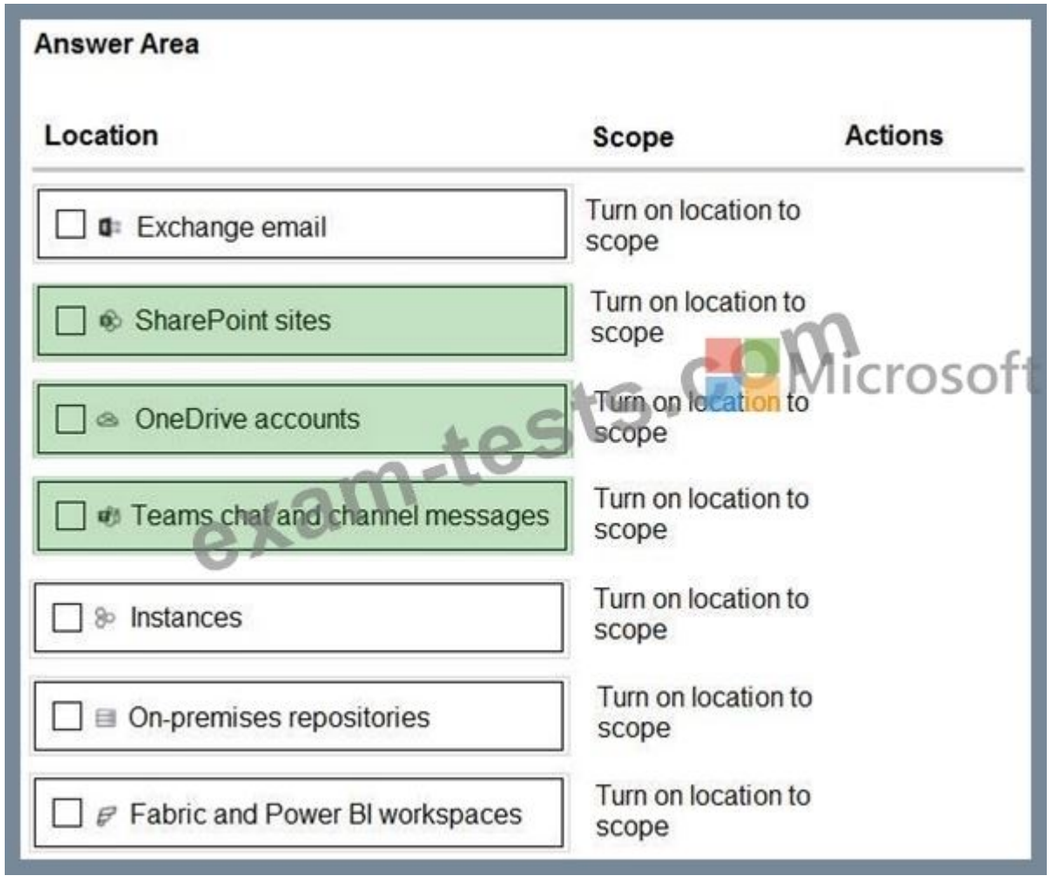
Which three locations should you select? To answer, select the appropriate locations in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Location	Scope	Actions
☐ Exchange email	Turn on location to scope	
☐ SharePoint sites	Turn on location to scope	
☐ OneDrive accounts	Turn on location to scope	
☐ Teams chat and channel messages	Turn on location to scope	
☐ Instances	Turn on location to scope	
☐ On-premises repositories	Turn on location to scope	
☐ Fabric and Power BI workspaces	Turn on location to scope	

Answer:



Explanation:

Reference:

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

NEW QUESTION: 107

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?

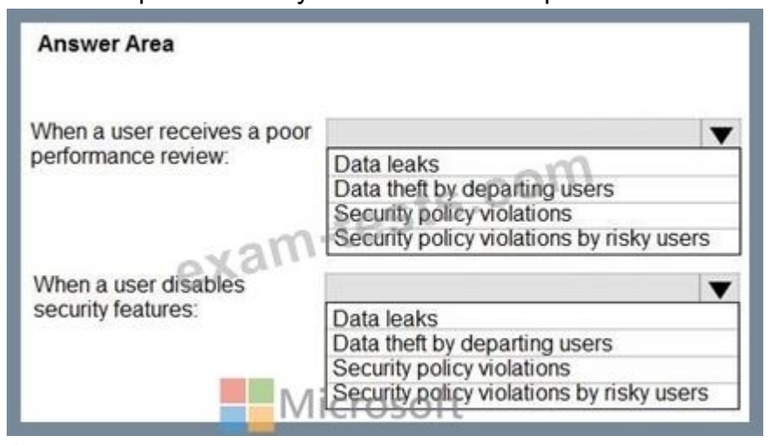
A. Yes

B. No

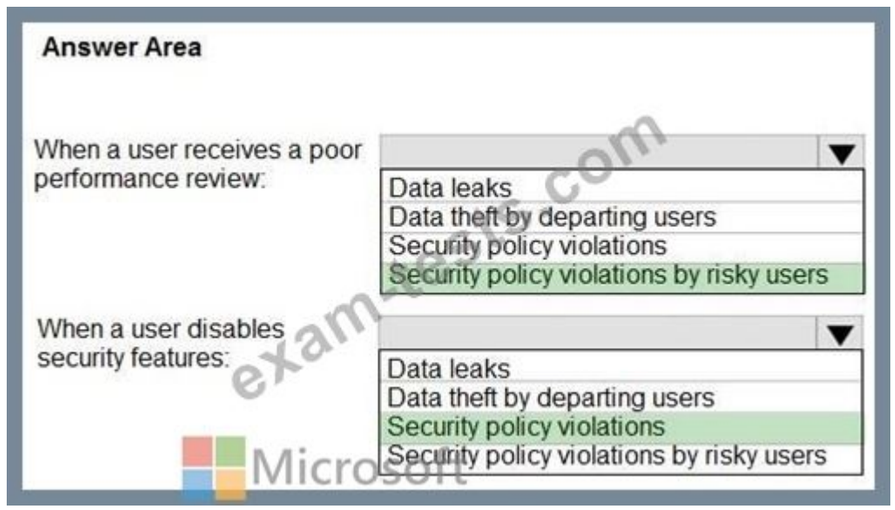
Answer: B (LEAVE A REPLY)
To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.
Text patterns in mail flow rules are not as reliable as sensitive information types in DLP.
Mail flow rules lack advanced content detection and machine learning-based classification, making them less effective than DLP.

NEW QUESTION: 108
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 User 1 appeal 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 User I. 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-AuditConfig -Workload Exchange command.
Does that meet the goal?
A. No
B. Yes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 109
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:



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: 110

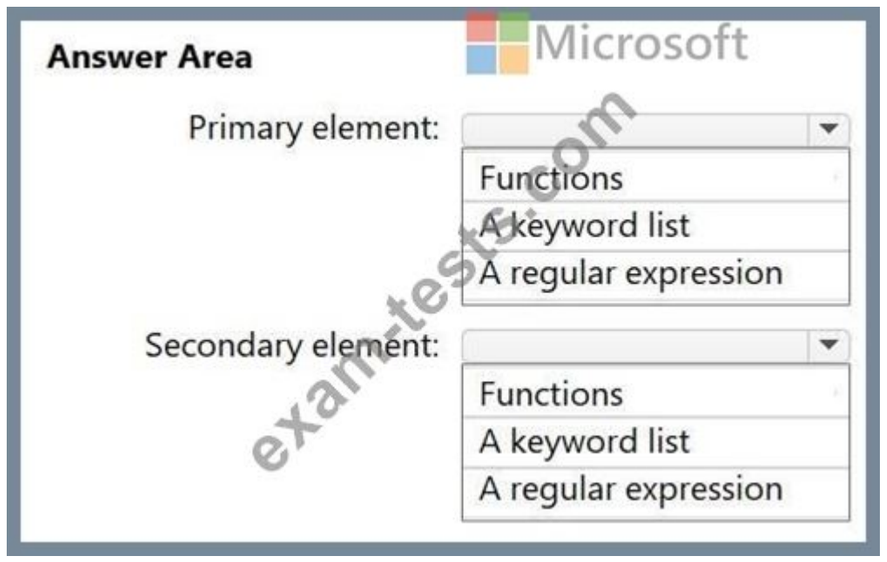
Hotspot Question

You have a Microsoft 365 tenant.

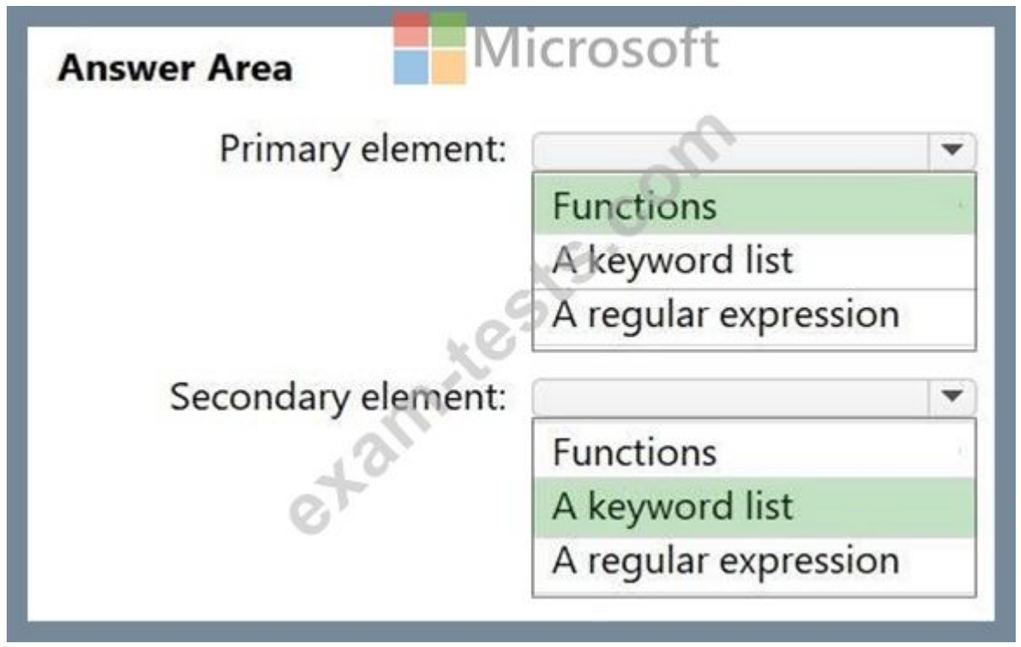
You need to create a new sensitive info type for items that contain the following:

- An employee ID number that consists of the hire date of the employee
followed by a three digit number
- The words "Employee", "ID", or "Identification" within 300 characters of the employee ID number What should you use for the primary and secondary elements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Box 1: Functions

Need to include use a date function for the primary element.

Note: Create custom sensitive information types

The primary element can be a Regular expression with an optional validator, a Keyword list, a Keyword dictionary, or one of the pre-configured Functions.

Box 2: A keyword list

Use a keyword list which includes the words "Employee", "ID", or "Identification".

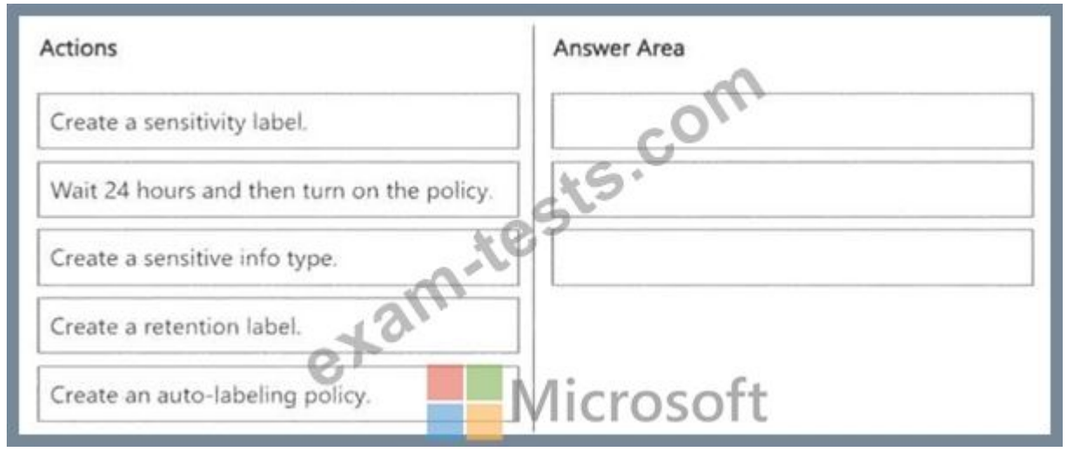
Reference:

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

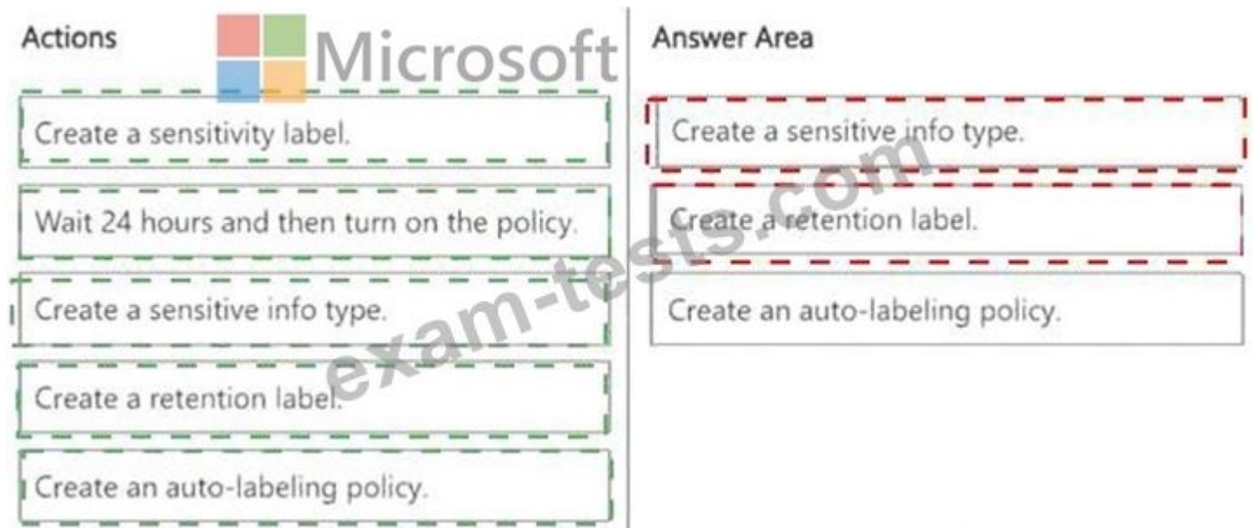
NEW QUESTION: 111

You need to meet the technical requirements for the Site1 documents.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

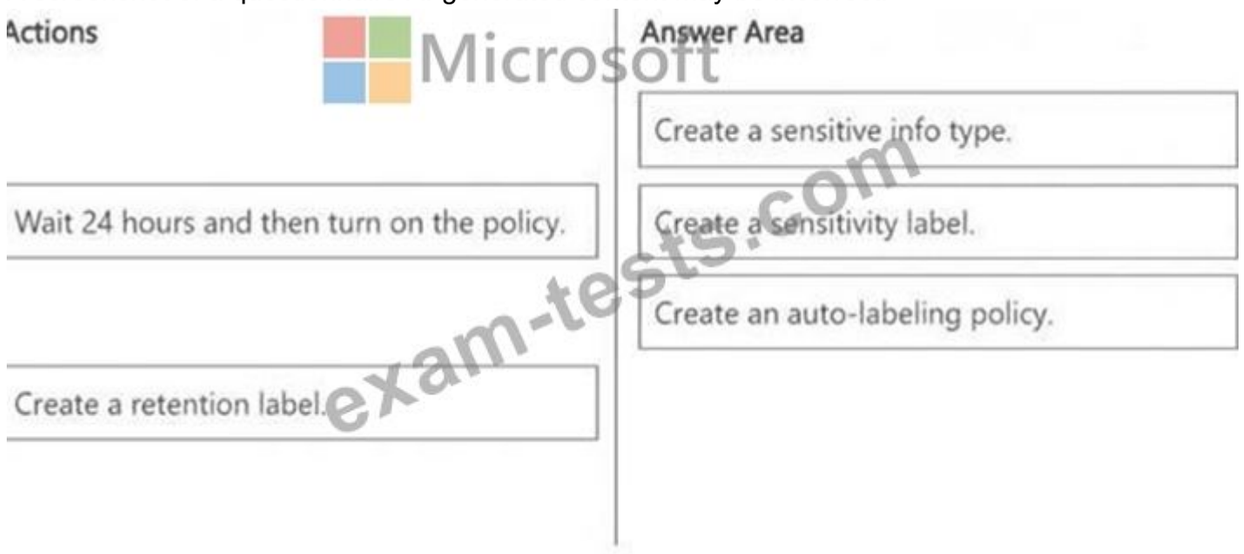


Answer:



Explanation:

A screenshot of a questionnaire AI-generated content may be incorrect.



The goal is to automatically label documents in Site1 that contain credit card numbers. To achieve this, we need a sensitivity label with an auto-labeling policy based on a sensitive info type

that detects credit card numbers.
Step 1: Create a Sensitive Info Type
A sensitive info type is needed to detect credit card numbers in documents.
Microsoft Purview includes built-in sensitive info types for credit card numbers, but we can also create a custom one if necessary.
Step 2: Create a Sensitivity Label
A sensitivity label is required to classify and protect documents containing sensitive information.
This label can apply encryption, watermarking, or access controls to credit card data.
Step 3: Create an Auto-Labeling Policy
An auto-labeling policy ensures that the sensitivity label is applied automatically when credit card numbers are detected in Site1.
This policy is configured to scan files and automatically apply the correct sensitivity label.
Topic 1, Contoso, Ltd Case Study 1
Instructions
This is a case study. Case studies are not timed separately from other exam sections. You can use as much exam time as you would like to complete each case study. However, there might be additional case studies or other exam sections. Manage your time to ensure that you can complete all the exam sections in the time provided. Pay attention to the Exam Progress at the top of the screen so you have sufficient time to complete any exam sections that follow this case study.
To answer the case study questions, you will need to reference information that is provided in the case. Case studies and associated questions might contain exhibits or other resources that provide more information about the scenario described in the case. Information provided in an individual question does not apply to the other questions in the case study.
A Review Screen will appear at the end of this case study. From the Review Screen, you can review and change your answers before you move to the next exam section. After you leave this case study, you will NOT be able to return to it.
To start the case study
To display the first question in this case study, select the "Next" button. To the left of the question, a menu provides links to information such as business requirements, the existing environment, and problem statements. Please read through all this information before answering any questions. When you are ready to answer a question, select the "Question" button to return to the question.
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.

NEW QUESTION: 112
You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3 and a file named Filetdocx.
You create a sensitivity label named Label1 as shown in the following exhibit.

You apply Label1 to File1.
For which users can Microsoft 365 Copilot summarize File1?
A. No user
B. User 1 only
C. User1 and User2 only
D. User1, User2, and User3
Answer: A (LEAVE A REPLY)
The sensitivity label Label1 assigns permissions (User1 = Co-Author, User2 = Reviewer, User3 = Viewer) and enables Double Key Encryption (DKE). Microsoft 365 Copilot can summarize content only when the service can access the file using the user's permissions. Content protected with Double Key Encryption is not accessible to Microsoft cloud services (including Copilot); as a result, Copilot cannot open or process DKE- protected files for any user, even if they can open the file themselves in Office apps.
Therefore, no user can use Microsoft 365 Copilot to summarize File1.
Reference: Microsoft Purview Double Key Encryption-service access limitations for Microsoft cloud services, including Copilot and search indexing.

NEW QUESTION: 113
You have a Microsoft 36S ES subscription that contains the devices shown in the following table.

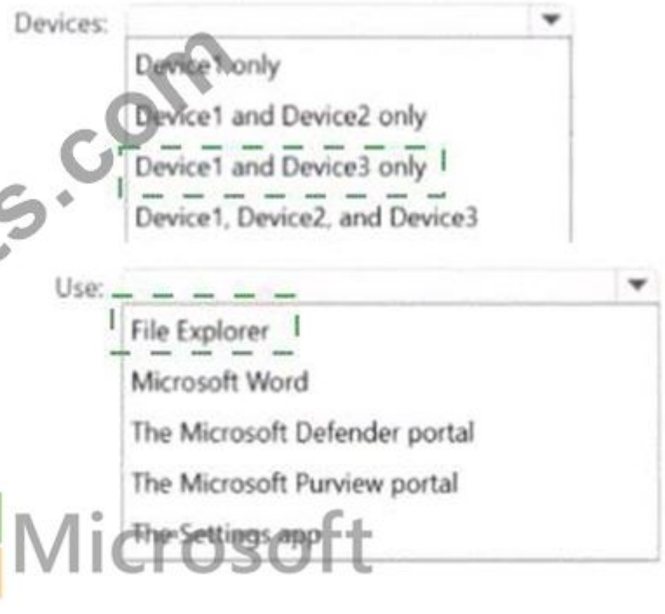
Name	Platform	Chipset
Device1	Windows 11	x64
Device2	Windows 11	ARM64
Device3	Windows 10	x86

You publish Microsoft Purview Information Protection sensitivity labels.

You plan to deploy the information protection client to the devices. The solution must ensure that the labels can be applied to sensitive images and documents On which devices can you install the information protection client, and what should users use to apply labels?

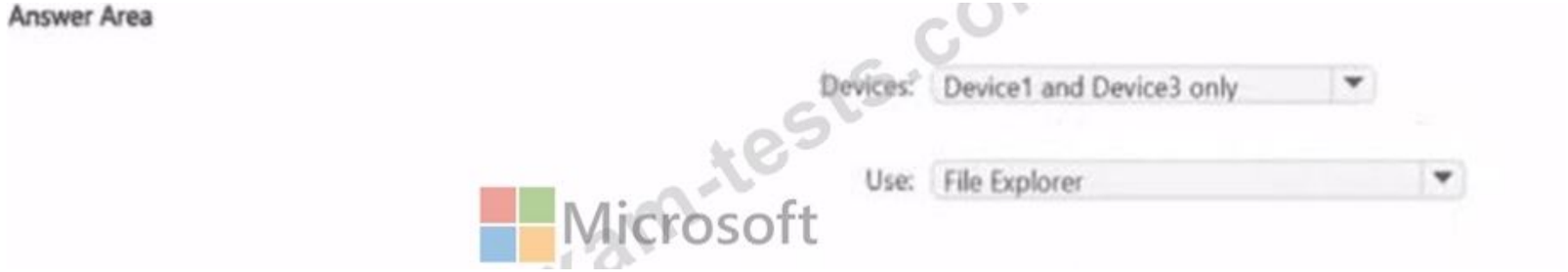
To answer, select the appropriate options in the answer area.

Answer:



Explanation:

Answer Area



Step 1 - Understanding the requirement
The task is about applying Microsoft Purview Information Protection sensitivity labels to sensitive images and documents using the Azure Information Protection (AIP) unified labeling client.
Sensitivity labels in Purview can be applied in Microsoft 365 apps (Word, Excel, Outlook, PowerPoint), but to label non-Office files like images, PDFs, and other documents, users must use the AIP unified labeling client.
With the AIP client installed, labels can be applied directly in File Explorer by right-clicking the file.
Step 2 - Device compatibility
The AIP unified labeling client runs on Windows devices only.
In the question's context (based on the provided dropdowns), all listed devices (Device1, Device2, Device3) are compatible Windows endpoints.
Therefore, the AIP client can be deployed to all three devices.
Step 3 - How users apply labels
For Office documents # labels can be applied from the ribbon inside Word, Excel, PowerPoint.
For other file types (images, PDFs, text files, etc.) # labels must be applied using File Explorer via the AIP client.
Reference:
Install and use the Azure Information Protection unified labeling client Apply sensitivity labels to files and emails in Microsoft Purview

NEW QUESTION: 114
Hotspot Question
You have a Microsoft 365 subscription that uses Microsoft Purview data loss prevention (DLP) policies. The subscription contains the devices shown in the following table.

Name	Operating system	Microsoft Defender for Endpoint	Installed browser
Device1	Windows 11	Onboarded	Microsoft Edge, Google Chrome
Device2	macOS	Not onboarded	Google Chrome, Firefox

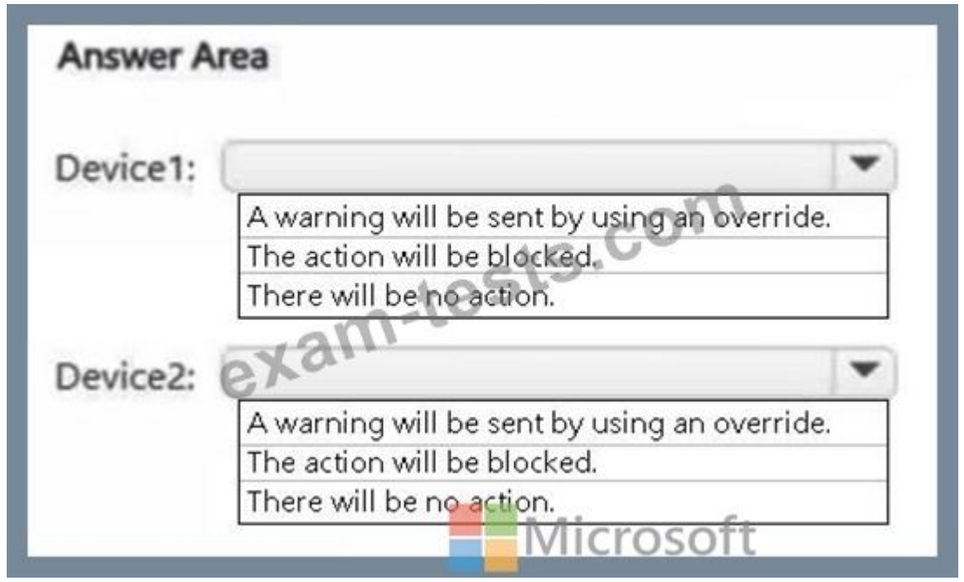
You create a DLP policy that has the following configurations:
- Name: Policy1
- Locations: Devices
- Action (enforcement): Block
- Adaptive protection Enabled
- Targets elevated risk users
- Users and groups: All users and groups
- User notification: Notify users (optional)
- Targeted URLs: Unapproved AI websites
- Sensitive information types (SITs): Confidential

You deploy Policy1 and set the mode to enforcement.

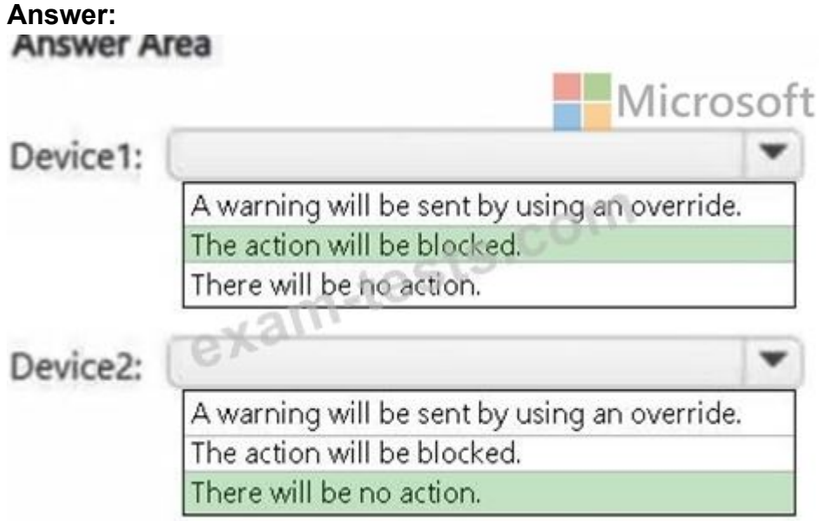
What will occur when a user on each device attempts to paste text to a Microsoft Copilot website?

To answer, select the options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Box 1: The action will be blocked.

The paste action will be blocked in Microsoft Edge, and the user will receive a notification. If the user attempts to bypass this by using Google Chrome, the browser itself will be completely blocked from accessing the site (or pasting will be natively blocked if the Microsoft Purview Extension is installed).

Device 1 (Windows 11 - Onboarded)

Because Device1 is onboarded via Microsoft Defender for Endpoint, it actively pulls and enforces Microsoft Purview Endpoint DLP rules at the operating system and application level.

Microsoft Edge: Edge features native integration with Microsoft Purview. When the user attempts to paste text flagged with the Confidential SIT into an unapproved AI domain, Edge intercepts the clipboard action natively and blocks the paste, triggering a user notification pop-up.

Google Chrome: Because D evice11 is a managed Windows endpoint, Endpoint DLP settings will actively monitor browser activity. If the Microsoft Purview Extension for Chrome is present, the paste will be blocked inline exactly like Edge. If the extension is missing, Purview's network/browser restrictions will block access to the targeted URL entirely within Chrome to prevent policy circumvention.

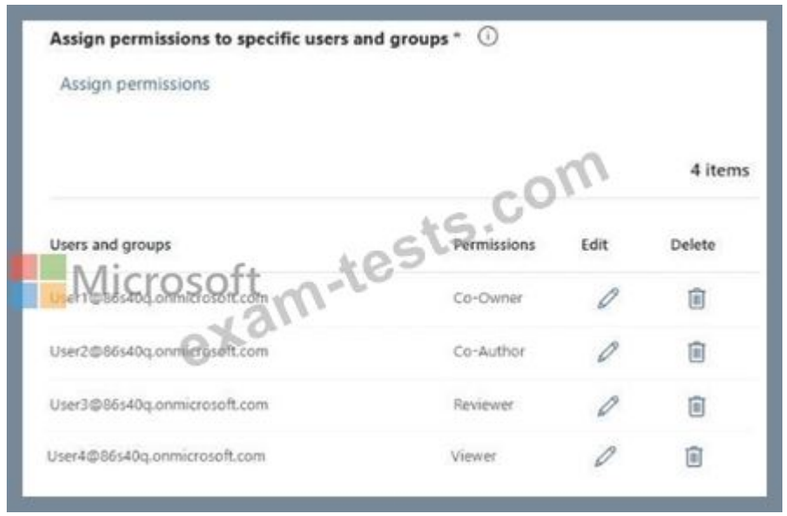
Box 2: There will be no action.
The policy will fail to evaluate or enforce any restrictions, allowing the text to be pasted freely in both Firefox and Google Chrome.
Device 2 (MacOS - Not Onboarded)
The "Devices" location in Microsoft Purview DLP policies relies entirely on local OS telemetry and compliance hooks.
No Enforcement: Because Device 2 is not onboarded into Microsoft Defender for Endpoint (or Microsoft Purview device management), the device does not download the organizational DLP policy binaries or rules.
Browser Behavior: Neither Firefox nor Google Chrome on MacOS has a native mechanism to communicate with your tenant's Purview configuration without an onboarded base OS layer.
Result: The policy engine remains completely blind to Device2's clipboard and network activity, resulting in no block and no user notification.
Reference:
https://learn.microsoft.com/en-us/purview/endpoint-dlp-getting-started

NEW QUESTION: 115
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 Exchange Online PowerShell. run Start-ManagedFolderAssistant.
B. From the Microsoft Purview portal, create a data loss prevention (DLP) policy.
C. From the Microsoft Purview portal, create a label policy.
D. From Exchange Online PowerShell, run start -RetentionAutoTagLearning.
Answer: A (LEAVE A REPLY)
Retention policy tags (MRM) for Exchange Online are applied by the Managed Folder Assistant (MFA). To apply a newly created Exchange retention policy to mailbox items immediately, you manually invoke MFA with Start-ManagedFolderAssistant for the mailbox or set of mailboxes. Creating DLP policies or label policies in Purview does not accelerate MRM processing.

NEW QUESTION: 116
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 5
You need to ensure that a group named U.S. Sales can store files containing information subject to General Data Protection Regulation (GDPR) in their OneDrive accounts. All other current GDPR restrictions must remain in effect.
Answer:
Note: Policy templates

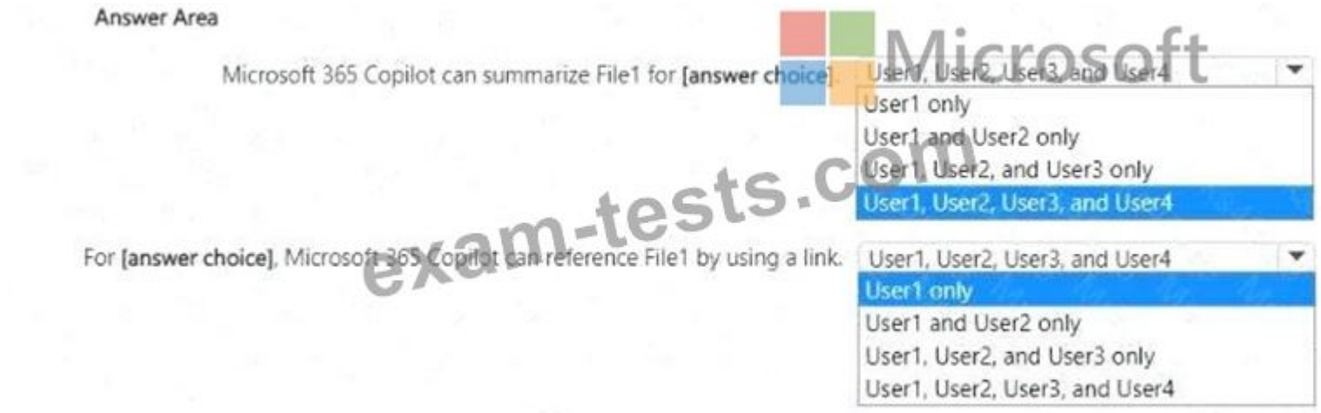
DLP policy templates are sorted into four categories:
* policies that can detect and protect types of Financial information.
* Medical and health
* Privacy
- Includes General Data Protection Regulation (GDPR) Enhanced
* Custom policy
Step 1: Sign in to the Microsoft Purview compliance portal.
Step 2: In the Microsoft Purview compliance portal > left navigation > Solutions > Data loss prevention > Policies > + Create policy.
Step 3: Select Custom from the Categories list.
Step 4: Select Custom from the Regulations list.
Step 5: Give the policy a name.
Step 6: Fill in a description. (Skip)
Step 7: Select Next.
Step 8: Select Full directory under Admin units.
Step 9: Set the OneDrive location status to On. Set all the other location status to Off.
Step 10: Edit the OneDrive accounts scope. Select All users and group >Include users and groups > + Include > Include groups and add the U.S. Sales group.
Question is: You need to ensure that a group named U.S. Sales can store files containing information subject to General Data Protection Regulation (GDPR) in their OneDrive accounts. All other current GDPR restrictions must remain in effect.
Step 11: Select Done. Select Done. Select Next.
Step 12: On the Define policy settings page, the Create or customize advanced DLP rules option should already be selected.
Step 13: Select Next. Select Create rule. Name the rule and provide a description.
Step 14: Under Conditions select + Add condition >
Step 15: Select Content contains > Add > Sensitive info types > General Data Protection Regulation (GDPR). Choose Add.
Step 16: Under Actions, select Add an action > Allow Access (or similar) Step 17: Finish the wizard: Choose Save. Choose Next. Choose Done Reference:
https://learn.microsoft.com/en-us/purview/dlp-policy-reference
https://learn.microsoft.com/en-us/purview/dlp-create-deploy-policy

NEW QUESTION: 117
You have a Microsoft 365 E5 subscription that contains four users named User1, User2, User3, and User4 and a file named File1.docx.
To File1, you apply a sensitivity label that has the permissions shown in the following exhibit.

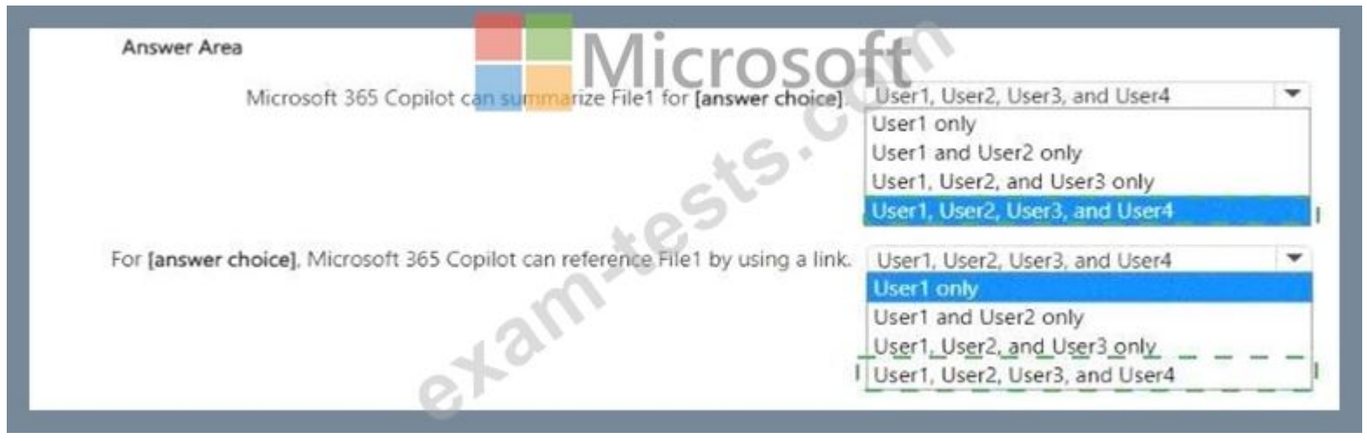


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

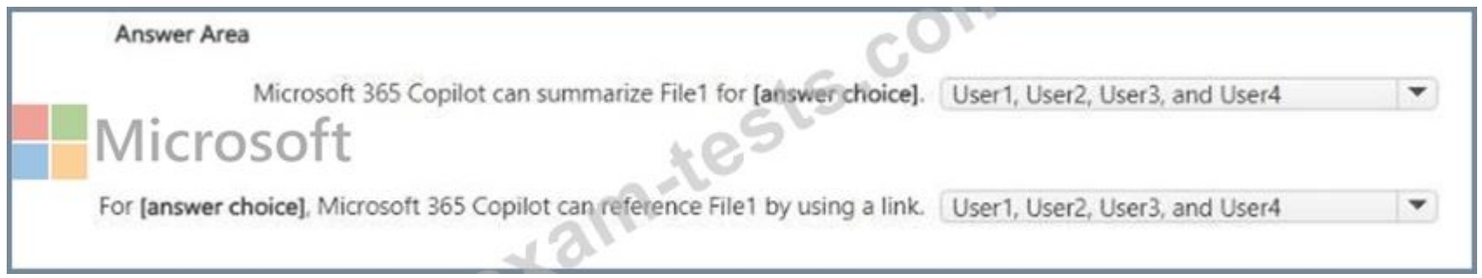
NOTE; Each correct selection is worth one point.



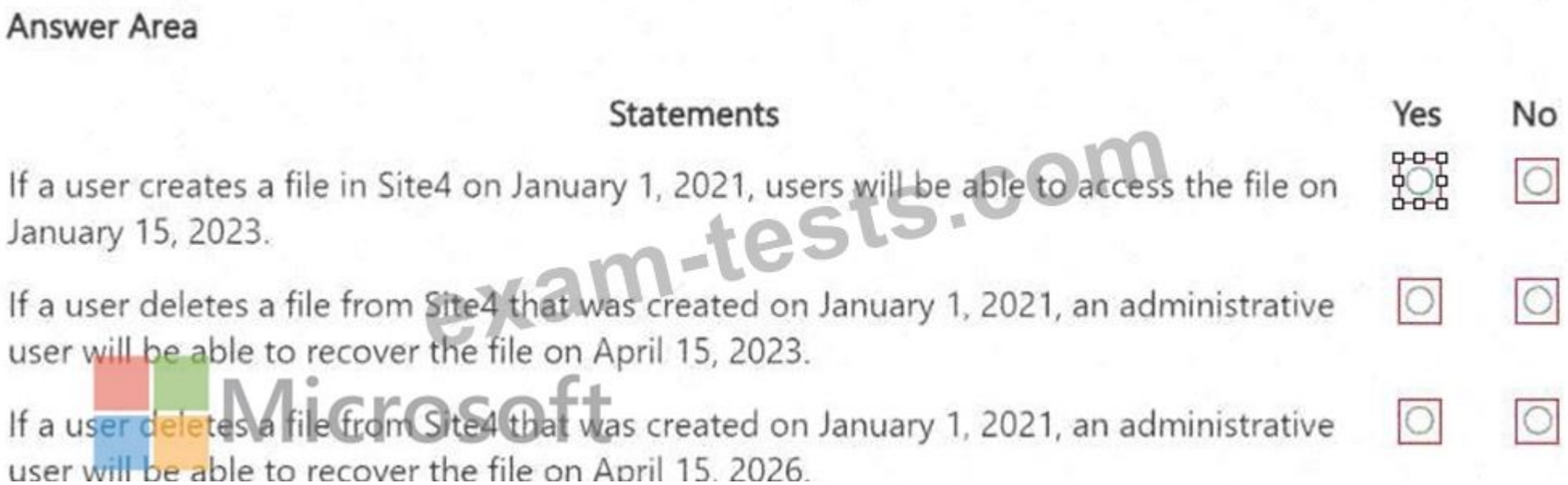
Answer:



Explanation:



NEW QUESTION: 118
HOTSPOT
You are reviewing policies for the SharePoint Online environment.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:
A white paper with black text AI-generated content may be incorrect.

Answer Area

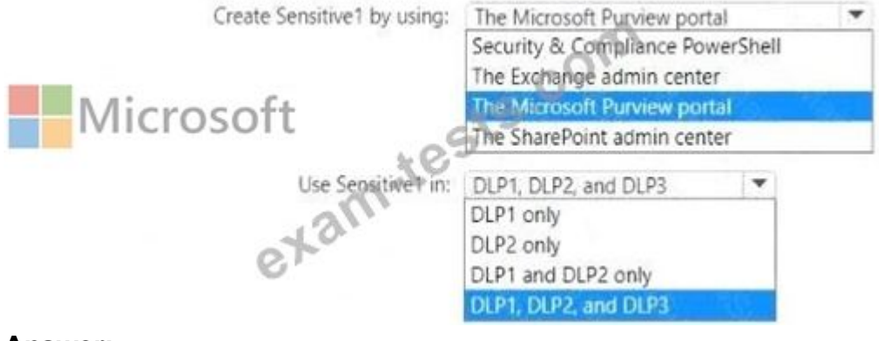
Statements	Yes	No
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	○	○
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2023.	○	○
If a user deletes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

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

NEW QUESTION: 119
You have a Microsoft 365 E5 subscription that contains the data loss prevention (DLP) policies shown in the following table.

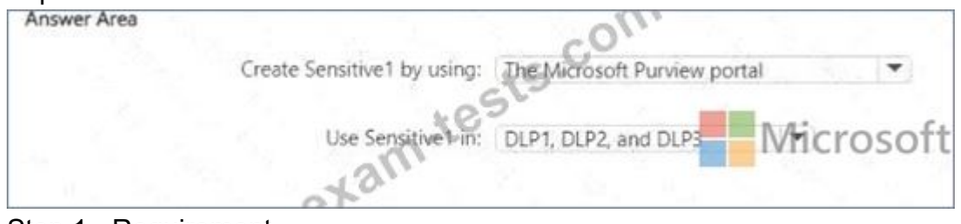
Name	Applied to
DLP1	Microsoft Exchange Online email
DLP2	Microsoft SharePoint Online sites
DLP3	Microsoft Teams chat and channel messages

You have a custom employee information form named Template1 .docx.
You plan to create a sensitive info type named Sensitive! 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.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Step 1 - Requirement

You want to create a custom sensitive info type named Sensitive1.

This SIT will be created from a document fingerprint of Template1.docx.

You then want to use Sensitive1 in DLP policies.

Step 2 - Where do you create custom Sensitive Info Types?

Custom SITs (including document fingerprinting) can only be created in the Microsoft Purview compliance portal.

They cannot be created in the Exchange admin center, SharePoint admin center, or directly in PowerShell.

Answer for creation: The Microsoft Purview portal

Reference: Create a custom sensitive information type with document fingerprinting Step 3 - Where can custom Sensitive Info Types be used?

Once created, custom SITs are tenant-wide and can be used across all workloads that support DLP:

Exchange email

SharePoint Online sites

OneDrive

Teams chat and channel messages

In the table, the DLP policies are:

DLP1 # Exchange Online email

DLP2 # SharePoint Online sites

DLP3 # Teams chat and channel messages

Since Sensitive1 is a custom SIT, it can be used in all three policies.

Answer for usage: DLP1, DLP2, and DLP3

NEW QUESTION: 120

Hotspot Question

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

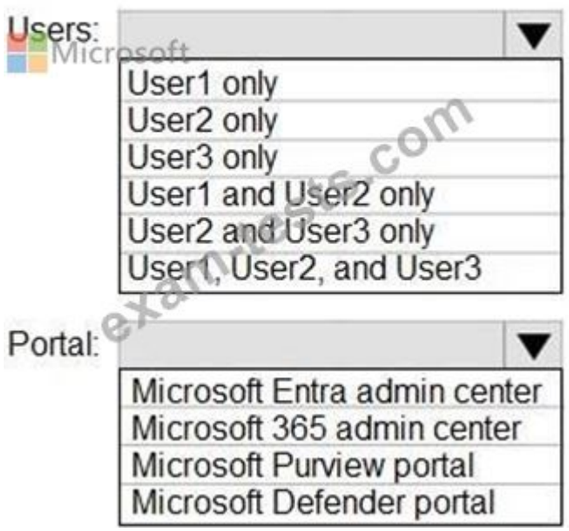
Name	Role
User1	Compliance Administrator
User2	Security Operator
User3	eDiscovery Manager

You need to implement sensitivity labels.

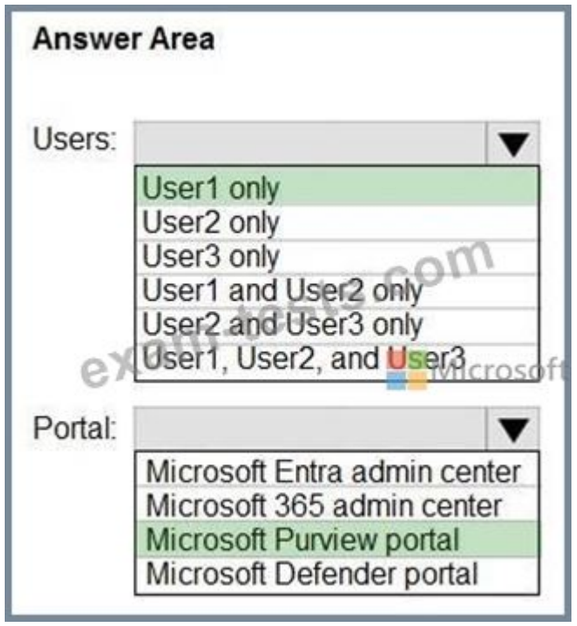
Which users can create sensitivity labels, and which portal should the users use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:



Explanation:

Reference:

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

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

NEW QUESTION: 121
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: B (LEAVE A REPLY)
* 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: 122
You have a Microsoft 365 E5 subscription.
Users access their mailbox by using the following apps.

* Outlook for Microsoft 365
* Outlook on the web
* Outlook Mobile fiOS. Android)

You create a data loss prevention (DLP) policy named DLP1 that has the following settings:

* Location; Exchange email
* Status: On
* User notifications: On
* Notify users with a policy tip: Enabled

Which apps display a policy tip when content is matched by using DIP1 ?

A. Outlook for Microsoft 365 only
B. Outlook on the web only
C. Outlook for Microsoft 365 and Outlook on the web only
D. Outlook for Microsoft 365 and Outlook Mobile (iOS. Android) only
E. Outlook for Microsoft 365. Outlook on the web, and Outlook Mobile (iOS. Android)

Answer: C (LEAVE A REPLY)

Policy tips in DLP: Policy tips are messages shown to users when their action (such as sending sensitive content via email) conflicts with a DLP policy.

For Exchange email location, policy tips are supported in the following apps:

Outlook for Microsoft 365 (desktop client) #

Outlook on the web (OWA) #

Outlook Mobile (iOS/Android) # Policy tips are not shown in mobile apps. Instead, DLP actions (block/restrict /send incident report) still apply, but the user does not see a policy tip notification.

Therefore:

Supported: Outlook for Microsoft 365, Outlook on the web.

Not supported: Outlook Mobile apps.

Reference:

Microsoft Learn: Policy tips in DLP

Quote: "Policy tips are supported in Outlook on the web and Outlook 2013 and later. Policy tips are not supported in Outlook mobile apps."

NEW QUESTION: 123

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.

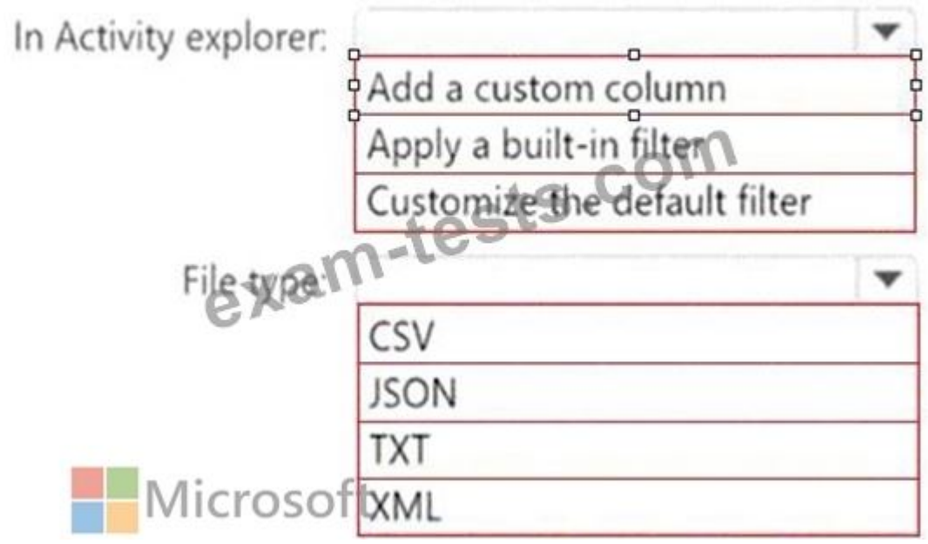
Answer: (SHOW ANSWER)

Required for monitoring interactions with third-party generative AI sites:

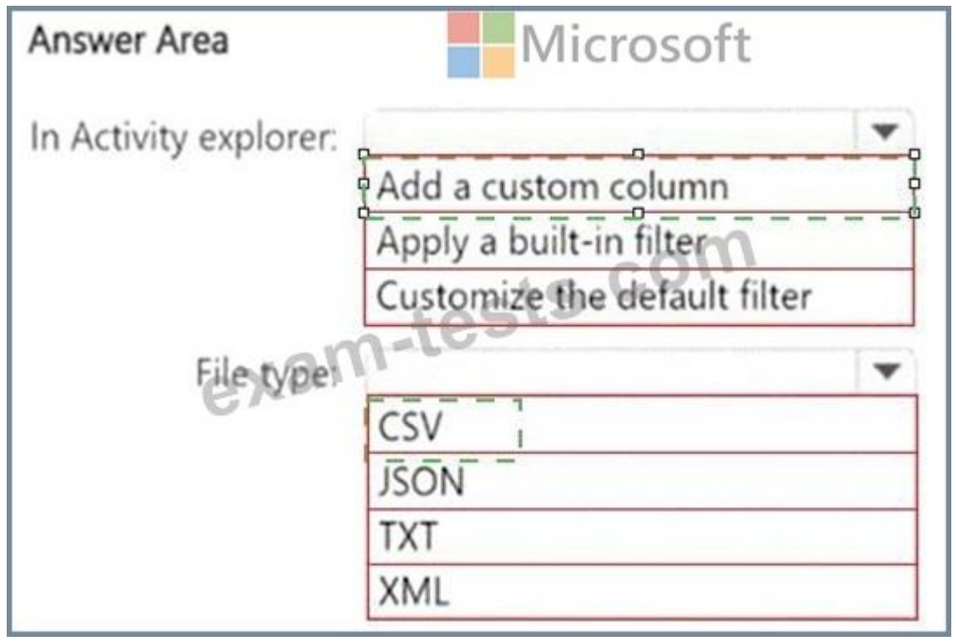
[B] * Devices are onboarded to Microsoft Purview, required for:
- Gaining visibility into sensitive information that's shared with third-party generative AI sites. For example, a user pastes credit card numbers into ChatGPT.
[A]- Applying endpoint DLP policies to warn or block users from sharing sensitive 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: 124
HOTSPOT
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.
You plan to export DLP activity by using Activity explorer.
The exported file needs to display the sensitive info type detected for each DLP rule match.
What should you do in Activity explorer before exporting the data, and in which file format is the file exported? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:



Explanation:

Box 1: To include the sensitive info type detected for each DLP rule match, you need to add a custom column in Activity Explorer. This ensures that the exported file contains specific details about the detected sensitive information types.

Box 2: DLP activity exports from Activity Explorer are always in CSV (Comma-Separated Values) format.

This format allows for easy data analysis and reporting in Excel or other data-processing tools.